HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 043 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 2, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 2, 2017

● (1530)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I would like to call the 43rd meeting of the ethics committee to order. I think I need to turn the floor immediately over to our clerk for the first order of business.

[*Translation*]

The Clerk of the Committee (Mr. Hugues La Rue): Hello everyone.

Pursuant to Standing Order 106(2), we need to elect the first vice-chair, who must be a member of the government party.

I'm now ready to receive motions for the election of the first vice-chair.

[*English*]

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Mr. Chair, I nominate Nathaniel Erskine-Smith as vice-chair.

[*Translation*]

The Clerk: It was moved by Mr. Kelly that Mr. Erskine-Smith be elected vice-chair of the committee.

Are there any other motions?

[*English*]

Mr. Erskine-Smith is duly elected vice-chair of the committee.

(Motion agreed to)

The Chair: Congratulations, Mr. Erskine-Smith.

Let's get back to the item before us, colleagues, now that is taken care of.

Colleagues, we are pleased to have with us today in our continued study of the SCISA, otherwise known as Security of Canada Information Sharing Act, from the Department of Transport, Mr. Donald Roussel, associate assistant deputy minister, safety and security group, and Marie-France Paquet, director general, intermodal surface, security, and emergency preparedness. From the Communications Security Establishment, we have Mr. Dominic Rochon, deputy chief, policy and communications. From the Department of National Defence, we have Mr. Stephen Burt, assistant chief of defence intelligence, Canadian Forces intelligence command. There are also all sorts of other support staff in the room.

We thank you very much for being here. It's much appreciated. We've had a lot of testimony. I'm sure you've had an opportunity to review some of that testimony from groups presenting here before the committee. Now it's our pleasure to actually hear from the folks who use the legislation.

We'll hear for up to 10 minutes from each of your respective departments in the order in which you were introduced.

Mr. Roussel or Madam Paquet, the floor is yours for up to 10 minutes, please.

Mr. Donald Roussel (Associate Assistant Deputy Minister, Safety and Security Group, Department of Transport): Thank you, Mr. Chairman, for the invitation to appear before the committee. My name is Donald Roussel, and I am the associate assistant deputy minister for safety and security at Transport Canada. I am joined, as you mentioned, by Marie-France Paquet, director general, intermodal surface, security, and emergency preparedness.

I will go through an overview of the mandate of our department, which includes the promotion of safe, secure, and efficient transportation for Canada and Canadians.

To fulfill our mandate, the department uses, updates, or develops legislation, regulations, policies, and standards to safeguard the integrity of the air, marine, and surface modes of transportation for Canada. We also implement programs. We monitor, test, and inspect to enforce the regulations and the standards.

The main groups in charge of promoting security are aviation security, marine safety and security, surface and intermodal security, the security screening program, and security intelligence assessment.

The aviation security directorate is responsible for safeguarding the integrity and security of the Canadian aviation system through a comprehensive suite of legislation, policies, regulations, and security measures. The directorate regulates and conducts oversight of the industry, including airports, air carriers, and airport tenants, and the Canadian Air Transport Security Authority, more known as CATSA, which provides screening services of passengers, their baggage, and non-passengers at 89 designated airports.

The marine safety and security directorate develops and implements policies and regulations promoting the safety and security of the marine transportation system, and conducts related oversight. This includes mandatory reporting of security incidents by industry, and comprehensive safety and security inspection regimes.

The surface and intermodal security directorate manages Transport Canada's rail security program. Guided by the Railway Safety Act, the International Bridges and Tunnels Act, and the Transportation of Dangerous Good Act, SIMS works with partners to enhance the security of surface and intermodal transportation across Canada.

The security screening branch collaborates with security and intelligence agencies and administers the transportation security clearance program to mitigate risks posed by individuals who are potential threats to aviation or maritime transportation and infrastructure.

The security intelligence assessment branch is the departmental point of contact with the intelligence community. It is responsible for analyzing and disseminating relevant intelligence within Transport and to industry stakeholders.

Finally, the emergency preparedness branch, which includes our situation centre, responds to emergency situations, safety and security incidents, natural disasters, or emerging threats impacting the national transportation system. The situation centre operates on a 24/7 basis and works in close co-operation with other government response centres.

On national security responsibilities, I will now turn to Transport's jurisdiction and responsibilities with respect to measures to mitigate external activities that undermine the national security of Canada and describe the safeguards ensuring that exchanges of information are conducted in compliance with federal legislation and policies.

Canada's national transportation system is vital to our economic prosperity and a key national security component that can be undermined by criminal activity, threats to, or interference with this vast and complex system.

Our responsibilities include identifying, tracking and responding to threats to surface—including rail, international bridges and tunnels—marine, and aviation transportation emanating from terrorists, sabotage, or other forms of unlawful interference, such as hostile cyber activity. Our security intelligence assessment branch depends on open source information, as well as classified information from agencies like the Canadian Security Intelligence Service or CSIS, the Royal Canadian Mounted Police, Global Affairs Canada, and the Communications Security Establishment Canada.

● (1535)

Access to security intelligence information allows Transport Canada to effectively and proactively identify and address threats to transportation. Any restrictions or reductions in the quality and quantity of information originating from the agencies with national security responsibilities could undermine our ability to meet or legislate responsibilities and negatively impact the security of Canada.

Transport Canada relies on multiple legislative and policy instruments to fulfill its mandate. These instruments allow the department to implement appropriate policies and regulations, deploy technologies that enhance transportation security, and conduct oversight and enforcement. I will briefly describe some of the legislation that Transport administers in relation to its national security responsibilities.

The Aeronautics Act is the primary legislation governing civil aviation in Canada and authorizes the development of regulations and security measures for the security of aerodromes and commercial aircraft operations. The Marine Transportation Security Act and the marine transportation security regulations provide the Minister of Transport with the authority to establish measures and regulations to ensure the security of Canada's marine transportation industry. This includes preventive measures and a framework to detect incidents that could affect vessels or marine facilities.

The Railway Safety Act promotes and provides for the safety and security of the public and personnel, as well as the protection of property and the environment for railway operations. The act has a number of instruments that can be used to promote security, including the issuance of emergency directives and security measures. TC has yet to resort to Security of Canada Information Sharing Act provisions to fulfill its national security responsibilities. Information exchanges occur under existing TC legislation or legal authorities of other institutions, as well as under the Privacy Act.

Regarding information safeguard mechanisms, information on security threats is found in different government institutions. That is why efficient and responsible sharing of information among government institutions is essential to a government's ability to identify, understand, and respond to threats to its national security. I will now describe the mechanisms in place to ensure that exchanges of information at Transport Canada respect Canadian laws and policies.

Since 2012, we have been guided by a comprehensive document entitled “The Transport Canada Intelligence Function Guidelines to Intelligence and Information Sharing”. It has clear instructions on information disclosure, including personal information among Government of Canada departments and agencies. All TC programs involving national security information disclosure include effective tracking systems to ensure privacy rights are respected. Here are some examples on how personal information disclosure is managed in two key programs with major national security implications.

First, the security screening program involves the use of a records management database and a stand-alone network to manage personal information on government employees, as well as workers who require access to restricted areas of ports and airports. Information is collected and disclosed pursuant to the appropriate consent obtained with the applicant's signature.

Secondly, the passenger protect program administered by Public Safety and the application of the Secure Air Travel Act aim to prevent listed individuals from threatening transportation security or using civil aviation to travel for the purposes of terrorism. TC is mainly responsible for delivering the operational components of the program, including sharing the SATA list with air carriers, vetting potential matches identified by air carriers on a 24/7 basis, contacting PSC in the event of a positive match, communicating PSC's decisions to air carriers, and conducting oversight, compliance, and enforcement of SATA and its regulations. All sharing is authorized by and performed within the authorities and scope of the SATA.

● (1540)

Transport Canada identifies a limited number of officials authorized to receive information for exchanges under the Security of Canada Information Sharing Act, and a similar instrument for disclosure is in preparation. Continual efforts, including training, are under way in the department to ensure that the employees are aware of their responsibilities concerning the collection and use of personal information under the Privacy Act.

Sharing information on known threats or to prevent threats from developing is critical. We are committed to doing so in a responsible manner.

I would like to thank you for the opportunity to contribute to your study, and I welcome your questions.

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

We now move to Mr. Rochon, please, for up to 10 minutes.

Mr. Dominic Rochon (Deputy Chief, Policy and Communications, Communications Security Establishment): Thank you and good afternoon, Mr. Chair and members of the committee.

My name is Dominic Rochon, and I am CSE's deputy chief for policy and communications. I'll add that I have the distinction of being CSE's chief privacy officer and the delegated authority under the Access to Information Act and the Privacy Act. It is a pleasure to appear before you today as you continue your study of the Security of Canada Information Sharing Act, otherwise known as SCISA.

[*Translation*]

I've been invited here today to clarify the mandate of the Communications Security Establishment, or CSE, and to provide insights into how CSE protects the privacy of Canadians while engaging in activities that ultimately protect Canadians from foreign threats.

[*English*]

For committee members unfamiliar with CSE and CSE's history, I can tell you that CSE has been in the business of protecting Canadians for over 70 years. Protecting the privacy interests of Canadians and persons in Canada has always been integral to the performance of this mission.

Let me first start by explaining our mandate and the work that CSE does to protect Canada. Our mandate consists of three parts, as defined in the National Defence Act. The first part, referred to as part (a), authorizes CSE "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities".

[*Translation*]

I emphasize "foreign" because CSE only directs its activities at foreign communications. CSE is prohibited by law from directing its activities at Canadians anywhere or at anyone in Canada.

CSE produces valuable intelligence under part (a) of its mandate. For example, CSE provides vital information to protect Canadian troops in Iraq as they contribute to the global coalition to dismantle and defeat Daesh.

In addition, CSE's foreign signals intelligence has also played a vital role in uncovering foreign-based extremists' efforts to attract, radicalize and train individuals to carry out terrorist attacks in Canada and abroad.

● (1545)

[*English*]

The second part of our mandate, known as part (b), authorizes CSE "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada". This part of our mandate authorizes CSE to protect Canada from the growing cyber threat.

Cyber threats used to be the exclusive domain of nation-states. That is not the case anymore, as malicious cyber tools become easier to obtain and the motivations for malicious actors become more diverse. In this rapidly changing threat environment, the services of CSE have become increasingly important.

Across the government, CSE is protecting 700 million connections daily from a user population of about 377,000 people. Every day we block over 100 million malicious attempts to identify vulnerabilities and to penetrate or compromise Government of Canada networks. CSE also shares cyber threat information with Public Safety Canada for further dissemination to the private sector in order to protect the intellectual property of Canadian businesses.

[*Translation*]

Finally, the third part of our mandate, referred to as part (c), authorizes CSE to provide technical and operational assistance to federal law enforcement and security agencies in support of their lawful mandate. This part of the mandate is important for Canada's national security given that CSE possesses unique skills and tools not found in other government departments, particularly in the area of encryption. We know, for example, that terrorists are adaptive and tech-savvy. They use cutting-edge technology, smartphones and messaging applications to communicate. They also use very advanced encryption techniques to avoid detection.

[*English*]

As a result, the threat puzzle that intelligence agencies try to piece together is not always straightforward and requires co-operation to solve—a reality, in fact, highlighted in the preamble of SCISA. Sharing foreign intelligence and cyber threat information with our domestic partners is crucial to a whole-of-government approach to protecting Canadians. It is by sharing intelligence that we warn the Government of Canada about the intentions and capabilities of those beyond our borders who mean us harm.

When doing so, Canadians and persons in Canada cannot be the focus of CSE's activities, and CSE must apply measures to protect the privacy interests of Canadians included in any information being shared. These privacy measures take the form of rendering Canadian identifying information found in the intelligence being shared unintelligible, leaving it to the receiving Government of Canada department or agency to demonstrate a need for that information and the authority to receive it.

[*Translation*]

Although information sharing is essential to protecting Canada's security, CSE recognizes that the sharing of information could potentially touch upon fundamental rights and freedoms, particularly the right to privacy.

I want to stress that, not only is protecting the privacy of Canadians a fundamental part of CSE's organizational culture, it's also enshrined in CSE's mandate. The National Defence Act directs CSE to protect the privacy of Canadians in the use and retention of information.

As such, CSE has multiple policies, structures and processes in place to ensure continued adherence to privacy laws and policies.

[*English*]

These structures include executive control and oversight, operational policies, procedures and compliance measures, an on-site legal team from the Department of Justice, and active ongoing monitoring of internal processes. CSE's privacy framework includes operational policies that set out specific handling processes, retention periods, and sharing guidelines. These policies also allow for the validation, tracking, and auditing of information received.

CSE also provides regular training and testing for staff on our mandate, privacy rules, and compliance. In addition, all of CSE's activities are subject to robust, external, expert review by the independent CSE commissioner. The CSE commissioner, who is usually a supernumerary judge or retired judge of a superior court, has full access to CSE employees and records.

[*Translation*]

I would also like to add that the CSE commissioner has all the power of the commissioner under part II of the Inquiries Act, including the ability to inspect any records held by CSE and the power to subpoena CSE employees to provide information.

The work of the CSE commissioner has had a positive impact on CSE's accountability, transparency and compliance. It has also led to CSE strengthening a number of its policies and practices. The Office of the CSE Commissioner staff regularly interact with CSE employees when conducting reviews. Since 1996, CSE has accepted and implemented all the CSE commissioner's privacy-related recommendations.

● (1550)

[*English*]

Though much of what we do is classified, we are committed to becoming more open and transparent about how we protect Canadians' security and their privacy. We know that openness is crucial to ensuring public trust in what we do, and as the government pursues its overall national security agenda, we continue to be forthcoming about our operations.

With respect to SCISA, you are aware that SCISA lists CSE as an entity that can receive information from another Government of Canada institution. I want to emphasize that SCISA does not supersede or expand CSE's authorities to collect or receive information from our domestic partners. To date, CSE has not relied on SCISA to receive or disclose information. CSE's existing procedures and processes to authorize and manage information sharing meet or exceed those set out in SCISA.

When sharing information, CSE currently relies on authorities under the National Defence Act. Information sharing at CSE is undertaken in accordance with the provisions of the Privacy Act. CSE's established information-sharing arrangements are set out in information-sharing agreements with our domestic security and intelligence partners.

CSE may also receive information from Government of Canada agencies under the National Defence Act and the Privacy Act authorities when relevant to its mandate, although the need to receive information is minimal considering CSE cannot direct its activities against Canadians or persons in Canada.

I should add that the CSE commissioner does conduct an annual review of our information-sharing disclosure activities, and to date he has always found that these activities were done in compliance with the law.

I'll conclude my remarks by stating that I am confident in our ability to fulfill our mandate while safeguarding the privacy of Canadians. My confidence stems from both the rigorous legal and policy frameworks in place to protect the privacy of Canadians, and the professionalism and commitment of CSE's highly skilled workforce.

Thank you for inviting me here today. It would be my pleasure to answer any questions you might have.

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

We now have our last witness of the day, Mr. Burt, for up to 10 minutes, please.

[*Translation*]

Mr. Stephen Burt (Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command, Department of National Defence): Mr. Chair and members of Parliament, thank you very for the invitation to appear here this afternoon.

It's my distinct pleasure to speak to you today about the Security of Canada Information Sharing Act, or SCISA.

[*English*]

Before I speak about SCISA and provide my organization's perspective on it, I'd like to provide some background on the role of my organization because I think it is perhaps not as well known as some of the others.

The chief of defence intelligence, or CDI, is the functional authority for defence intelligence in Canada. The CDI is also the commander of the Canadian Forces intelligence command, or CFINTCOM, an organization with a mandate to provide credible, timely, and integrated defence intelligence capabilities, products, and services to the Canadian Armed Forces, the Department of National Defence, the Government of Canada, and our allies in support of Canada's national security objectives.

Defence intelligence is a key element in the ability of the Government of Canada to make informed decisions on defence issues, national security, and foreign affairs. You can be assured that our intelligence capability is world class, boasting a strong team of dedicated professionals and benefiting from productive relationships with other government departments as well as our partners in the Five Eyes community

CFINTCOM focuses the vast majority of its energy on foreign military threats and support to CAF operations abroad. However, I appreciate the opportunity to discuss domestic information sharing under SCISA and turn now to the subject at hand.

First, please allow me a word concerning our current information-sharing authorities outside of SCISA and the measures we take to protect personal information when it comes into our care. Department of National Defence and the Canadian Armed Forces information-sharing activities are generally conducted under the crown prerogative for National Defence, and we have in place a robust governance regime that includes numerous policies, memoranda of understanding, and other information-sharing arrangements as well as oversight and accountability mechanisms related to the handling of that information.

The majority of the information that National Defence and the CAF share and receive is operational and not personal in nature. This can include information regarding deployed CAF assets, defence intelligence in support of operations such as satellite imagery products, or imagery in support of activities undertaken with foreign defence partners.

[*Translation*]

However, although SCISA could be used to receive and share that type of information, the Crown prerogative also serves as the legal basis to receive and share personal information in the national security field as part of the mandate of the national counter-intelligence program.

Under this program, the Canadian Armed Forces ensure that threats to the security of National Defence and the Canadian Armed Forces in Canada or on deployments abroad are identified, investigated and countered.

● (1555)

[*English*]

In fulfilling this mission, the Canadian Forces national counter-intelligence unit shares and receives information, including personal information, with police and security intelligence agencies under the auspices of the security intelligence liaison program. Activities conducted under this program are authorized by an internal oversight to ensure compliance and consistency with the national counter-intelligence program's mandate, including that the receipt and dissemination of information is carried out in accordance with National Defence and CAF policy and access to information and privacy legislation.

With respect to SCISA, let me first point out that the act does not create or expand the collection mandates of any federal departments or agencies, including those who use the act. Any information that will be shared with listed departments or agencies will have been collected lawfully and in accordance with the collector's mandate. The type and nature of information that is being shared with listed departments and agencies are the same as they have been receiving in the past. Only the sharing has been facilitated.

The main contribution of SCISA is the following. A department that will have collected information in accordance with its mandate, and therefore for a certain purpose, is now able to share that information with another department, even though the recipient will use it for a different purpose, as long as it is in line with its mandate and the information relates to an activity that undermines the security of Canada.

Further, only the head of an institution listed in the schedule or his or her delegate can receive this information. This is a marked departure from normal business where anyone in an organization can be part of a sharing arrangement. Having the head of the institution involved helps ensure that the requirements will be followed.

At the time of our last communication to the Privacy Commissioner in September 2016, DND and the CAF had not shared or received any information under SCISA. Since then, there has been a single instance in which we shared information under the act.

In addition to the authority found under SCISA, other forms of authority, notably the crown prerogative, can and will continue to be used by DND and the CAF. Note that SCISA does not in any way limit or affect the information-sharing authorities provided under the prerogative. For clarity, this is stated in the act itself in section 8. SCISA does, however, assist other government organizations in sharing with DND and the CAF. For this reason, we remain supportive of SCISA and wish to remain on the list of recipient organizations in schedule 3 of the act.

Should a government institution wish to share information with DND or the CAF under SCISA, we will adhere to the following process for receipt. Discussions with the providing institution will take place to establish whether the information is relevant and within our mandate to receive and whether it relates to activities that undermine the security of Canada. Once received, the information will be examined to determine which internal organizations in DND and CAF should have access to it.

Any information received under SCISA will be assessed in accordance with the requirements of the Privacy Act, the Access to Information Act, and all associated Treasury Board Secretariat policy and direction.

[*Translation*]

This concludes my presentation.

Thank you for your attention, and I look forward to answering your questions.

[*English*]

The Chair: We are going to start the seven-minute rounds of questions with Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thanks for a very informative group of submissions. Mr. Roussel, your submission was first, and it's interesting that it relates in a more direct way to the average Canadian than the other presentations, but we'll get to them all.

What's your history with the department? How long have you been doing what you do?

Mr. Donald Roussel: I'm a bit of an anomaly in Ottawa. Next week I will have been with Transport Canada for 29 years. I started as a field inspector and moved up to DG of marine safety and security, and I've been the associate ADM in the safety and security group since 2014.

Mr. Bob Bratina: It's safe to say you have a pretty good handle on it.

Mr. Donald Roussel: Yes, I know a bit about the business.

Mr. Bob Bratina: Thank you. I assumed so but I wanted to hear your credentials.

The first thing that strikes me when we listen to all the submissions is the lack of use of SCISA. You state that your department has yet to use SCISA's provisions, so what do you see as the role of SCISA?

● (1600)

Mr. Donald Roussel: First, it is a fairly young piece of legislation, 2015. As a young piece of legislation, we need to learn the tools. Mr. Burt commented that this is like a tool box. When we requested to be in the annex, the review of all of our legislation demonstrated that we had some limitations on what we could ask for or share.

For example, under the Aeronautics Act, we could only share a series of elements on the passengers and how they wanted to travel, which would not necessarily be broad enough to help us mitigate the risk. We needed a broader tool. In our analysis, we may have a screwdriver and a hammer but we needed the whole tool box to be able to do a better job.

The other element, which is significantly troublesome, is that if we have information and we know information is out there, not being able to ask the intelligence gatherers for that information is not very useful. We have to be able to ask specifically for what we're looking for and what information they could have gathered to share with us to be able to do our work more broadly.

Mr. Bob Bratina: You've had this history and you must have.... I'm not asking you to explain any incidents that occurred, but incidents have occurred in the past, which I gather from your presentation were dealt with quickly and reliably by the department prior to the new act.

Is that fair to say?

Mr. Donald Roussel: They were dealt with, but with a significant amount of complexity and legal challenges that made the work a lot more complicated. When we are in security measures, time is of the essence. How fast can we receive the information to make the proper analysis and then convey the appropriate actions?

When we have a cumbersome suite of legislation that we have to navigate, it makes our work fairly difficult. SCISA does help us to be able to move faster. We have not used it yet but we know potentially we could use it.

Mr. Bob Bratina: Mr. Rochon, in collecting information, how much information originates with anonymous tips? Does your organization get little brown envelopes or mystery calls in the night?

Mr. Dominic Rochon: That's an interesting question. I wasn't expecting that. To be fair, I don't know specifically what the answer to that question would be. I would say that, no, we don't get anonymous tips through brown envelopes and the like. We do have, obviously, long-standing partnerships with our security and intelligence domestic partners. Obviously, we work closely with RCMP and CSIS, which both, I would say, understand our mandate, which is very much foreign, particularly when it comes to part (a) of our mandate. When you're speaking about foreign signals intelligence, if they perceive they have a tip or a lead on a foreign threat, there could be a sharing of information in that context. I would say that each department, each agency, has a mandate to already share that, and we obviously have a mandate to receive that.

The same applies in part (b) of our mandate when it comes to protecting systems of importance to the Government of Canada. If there's relevant cyber information that we need to receive in order to be able to protect systems of importance, those tips can come.

Going back to the original question that you asked Mr. Roussel, about the fact that we haven't used the act to date, I think that speaks more to the fact that there are possibly departments and agencies out there in the broader security intelligence field, or maybe even beyond, within the Government of Canada, that don't necessarily understand what our mandate is. I think SCISA will educate departments and agencies specifically on the 17 departments and agencies that are listed as recipient agencies. As that education becomes deeper, I think you'll see people starting to see the benefits of being able to say, “Well, actually, here's an opportunity where I would be able to share because I understand their mandate better.” That might not be happening now.

Again, in our particular case, and as I mentioned in my opening remarks, as it pertains to foreign signals intelligence, because our main focus is foreign, the use of SCISA might not be that predominant, but it remains to be seen.

● (1605)

Mr. Bob Bratina: I was getting at reliability in terms of receiving information and the safeguards so that the information is reliable, and so on.

What you're telling me is that a group like the RCMP will send you something and you would be sure that they wouldn't just call you up on an inconsequential matter, that it would have been vetted carefully.

Mr. Dominic Rochon: I'll use foreign signals intelligence as an example and I'll leave part (b) aside for the moment.

What they understand is that we collect foreign signals intelligence in accordance with intelligence priorities that are set by cabinet. They understand what those intelligence priorities are. They understand that we're limited within our mandate to direct our activities outside of Canada at foreigners. As a result, if they have something in that context, they'll obviously say, “Here's something that might lead to the collection of foreign intelligence that we're interested in. Therefore you have a mandate to collect it, ultimately assess it, and disseminate that across governments for the benefit of the intelligence community.” It's understood.

Mr. Bob Bratina: I see.

The Chair: Thank you, Mr. Bratina. We're already at eight minutes.

Mr. Jeneroux, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you.

Thank you for attending the committee today, and thanks to your staff for preparing your remarks as well.

I would like to go back to when SCISA was created and some of the debate surrounding the creation of SCISA. There were many concerned at the time that the new information-sharing provisions provided to our intelligence organizations were too broad and were not sufficiently accompanied by the appropriate oversight mechanisms. We have heard some come into this committee and testify more on a hypothetical “this could be” or “that could be”.

I have a simple question for all of you at the table. Since SCISA has come into force, have you seen an abuse in the new information-sharing powers or a misuse in them?

I'll start with Mr. Burt.

Mr. Stephen Burt: No, absolutely not.

Mr. Dominic Rochon: I would echo that no.

Mr. Matt Jeneroux: Then what do you do in your organizations to ensure that the privacy of Canadians remains paramount and is protected?

Mr. Burt.

Mr. Stephen Burt: What do we do to ensure that the privacy of Canadians remains paramount? Like Mr. Rochon, most of our work, as I said, is directed overseas, and it's part of Canadian operations abroad.

Where we do deal with Canadians is on our counter-intelligence program, but there it really has to be restricted to something that directly affects the security of National Defence or the CAF, so it has to deal with our employees, Canadian Armed Forces personnel, our property assets, and whatnot.

In circumstances where there is a nexus to that, we generally work with partners in law enforcement and national security. The mandate of our counter-intelligence unit is very focused. It can investigate, but it is not a law enforcement agency in its own right, so generally, those circumstances are ones where we are working in co-operation with law enforcement agencies or other partners, and their rules apply.

As you said at the beginning, SCISA doesn't actually change our ability to collect information. It doesn't change the mandate under which we can use that information. All it does is provide a very useful framework to move that information between departments when it seems like that might be necessary. The protections in place are all the usual protections in terms of the charter, the Criminal Code, and the protections that are in place within the various mandates of organizations like the RCMP, CSIS, and whatnot.

Mr. Dominic Rochon: We actually have a foundational operational policy, and that policy is entitled “Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities”. I'm responsible for operational policy within our organization, and that's the foundational policy. All other policies stem from that. This shows you the importance we attach to the privacy of Canadians.

We're required by law to implement measures to protect the privacy of Canadians. That is stipulated in the National Defence Act. We have ministerial directives and ministerial authorizations that then further emphasize that. We have training in place for anyone who would be accessing information within our systems, etc. This is extensive training that we don't just produce for people who work within our organization. We actually go to partner organizations and provide them with training to make sure that they understand exactly what our mandates are, etc.

Beyond that, we have compliance regimes. We have internal oversight. We have our own audit and evaluation shop that reviews our information sharing and privacy practices. As I mentioned in my opening remarks, we have our own legal unit that reviews these practices, as well. Provided by the Department of Justice, they're there to provide us with legal advice.

Then we also have external review where we have.... I think you've had our commissioner appear before you here as a witness. We have independent and expert oversight with regard to our activities, and as I mentioned in my opening remarks, our commissioner produces an annual report that looks at our privacy practices.

● (1610)

The Chair: Is that everything, Mr. Rochon? Okay.

Madam Paquet.

Ms. Marie-France Paquet (Director General, Intermodal Surface, Security and Emergency Preparedness, Safety and Security Group, Department of Transport): Thank you very much.

To my colleagues here at Transport Canada, of course, privacy is paramount, and I will give you one example. On top of all the training we provide to our people, we run different programs within the safety and security group and with Transport Canada writ large. Within the transportation security clearance program, we receive applications from individual workers who desire to work in restricted areas within ports and airports, for example. When they sign their application, they sign a consent.

Privacy is, of course, paramount in how we share the information, but when individuals willingly come with their applications and consent, we will share the information with, let's say, the RCMP for the benefit of background checks. That's just an example from within our own programs of how individuals have to consent. It's the same thing in the air cargo security program. Businesses that wish to be part of the program have to consent to share some of the information with, let's say, the CBSA, for example.

Mr. Matt Jeneroux: To pick up on one point that you said, Mr. Rochon, you help support or train other organizations...?

Mr. Dominic Rochon: Yes. Because we have long-standing practices of information sharing with, for example, the RCMP and CSIS, we offer people who are experts in our operational policies to go and meet with people within their shops.

We have protocols set up, so exchange of information just doesn't happen from any employee to another employee. There are strict protocols in terms of how that information is shared. As for the people who are involved in that sharing, there's an exchange and training process involved where we'll go and give sessions to explain to people exactly what the handling process is, and in some cases, there may even be testing.

Mr. Matt Jeneroux: Fair enough.

It looks like I just have 45 seconds left. I'll leave it with one final confirmation. In all of your opinions, there has been no abuse, and there is proper oversight when it comes to SCISA.

That was a yes from all of them.

Thank you, Mr. Chair.

The Chair: You're welcome, Mr. Jeneroux.

[*Translation*]

Mr. Dusseault, you have the floor and you have seven minutes.

Mr. Pierre-Luc Dusseault (Sherbrooke, NDP): Thank you, Mr. Chair.

I also want to thank the witnesses for being here today.

I want to go back to the issue regarding the usefulness of the Transport Canada legislation. It was said that this legislation hasn't been used yet because it's very recent. If I understood correctly, Mr. Rochon said that the legislation wasn't necessarily useful. My question is for him and for the Department of National Defence representative.

Mr. Rochon, you said that your enabling legislation already allows you to share information. You also said that the privacy legislation provides a certain framework for sharing information. If I understood correctly, you don't see a real use for the Security of Canada Information Sharing Act.

Mr. Dominic Rochon: I wouldn't necessarily draw that conclusion. I think Mr. Roussel mentioned that the legislation is still recent. Of course, we haven't used the legislation yet. It's difficult for me to tell you, after a year, if the legislation is very useful. However, I think it could be useful. I told Mr. Bratina earlier that we still aren't sure that people understand our mandate. There may be opportunities later for other departments to gain a better understanding of the two parts of our mandate and maybe to find situations where sharing information under SCISA would be beneficial with regard to our mandate and the mandate of other departments.

● (1615)

Mr. Pierre-Luc Dusseault: Do you share information with different departments and agencies that isn't necessarily related to Canadians, but to international threats?

[*English*]

Mr. Dominic Rochon: I'll just break into English, if you'll allow me, because I'm a bit more familiar with some of the terminology and how we do things.

In terms of our disclosure of information, we have a clear mandate —in part (a) of our mandate—to collect foreign signals intelligence. We do that and we don't just do it for our own purposes. We obviously do it for Government of Canada departments and agencies. As we collect information, we assess that information and disseminate it to people who are authorized and need to receive it within the departments and agencies.

There is no need for SCISA in that instance. We're going to be continuing that practice, which we've always had and which it is clear in our mandate that we can do, and it's clear that other departments and agencies have people who are in need of that information in order to receive foreign intelligence. For our disclosure, I don't foresee any usefulness, particularly. However, for people to disclose information to us—whether to help in that foreign intelligence mandate or indeed in part (b) of our mandate—I foresee that there may be some usefulness. I can't tell you for sure. I certainly wouldn't say that it's a foregone conclusion that we would never use it. I think it's too early.

[*Translation*]

Mr. Pierre-Luc Dusseault: My next question is for you three and it concerns the retention of information.

CSIS was criticized for retaining information on Canadians for ten years. What are your policies for the retention of information on Canadians?

Mr. Rochon, this issue may be less applicable to you since your mandate doesn't necessarily involve information on Canadians. However, this issue may concern Transport Canada.

How long do you retain information before destroying it?

Ms. Marie-France Paquet: Let's first go back to the aviation transportation security clearance program.

Every year, we have a data bank of approximately 20,000 applications. These are people who have security clearances to work in the restricted areas of ports and airports. Once the clearance has expired, we keep it for two years. We then dispose of it in keeping with the normal procedures. We keep it for two years in case we need to verify things and we then dispose of the information.

Mr. Pierre-Luc Dusseault: Okay. We're talking about information on people who have clearance to work in secure areas.

Ms. Marie-France Paquet: Yes.

Mr. Pierre-Luc Dusseault: Let's take a broader look at the management of the Security of Canada Information Sharing Act. I want to know whether a policy on the retention of information is applied in frameworks other than this one.

Is this the only context in which you have information related to the security of Canada?

Mr. Donald Roussel: The Department of Transport doesn't collect information, but uses the information of other agencies. When we have information on individuals in particular, the policy mentioned by Ms. Paquet applies.

Mr. Pierre-Luc Dusseault: Okay.

Mr. Burt, do you have anything to add?

Mr. Stephen Burt: We also don't collect information on Canadians. When we receive information of that nature, it's usually part of a judicial inquiry conducted by the RCMP, for example, that concerns a member of the Canadian Armed Forces or a National Defence employee. In these cases, we determine what we can do and how we can be useful to the inquiry. The fact remains that all this is managed by that organization's legislation and regulations. On our own, we don't have a role in collecting information on Canadians.

● (1620)

Mr. Pierre-Luc Dusseault: Okay.

Mr. Rochon, when you have information in your possession that shows a potential threat to the security of Canada, do you conduct a type of verification to ensure the information is reliable and of good quality before disseminating it to Canadian agencies?

Mr. Dominic Rochon: It's a complicated question.

[*English*]

In terms of the information we collect in our foreign signals intelligence mandate, we need to make sure that it meets with an intelligence priority as set by the government, that it pertains to international security and defence. That's sort of our staple.

We also have to, obviously, make sure that it's directed at non-Canadians outside of the country. Those are the staples in terms of what it is that we're collecting and the threshold that we're measuring.

From there, we assess that information and then we disseminate it. The litmus test is that our clients in the RCMP, CSIS, and other departments and agencies will then provide feedback to let us know whether that information was useful.

As far as foreign intelligence is concerned, we don't have any investigatory powers. We don't have any powers of arrest. We just provide foreign intelligence, and all of our foreign intelligence is caveated with the fact that it stems from our collection capabilities and what we were able to collect. We're ultimately, in part (a) of our mandate, not assessing. There are other parts of the government that will take our information, fuse it with other intelligence from other parts of the security intelligence apparatus, and then ultimately come up with the assessment.

The Chair: Thank you very much, Mr. Dusseault. We're well over time, but I appreciate that.

For the last of our seven-minute round, we'll go to Mr. Saini, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much for being here today. I want to pick up on my colleague Mr. Dusseault's point about retention of information. I think this is a technical question. This may be applicable to some of you and not to some of you.

You might receive information that might be relevant, that might be actionable, and you might receive information that might be redundant or might not be used. Madame Paquet said they keep it for two years. When you retain it, what is the protocol for keeping that information? What is the protocol if that information it is not actionable, is not relevant? How do you dispose of that information?

Mr. Stephen Burt: I can take a crack at that.

Much as I think Mr. Rochon will probably tell you, in the context of our operations abroad, the issue of holding onto information is a bit of a different set of questions. We're not dealing with information that is necessarily touching on individuals in the same way. Information can be databased for quite a long time, because you want your analysts to be able to go back and cross-check things and figure out what has happened in the past on certain files.

There are not the same kinds of timelines that there would be when you're dealing with private information, whether it's of staff or people who you're regulating, or if you were dealing with legal cases or national security investigations regarding Canadians where there are privacy concerns. For the vast majority of what we collect in terms of operational information, there is no formal process around how long you can keep it. The goal is to database it usefully so that you have good information to look back upon.

Mr. Dominic Rochon: I would agree with that.

It's very similar in terms of our foreign signals intelligence activities as well as cyber-threat activities. If we've collected information that's useful and there's an ongoing threat, we're going to continue to use that information. Obviously, we're not in the business of collecting information about Canadians. Not to get too technical, but we do come into contact with information. We may collect it incidentally. We have very strict rules that we are to delete that information immediately unless it has value with regard to a threat to Canada. If we can show that it does have that value, and there's an interest when it comes to the security and defence of Canada, then we will keep it and we'll report on it. However, we still put measures in place to protect that information within our systems.

Specifically, as it pertains to retention periods, your question is more about how long we retain things. We have retention periods for most of the collection of information that we have. We have ministerial directives that impose those retention periods. We follow them and they are reviewed by our commissioner to make sure that we adhere to them. That's how I would couch it.

● (1625)

Mr. Raj Saini: Do you have anything to add?

Ms. Marie-France Paquet: I'll just add that on the aviation security side, we get information on the advance passenger manifest, as we call it. We keep that information for only seven days.

Mr. Raj Saini: Then you destroy it after exactly seven days.

I'm sure some of you have also written sharing agreements with foreign governments and foreign entities. Do you deal with any kind of information that involves the privacy of Canadians?

Mr. Stephen Burt: It's a bit like what was just said. Occasionally, you would come across that information incidentally. It does happen on deployed operations that you would come across things that do or may impact on Canadians. When those cases occur, we hand them over to the appropriate Canadian authorities. We would do that regardless of SCISA.

SCISA provides a good framework for doing it. In fact, the one case that we have had involved exactly that kind of information that came from a foreign partner and was relevant to CSIS's mandate.

Mr. Raj Saini: You don't send Canadian information abroad. It comes to you.

Mr. Stephen Burt: We don't collect Canadian information intentionally.

Mr. Dominic Rochon: We don't collect the Canadian information, and we wouldn't be sending specifically private communications about Canadians. That being said, we're part of a Five Eyes, cryptologic, long-standing arrangement. We have a long-standing agreement that we don't conduct activities on our citizens, and we don't conduct activities on their citizens and vice versa. It's a long-standing protocol, and it has served us in good stead for about 70 years now. That being said, when you say “information”, it gets a little bit more complex in terms of what it is that we do because there's the whole issue of metadata.

Nevertheless, if there's an exchange of information that may or could involve a Canadian, we have measures in place that protect that information. Therefore, we render that information unintelligible, as I mentioned in my opening remarks. If it does get passed on, any information about a Canadian would be rendered unintelligible, so they wouldn't be able to see it. If they wanted to see it, they would have to come back and explain to us that they have an imminent threat and ask for the personal information. Then we would make an assessment as to whether or not we could share it.

Mr. Raj Saini: The other question I had is, do you ever use warrants or anything to obtain any kind of information? Maybe specifically not you, because you deal with foreign information, but do any of your organizations use warrants?

Mr. Stephen Burt: My organization does not use warrants. Occasionally, if we are operating in support of a domestic law enforcement agency, we'll be authorized under a warrant by them, and all the rules of that warrant will apply. That's when we're working in support of them, and effectively we're part of their organization for those purposes.

Mr. Dominic Rochon: That's exactly the same.

Part (c) of our mandate essentially gives us—

Mr. Raj Saini: You don't use warrants on your own. You use it as part of another thing.

Mr. Dominic Rochon: Correct.

Mr. Donald Roussel: For us, it's not within that context that we will use a warrant. It will be under compliance and enforcement, under the safety regulations in particular where we're seeking information. It's not necessarily on individuals but on the operations of a company, the bookkeeping and so forth. It's not under the security mandate.

Mr. Raj Saini: Thank you very much.

The Chair: Okay. Thank you very much, Mr. Saini.

We now move to our five-minute round, colleagues. We'll go to Mr. Kelly, please.

Mr. Pat Kelly: Thank you, Mr. Chair.

On Tuesday, we had witnesses who made claims that would indeed be very disturbing if the substance of these claims were true. I'm going to ask you to confirm whether some of the things that were said about threats to the privacy of Canadians, and specifically about SCISA, are correct or not.

A concern was raised about bulk data collection and bulk data sharing between listed recipients, in contrast to a nuanced or targeted collection and sharing approach. I'd like you to comment on what bulk data collection and sharing means, and whether Canadian agencies and organizations do it.

Specifically, it was stated on Tuesday that, under SCISA, there's no limit on data sharing and no oversight. It was characterized as a blank cheque for Canada's national security agencies. It was stated also, as an example, that CSIS could go to the RCMP and ask for all the information it collected under warrants, but once in CSIS's hands, the information would not be subject to the conditions set out in the warrant. It was claimed that Canada hoovers up as much information about innocent people as possible through bulk data collection instead of a targeted approach.

These were some of things we heard in Tuesday's committee meeting. I would like each of you to comment on those claims, and whether these are legitimate concerns about privacy under SCISA.

● (1630)

Mr. Stephen Burt: I'm happy to go first on that.

It's clearly stated in the legislation that SCISA does not affect collection mandates whatsoever, so there is no net effect of SCISA on collection of any kind, bulk or otherwise.

Mr. Pat Kelly: Okay. These appear to be gross exaggerations or mischaracterizations of the powers under SCISA.

Mr. Stephen Burt: To simply state what's in the act, in terms of sharing I would say what SCISA brings to the table is a clear framework with a couple of tests in it for whether or not the information can be shared. It's a very short piece of legislation. It's written very clearly, and the tests, I think, are laid out with some precision in terms of the wording.

It facilitates sharing, certainly. That was the intent of the act.

Mr. Pat Kelly: Okay.

Mr. Rochon.

Mr. Dominic Rochon: I don't really have much to add. Mr. Burt covered exactly the point.

We collect information. We certainly don't then turn around, whether it be under our authorities or under these new SCISA authorities, and share it in bulk.

The information that we collect, we then assess. That assessed information then gets disseminated through end-product reports to client departments when it comes to our foreign signals intelligence. There are processes in place that are measured and proportionate in terms of understanding exactly how information should be shared.

I have no reason to believe that SCISA somehow now facilitates bulk sharing. It doesn't create any new authorities, as Mr. Burt pointed out.

Mr. Stephen Burt: If I could add one more point....

Mr. Pat Kelly: Please do.

Mr. Stephen Burt: The need to know, determining who you actually want to share sensitive information with because of the risk to that information, is still a very real principle in the intelligence community.

Mr. Pat Kelly: Thank you.

Mr. Donald Roussel: At Transport Canada we do not collect information. We only use it. We use the information that we receive or request about specific individuals or organizations, or for other needs. It's very limited. We do not seek bulk data. Our mandate is very specific.

Mr. Pat Kelly: Thank you.

On the one hand, one of the criticisms offered has been this fear of increased and wholesale dissemination of information between departments, and indeed, between governments. I'm struck also by hearing today—not for the first time—about departments that make fairly limited use of SCISA.

Today, I've heard testimony that SCISA is not a tool that you turn to very often, or indeed at all, yet you can foresee its possible necessity or benefit. An organization may need SCISA to obtain information that would be in the interest of Canadian security for an agency to possess. Am I correctly characterizing roughly how you see SCISA?

Mr. Stephen Burt: I think I would agree in general terms with that. I think that the legislation was passed in response to a perceived need for a framework to do exactly the kind of sharing that we had trouble with from time to time previously. By providing a framework for that sharing, it is a useful tool. It has not yet been much used, but the potential....

I think all of us have probably been in situations where we were in receipt of information that we thought might be useful to someone, but we weren't sure what our authorities were to actually pass it on. This provides, as I said earlier, a couple of simple tests so you don't have to move heaven and earth to actually figure out how you can make that determination.

● (1635)

Mr. Dominic Rochon: Maybe I'll just add really quickly that it also provides an opportunity to provide better understanding, better consistency, and better discipline in terms of how that information is being shared across 17 departments, as opposed to the way that we've been doing it.

[*Translation*]

The Chair: Mr. Massé, you have the floor and you have five minutes.

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

I want to welcome the witnesses and thank them for participating in the committee's work. It's very much appreciated.

Mr. Rochon, in your presentation, you said the following:

[*English*]

"we collect foreign signals".

[*Translation*]

In French, you said that you acquire and use information from the global information infrastructure.

I want you to explain what this means. Are you talking about cellular signals, or information from texts or emails? Explain to me what these signals are.

Mr. Dominic Rochon: It's everything you mentioned.

[*English*]

We collect foreign signals intelligence from the global information infrastructure. The global information infrastructure can be the Internet. Traditionally, going back to after the First World War, it was radio waves. I, unfortunately, can't get into all of our capabilities in terms of what it is that we're collecting, but in simple terms, the things that you were highlighting, whether it be.... Telecommunications data, essentially, is covered.

[*Translation*]

Mr. Rémi Massé: Thank you.

What mechanisms do you use to manage the information? What mechanisms help you conduct research to identify what is relevant in the data you collect?

Mr. Dominic Rochon: It's very complicated. I'll give you the response in English that we usually provide.

[*English*]

We use the analysis of metadata, essentially. That, of course, is something that is very much a debate, and I think, for the most part, is misunderstood in terms of the need for metadata. Metadata information, particularly telecommunications metadata, allows us to be able to tailor our collection capabilities, to be able to understand and go after the information that we actually need.

First and foremost, what are our guidelines in terms of what we're looking for? The Government of Canada, cabinet, sets the intelligence priorities. Intelligence priorities are obviously classified, but it's not hard to understand. There is counterterrorism, for example, and when we're supporting military operations, we need to go after information pertaining to that.

The Internet, unfortunately, doesn't have a place where all terrorists go, so we need to understand, as all this information is intermingled on the global information infrastructure, how many pieces of information are being transmitted. We need to analyze metadata. Metadata can be an IP address or an email address, but it can also be when a signal passes from a cell tower to a server to somewhere else. It's through the analysis of metadata that we can then hone our activities and be surgical about what it is that we want to go after, because, as you can imagine, the Internet is incredibly vast. If you actually pause for a moment and try to understand what is actually happening on the global information infrastructure in a minute—how many YouTube videos are uploaded, how many people are tweeting, how many people are using Skype, or texting, or using social media and all of the things that are happening there—it is incredibly complex and incredibly vast. You need to be surgical if you're going to go after what it is that you're looking for.

Mr. Rémi Massé: Maybe I should clarify my question. Is it fair to say that you have some sort of search engine that allows you to type different words so that you can target the specific information you're looking for? For the normal Canadian, we use Google. Do you have a search engine like Google that allows you to dig and find out what you're looking for?

Mr. Dominic Rochon: Unfortunately, I'm limited in what it is I can say to describe exactly how we do what we do. That would be a gross overgeneralization of how we go about it. It is infinitely more complex than that.

[*Translation*]

Mr. Rémi Massé: You also mentioned that you occasionally receive information on Canadians, but unintentionally.

How often does this happen and how much of that type of information do you receive?

● (1640)

[*English*]

Mr. Dominic Rochon: What I can say, because it's been reported on by our commissioner in the last three years, is this. I'll use a private communication because that's something that's definitive in terms of what a private comm involving a Canadian is. One end is a Canadian. It's a communication that either originates or ends in Canada. That's a private communication.

When we come across a private communication, incidentally—and maybe I'll give you a quick example. I'm not trying to take up your time. If we're targeting bad guy X in country Y, we can't control what bad buy X in country Y is going to do. He might pick up the phone and call you. He decides to call you, and we're actually monitoring and collecting his information. When he does that, he might be calling you to share a recipe for soup, or he might be calling you to say, "Bombing the Parliament Building tomorrow is a go." In the first example, if we come across a private communication and it has no relevance to international affairs, security, and defence, we delete it immediately. We mark that and we keep track of that marking, and our commissioner reviews and makes sure that we have deleted it and that there is no trace of it in our systems. In the second case, we keep it.

To your question in terms of volume, how many private comms did we keep over the course of a year? The first time that number was published was three years ago and that number was 66. Two years ago that number was 16, I believe, and last year that number was 340. You might be wondering if those are big numbers or small numbers.

As I was explaining to you earlier, just for yourself, for example, how many emails, phone calls, social media.... How many times do you actually use a private comm in a day? Multiply that by 365. Multiply that by the population in Canada, say 39 million, and you'll get an idea that there are billions and billions of private comms transmitting every single year. Of those billions and billions, the numbers in the last three years have been 66, 16, and 340 that we have kept for national security reasons. Hopefully, that gives you an idea of the volume.

The Chair: Thank you very much, Mr. Massé. We are at seven minutes, but that was a great line of questioning and response.

Mr. Kelly, you have the floor again for five minutes.

Mr. Pat Kelly: Thank you. Depending on the length of the answers, I may have Mr. Jeneroux jump in too.

Of the past witnesses that we've heard from, the subject of Maher Arar came up several times as an example of the dangers of poor information sharing practices between governments, and rightly so. In addition, we have had decades of investigation and inquiry into the Air India bombing, and in other countries, other investigations into catastrophic acts of terrorism. These have pointed to inadequate sharing practices between enforcement and intelligence organizations and the failure of prevention through inadequate sharing practices.

I'd like any of our witnesses to comment on the balance that the current system strikes between protecting privacy and protecting Canadians through appropriate information sharing.

Mr. Stephen Burt: Without touching on the specific cases you've cited, which I'm in no position to comment on in any case, there is always a tension in these issues in terms of what to share and what not to share. The intelligence business, fundamentally, gets some of the questions that others have asked earlier, particularly when you're dealing, as National Defence does, with all sources of information: signint, humint, imagery intelligence, etc. The issue of which source of information will give you the best of what you're looking for, and which is most credible and reliable in order to do what you think you need to do, operationally, is the constant struggle. Shifting through the volume of information, finding the pieces that are credible and reliable that pertain to the operation in which you are currently engaged is a huge amount of work.

There have been many cases, you cite, where not sufficient information was shared, be it because it wasn't found in time or because we were concerned about whether or not we could share it legitimately. There have been cases where information that unfortunately was not credible or reliable was shared and led to mistakes being made, operationally, of one kind or another.

Mistakes will continue to be made in this business. It's a difficult business, but having a clear framework within which you can make decisions around sharing is a benefit to the system.

● (1645)

Mr. Pat Kelly: How would you characterize SCISA, though? Does it give you the right balance? Do you think you have the right tools right now to be as good as you can be at not making mistakes?

Mr. Stephen Burt: I think SCISA is too new and too untested at the moment to determine whether or not it strikes the right balance. We may find as time goes by, if we keep the current formulation of the act, which is a decision for government and for Parliament, that there are tweaks that need to be made to shift the balance in one direction or another. At the moment, it strikes me that it is a much better tool than we had without it.

Mr. Pat Kelly: You're not ruling out then even that SCISA does not facilitate as much sharing as you might need?

Mr. Stephen Burt: As some of my colleagues have said, we have powers to share already. What SCISA does is clarify the rules and provide a framework in which you can do the sharing and track it, which was not the case previously.

Mr. Dominic Rochon: Unfortunately, I don't have much to add. I think Mr. Burt was very eloquent in the way he covered those points.

Again, we're in a tough position, not having used the act, either to disclose or receive anything. It's hard for us then to be able to give you an educated opinion as to whether or not we've effectively added this tool to the tool box and that it somehow has struck a better balance than what existed or a worse balance than what existed. The tension continues to exist, as Mr. Burt so eloquently put it. This is a new element that, in my personal opinion, looks like a framework that will facilitate a better understanding of each other's mandates, and possibly then, a better discipline can be put toward the sharing of the information. However, the proof will be over time as it's being used as to whether or not that balance is struck.

Mr. Pat Kelly: Some critics are calling for its immediate repeal. Would that be unwise in your opinion?

Mr. Dominic Rochon: It's hard to say. It's too soon to tell.

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

We now move on to Mr. Long for five minutes, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair, and thank you to our witnesses today.

I'm going to go from left to right and start with you, Mr. Burt. Maybe you could give a yes or no or a short follow-up. Do you think SCISA is required for the protection of our national security?

Mr. Stephen Burt: SCISA provides a useful framework for determining whether or not information should be shared in the protection of our national security. It potentially could make decision-making on sharing or not sharing faster.

Mr. Dominic Rochon: I would agree with him and add that it is more efficient.

Mr. Donald Roussel: Yes, and we have concrete examples from the past that we can give to the committee on how it would have helped us in the past on fairly complex issues.

Mr. Wayne Long: Mr. Burt, in your opinion, do you feel there was a compelling explanation provided as to why previous laws were inadequate? In other words, do you think there was a strong enough explanation given to change and not just stay with what we had?

Mr. Stephen Burt: When the legislation was going through?

Mr. Wayne Long: Yes.

Mr. Stephen Burt To be honest, I wasn't in a business that would have had me paying attention to it when the legislation was going through. But I have certainly lived situations in the past, as Monsieur Roussel said, where I can imagine that this legislation, had it existed, would have been useful.

Mr. Wayne Long: Okay.

Mr. Roussel.

Mr. Donald Roussel: Yes, and even worse than that, some of our legislation prohibited, prior to that, some exchange of information.

● (1650)

Mr. Dominic Rochon: I'll echo what we've been saying, but maybe I'll take a different tack. I think National Defence, Foreign Affairs, or Global Affairs Canada, all had authority to disclose information, which means sharing information. All of those authorities would not necessarily be clear to each other in terms of the security intelligence community, or even beyond that, in terms of understanding each other's disclosure.

I'll use FINTRAC as an example. They are explicitly allowed in their legislation to be able to disclose information. It's very clear in that legislation. It's perhaps not so clear in terms of understanding the crown prerogative that Mr. Burt brought up in his opening remarks. SCISA provides a better framework, I think, to be able to understand each other's mandates and provide a mechanism whereby the sharing of information with the 17 recipient identified entities would be clearer.

That's the way I would couch it.

Mr. Wayne Long: As a last question, would you agree that SCISA has compounded a crisis of public confidence about surveillance in Canada? We live in a world where sometimes perception becomes reality. Would you agree with that?

Mr. Stephen Burt: That it has compounded a crisis...?

Mr. Wayne Long: About surveillance, about privacy in Canada.

Mr. Stephen Burt: I can't really express an opinion on that. I would hesitate to characterize the current concern with surveillance in Canada as a crisis. I think some people are concerned about some things.

I would say, just to pick up on Monsieur Rochon's last point, that one of the nice things about SCISA is that now, having shared a piece of information under SCISA, I have a mechanism to then go back to the organization I shared it with and say, “Hey, what did you do with that piece of information we shared?” It's being tracked, in a way. Previously, under the crown prerogative, we probably would have shared information regardless, and there would have been less of a process around it.

I think the act is very clear in what it lays out in terms of what that process is. I think if people have concerns, they can probably be addressed in the reading of the act.

Mr. Wayne Long: Okay.

Mr. Rochon.

Mr. Dominic Rochon: I would simply answer “no” to your question, because I don't think so.

Mr. Wayne Long: Mr. Roussel.

Mr. Donald Roussel: No.

Mr. Wayne Long: You don't think there's a perception out there of a crisis in public confidence at all.

Mr. Donald Roussel: I don't see a crisis. We don't feel it in our department.

Mr. Wayne Long: Okay. Thank you.

Thank you, Chair.

The Chair: Thank you, Mr. Long.

I'll just take a moment of the committee's time here to advise members, as we have some new members here. As your chair, I don't like to tell members of Parliament what they can or can't do, but I will read something out of O'Brien and Bosc. We have some department officials here, and I asked the clerk to find the paragraphs with regard to the line of questioning that was happening.

I'm passing no judgment on this. I just want members to be aware of what it says:

> There are no specific rules governing the nature of questions which may be put to witnesses appearing before committees

—which is fine—

> beyond the general requirement of relevance to the issue before the committee.

So it should be relevant and so on. It goes on to state that “Witnesses must answer all questions”, and the paragraph goes on to talk about compelling a witness to answer a question. However, it also moves on to talk about department officials:

> Particular attention is paid to the questioning of public servants. The obligation of a witness to answer all questions put by the committee must be balanced against the role that public servants play in providing confidential advice to their Ministers. The role of the public servant has traditionally been viewed in relation to the implementation and administration of government policy, rather than the determination of what that policy should be. Consequently, public servants have been excused from commenting on the policy decisions made by the government.

Some of the questions that I'm hearing from some members at the table today might be at that point. I'm just urging members to stick to more technical questions in regard to the implementation of the policy to find the facts and tease out the information. We'll have ministers who can come and talk more broadly about whether or not the policy is actually fair. I don't think we should be putting our public servants in that kind of a quandary, if we can help it, but I will be fair. If the public servants wish to answer those questions, they are more than able to. I will not intervene.

I'm just leaving that there for the edification of the committee members.

Mr. Wayne Long: I thought, Chair, they did answer the questions, and I appreciated their answers. Thank you.

The Chair: Okay. I just wanted to bring that up for information. I wasn't passing a ruling or making a judgment in any way, shape, or form.

We'll have Monsieur Dusseault for three minutes, please.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you, Mr. Chair.

I still want to stay on the subject of public confidence, while taking into account what you said.

Are you currently disclosing information regarding successful operations?

For example, I'm talking about cases where you received information that contained enough clues to prevent a dangerous act targeting Canada from being committed. In these cases, do you disclose the information?

● (1655)

Mr. Stephen Burt: What do you mean?

Mr. Pierre-Luc Dusseault: Without using Mr. Rochon's example of acts that could be committed on Parliament Hill, I want to know whether you ever, at this time, disclose information on successful operations.

Mr. Stephen Burt: Normally, the intelligence sector doesn't decide whether to disclose something. Political or departmental officials decide, for the public good, whether something should be disclosed or whether the information and process should be kept secure.

Mr. Pierre-Luc Dusseault: Can't it still happen?

Mr. Dominic Rochon: There may also be legal action. Therefore, we have limitations.

Mr. Pierre-Luc Dusseault: Okay.

I understand that disclosing the way you managed to acquire information may jeopardize your ability to continue preventing dangerous acts from being committed. That said, it would be possible to see with the committee how public confidence could be improved. People sometimes wonder what your services are used for. You may be able to show that the information is useful and can help make certain operations successful.

With regard to the oversight of agencies, the Privacy Commissioner noted that, under the new legislation, 14 of the 17 agencies were not subject to oversight.

What are your thoughts on the recommendation of the Commissioner who, if the committee were to proceed, could arrange that the 14 agencies be subject to oversight to ensure compliance with the legislation?

Mr. Stephen Burt: We're subject to the oversight of the Commissioner himself, the Office of the Information Commissioner and the Auditor General. We also have an ombudsman in the Department of National Defence. In terms of counter-intelligence, we have a judge advocate general committee consisting of lawyers who work internally and of external organizations that specifically monitor our counter-intelligence capacity.

I'm fairly confident about the mechanisms that govern us to ensure compliance with the legislation and policies under which we operate.

Mr. Pierre-Luc Dusseault: Is the Communications Security Establishment subject to oversight?

Mr. Dominic Rochon: Yes, we have a commissioner. We're one of the three—

Mr. Pierre-Luc Dusseault: —of the 17 agencies.

How is Transport Canada upholding the commissioner's recommendation that an oversight agency ensure compliance with the legislation?

[*English*]

The Chair: Mr. Dusseault, we're about a minute past. Do you have a quick—

[*Translation*]

Mr. Pierre-Luc Dusseault: Mr. Roussel, I want to hear your comments.

Mr. Donald Roussel: We leave it up to the commissioner to act based on the recommendations he makes. We don't have a particular opinion on the matter. We're already subject to a complete set of extremely strict verifications by both the Auditor General and the Privacy Commissioner.

[*English*]

The Chair: Thank you, Mr. Dusseault.

Thank you to our witnesses.

We do have about 12 minutes before we are going to go quickly to committee business. We're going to use that time for members of Parliament who haven't had an opportunity.

Mr. Dubourg, you have a couple of minutes, and Mr. Erskine-Smith, there's a couple of minutes for you. Then I'll have a couple of questions, if you don't mind.

Mr. Dubourg, the floor is yours.

[*Translation*]

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

I would like to welcome the witnesses who are here to help us with our work.

My first question is for you, Mr. Burt.

You said in your remarks that one of the main contributions of the SCISA is to allow a department to exchange information with another department, even if the recipient's use of the information will be different, provided it concerns Canada's security.

There are 17 institutions. Do you think there are too many? Not all of these institutions are mandated to consider Canada's security. Should there be some mechanism to ensure that these new information exchanges are appropriate?

● (1700)

Mr. Stephen Burt: I can't say if the number of institutions is appropriate. The institutions listed in the schedule of the SCISA are there either to provide information to others or to educate government agencies that have a national security mandate, as Mr. Rochon said. This is important for us. If the Department of National Defence is included in that schedule, it isn't because it doesn't have the means to share information, but rather because we want to clarify its mandate with all the other departments. It allows the departments that have national security information to share it with us.

Mr. Emmanuel Dubourg: Okay.

When you find information about Health Canada and the Canada Revenue Agency, for example, do you have a memorandum of understanding to share this information with these institutions?

Mr. Stephen Burt: We don't have a formal agreement with the various departments. We have more traditional ties with the CSE, for instance. The SCISA is the framework for this.

Mr. Emmanuel Dubourg: And not the current legislation.

Mr. Stephen Burt: The SCISA provides this framework. Otherwise there isn't one.

Mr. Emmanuel Dubourg: Right.

Mr. Rochon, you spoke earlier about the scope of the work you do. You said you block more than 100 million malicious access attempts almost every day. In terms of other access attempts in other departments, what do you do with that information? Do you keep it or do you automatically inform the department?

Mr. Dominic Rochon: No, it's impossible to keep that information.

Part B of our mandate deals with defending systems of importance to the government. Obviously, we see all kinds of situations every day. We block the malware we already know about. The goal isn't to keep all this information, but to see it pass, to block it and not to let it get through our defence systems.

Mr. Emmanuel Dubourg: I have one last question for you.

Are you concerned about the fact that the exchange of information between these institutions doesn't require legal intervention or a warrant from a judge?

Mr. Dominic Rochon: Under the current system?

Mr. Emmanuel Dubourg: Yes.

Mr. Dominic Rochon: No, not to my knowledge.

Mr. Stephen Burt: As I've mentioned a few times, it isn't that we couldn't share information before. This simply helps to better manage information sharing.

Mr. Emmanuel Dubourg: Thank you, Mr. Chair.

[*English*]

The Chair: Thank you, Mr. Dubourg.

Mr. Erskine-Smith, please.

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

I have just a few questions, first on relevance versus necessity. The legislation is, perhaps, too vague. We've had law professors come before us and say we should make it crystal clear that recipient institutions continue to operate within their own mandates. Perhaps we should also be very clear regarding a necessity test that the information accepted by recipient institutions will be necessary to their mandates, that relevance is only on the disclosing institution's side of things, and that it is being done to make it easier. These disclosing institutions aren't completely familiar with national security and your mandates, so rather than hindering the sharing of information, the relevance test would enable that information to flow.

Do you think that making it crystal clear that you are to operate within your mandates and that you are subject to a necessity test would be a hindrance to your operations in any way whatsoever?

● (1705)

Mr. Stephen Burt: I would say that, for any public servant, it's already crystal clear that you operate within your mandate. That's fairly fundamental to what we do.

The issue of necessity versus relevance, I think, is a question for the committee and for the government, in terms of what the appropriate test is to enable sharing.

Mr. Nathaniel Erskine-Smith: To pick up on the chair's point, I want to be clear about whether it would get in the way of your jobs in any way if we clarified that the recipient institutions were subject to a necessity test, that the information you receive had to be necessary to your mandate.

Mr. Stephen Burt: It's hard to say. My perception is that it would raise the bar. It would be a more difficult bar to meet for sharing, but it would depend on how it was formulated. It depends on what the committee and the government would like to achieve.

Mr. Nathaniel Erskine-Smith: Does anyone have any other views?

Mr. Dominic Rochon: I'll jump in and say that I can only use our example and our mandate. From a necessity versus a relevance perspective, in my case, if you're sharing information with me, it can't be directed at a Canadian. It has to be directed at a non-Canadian outside of Canada, number one. It has to be relevant to intelligence priorities as mandated by cabinet. It has to be for international affairs, security, or defence. Is it relevant to that or is it necessary for that?

Also, in terms of what I'm going to do with it or what my organization's going to do with it, we do foreign intelligence. You're going to give us a tip. We're going to then follow that tip down. If you think there's a threat against a Canadian embassy abroad, we're going to run down that tip. Is that tip necessary? Is it relevant? We don't know. It's the beginning of something that we're going to chase down, and then we're going to produce foreign intelligence on it. Then when we share foreign intelligence under our National Defence Act mandate, the assessors, the people who are going to fuse that intelligence, will ultimately decide whether there needs to be action upon that intelligence. It's difficult to answer your question.

Mr. Nathaniel Erskine-Smith: I have one last question. Two of your organizations have not actually received information, and Mr. Burt's has just one time. When that occurred and if that were to occur for the other two, who would be responsible for overseeing whether that sharing of information was responsible and appropriate?

Mr. Stephen Burt: Within our system, within my organization, we have a release and disclosure coordination office, whose business it is to determine what should be done with various information, whether it's being dealt with through a judicial process or being released through an access to information request, or in this case, being dealt with under SCISA. We have two points of contact under the act, two possible heads of organization: first, the minister for the department, and second, the chief of the defence staff for the armed forces. Two organizations have been delegated to receive that information and track it on their behalf. One is the release and disclosure office in my organization, and the other is the Canadian Forces integrated command centre, which is a 24/7 operation within our operational command.

Mr. Dominic Rochon: In our case, in terms of receiving information, it's very clear how it can be done mechanically. We have a 24/7 operations centre that at any given time would receive information coming in. Then there's a strict protocol in place under which it would reach out to disclosure offices, operational policy offices that report to me, which would ultimately then vet whether or not we're in a position to receive it and whether it fits within our mandate.

As Mr. Burt just said, we have delegated authority under SCISA. It's delegated to three deputy chiefs. I am one of them, and there is the deputy chief of foreign signals intelligence and the deputy chief of IT security, who ultimately will then weigh in as to whether or not we follow through with it.

Mr. Nathaniel Erskine-Smith: With CSIS or with CSE, is there no independent review?

Mr. Dominic Rochon: Independent review by someone who would receive information that—

Mr. Nathaniel Erskine-Smith: Well, SIRC is currently reviewing the information that CSIS has received subject to SCISA, for example. There's no independent review in that way.

Mr. Dominic Rochon: In our case, we have an independent commissioner who could review it.

Mr. Nathaniel Erskine-Smith: At CSE, that's right, yes.

Mr. Stephen Burt: We haven't received anything yet, but if it were to be reviewed, we would ask our chief of review services internally to undertake that.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you very much to our witnesses.

I have a couple of quick questions, if the committee will indulge me.

With regard to the effect of SCISA, if my interpretation or understanding here is correct, the tests made it a lot more clear and practical when it came to the sharing of information. I don't think we have really thoroughly discussed the issue of timeliness.

Mr. Burt, Mr. Rochon, and Mr. Roussel, in your agencies, how important sometimes is the timeliness of being able to share information? Does SCISA provide a more effective vehicle for the timely sharing of information?

● (1710)

Mr. Stephen Burt: Timeliness is a factor. Having said that, we don't live on *24* here. Generally speaking, as Mr. Rochon said, when you get a piece of information of any kind, it's the beginning of a process for an intelligence organization to try to run down exactly what that means.

Timeliness is a factor, but I guess I would submit that clarity is a big help when it comes to timeliness.

The Chair: Mr. Rochon.

Mr. Dominic Rochon: Yes, I'd echo that. Timeliness can be important. Certainly having a framework that is understood and that provides a better understanding of how information can flow can only improve timeliness. That can only improve the process of information sharing over time.

The Chair: Mr. Roussel.

Mr. Donald Roussel: For us, timeliness is critical when it comes to a plane, for example, that's moving at 900 kilometres an hour, coming towards us with possibly challenging individuals. Things are moving extremely fast in some domains. In others they're slower, but they're sometimes more complex. I can give the example of some of the immigrant ships that landed in Canada. That was extremely complex. That was in 2010, and it involved pretty well all the agencies. Exchanging information and having domain awareness as rapidly as possible was key to the success of the operation.

The Chair: Mr. Roussel, my question to you then is this. Does SCISA provide your agency with a better framework insofar as timeliness is concerned?

Mr. Donald Roussel: Yes, definitely.

The Chair: Thank you very much.

I would like to thank our witnesses for appearing here today. Your insights were very helpful.

Colleagues, we now move to our committee business. If you'll indulge me, we have some decisions that we need to make. It shouldn't be terribly complicated, so let's just get on to that.

We've been sent a letter by the chair of the Liaison Committee, which makes plans—

Mr. Bob Bratina: Are we in camera?

The Chair: No, we're not. Do you want to be?

Mr. Bob Bratina: No.

The Chair: I don't think there's anything here that will be terribly....

I received a letter from the chair of the Liaison Committee asking us if we have any committee travel. The subcommittee of liaison makes priorities and recommends them to the Liaison Committee for parliamentary committee travel.

I do not think we have anything. Should I respond? Unless somebody here has some ideas about a potential trip, I don't think we have anything to submit to the Liaison Committee for a request for travel. Does anybody foresee that?

No, so we'll just have our standard request of the standard committee amount for every study that we do.

Depending on the length of time that we're going to move on to PIPEDA, when we do, if we're going to hear from as many witnesses as have been submitted, we may actually have to ask for some more budget. I'm just letting colleagues know that. We should make sure that we have that discussion when we go to frame the length of any future studies that we have.

In terms of meetings, we have 26 meetings remaining until the end of June, excluding the last two sitting weeks of June, because we sometimes don't know when the House will adjourn.

We have witnesses this Thursday and witnesses next Tuesday for SCISA, and we have nothing booked, as you can see, for Thursday, February 9, and all the way through. We need to have some direction. We can continue asking witnesses to come on SCISA, or we can decide to wrap it up, move on with something else, and then provide some time. I'm getting the sense that we're done with SCISA witnesses, at this particular point. Do we want to bring in the ministers to close, or not? Is there no need? I'm sensing no need.

Then may I suggest that on February 9 we spend that day, or at least a portion of that day, giving priorities and instructions to the analysts for the draft report? Is that fine? Very good.

May I then suggest that with regard to Tuesday the 14th, through to the 16th, because we've already adopted a motion to study PIPEDA, I instruct the clerk to start inviting witnesses to testify on the 14th and 16th? That should give the analysts enough time to prepare a draft report.

When will we be able to have consideration of a draft report on SCISA?

● (1715)

Ms. Chloé Forget (Committee Researcher): Hugues and I discussed it. We thought that maybe we could have more time, and then study the report on March 7, if that is possible, if there's no sense of urgency—

The Chair: Is everybody fine with that? If there's no sense of urgency, then I'll instruct the clerk to start inviting witnesses for PIPEDA on February 14, 16, 21, and 23, unless other committee business supersedes. Is that okay?

Then we'll make a decision, post the break, where we come back for the consideration of the draft report, perhaps March 7. Does that satisfy members of the committee?

Mr. Dusseault.

Mr. Raj Saini: When would we have the report, the first draft? Is it on March 7 or prior to that?

The Chair: The first meeting to consider the draft report would be on March 7. We would likely have the draft report in our hands several days before.

Mr. Dusseault.

Mr. Pierre-Luc Dusseault: Do we give instructions to the analysts on the draft report?

The Chair: We're going to do that during part of our time on the ninth.

With regard to the meeting the 7th, which will be our last meeting, we have an issue with the number of people that agencies and departments want to have here. I'll let the clerk explain the issue.

The Clerk: As you can see, we have four agencies and departments that have been invited to come in. The total number of people who would be sitting at the table would be 10, and the room is fairly small. That would bring us all the way around....

On the part of foreign affairs, there seems to be quite a few people coming in. May I suggest that we might split the meeting into two panels of two organizations, and then spend an hour with each? That would solve our logistics issue.

The Chair: We do have room for 10 at the table, but it does become quite cumbersome to manage.

I'm sensing from the committee members that we're going to split the meeting.

Mr. Dusseault.

[*Translation*]

Mr. Pierre-Luc Dusseault: I'm not opposed to that, but I don't think that the four representatives from the Department of Foreign Affairs will all intervene. It's rather rare, even when there are two, that the two witnesses intervene. They are the ones who proposed these four people. I have no objection to splitting the meeting into two parts.

The Clerk: If I may, Mr. Chair, I would add that people from the department's parliamentary affairs sector explained that this affected more than one directorate within the department and that it seemed important to them that four people be able to appear to answer the committee members' questions.

[*English*]

The Chair: I think we have consensus then.

Hugues, if you want to set it up that way so we only have a manageable number of people at the table, that would be great.

Thank you, colleagues.

We have to deal with future studies. We have PIPEDA on the table. We've adopted a motion on privacy and federal political parties as per the motion adopted on October 18. We did actually pass that motion. Do you want to start inviting witnesses for that study, or are we going to just leave that and have PIPEDA as the priority?

Okay, I'm guessing PIPEDA is the priority.

All right. There was good government response to the committee's second report, as per the motion adopted by the committee on October 18. Do we want to, at some point in time, as a committee, review the government's response to our report?

Mr. Nathaniel Erskine-Smith: We could discuss that on the ninth as well.

The Chair: As part of the drafting...? I think that's a wise use of the time, Mr. Erskine-Smith. That's what we'll do then.

We have received a letter indicating orders in council. Ms. Dawson and Ms. Shepherd, the respective commissioners, have been reappointed for an interim period of six months. We have until April 4 to decide whether or not we wish to hear from these commissioners on their reappointments. Do you wish to invite the commissioners in again?

Mr. Dusseault.

[*Translation*]

Mr. Pierre-Luc Dusseault: The clerk or the analysts would need to confirm this, but I think this is the second time that Ms. Dawson's interim contract is being renewed.

[*English*]

The Chair: That is correct, Mr. Dusseault.

The question is that for every order in council for an appointment of a commissioner, the committee has the ability to request.... I'm sensing confusion in the room.

Mr. Jeneroux.

Mr. Matt Jeneroux: I don't think so, Mr. Chair. I'm not confused.

I would like to have them come in. I think I previously raised that it would be nice to have the commissioners in. They have been appointed, particularly in Ms. Dawson's case, time and time again. It would be nice to have them here. It would be nice to have a discussion on what she plans to do in the next six months. If it requires a motion, I'd be happy to make that motion.

● (1720)

Mr. Nathaniel Erskine-Smith: If I may, Chair, it's Thursday the 2nd, and we have witnesses for the 7th. Then we have two hours on Thursday the 9th to give instructions to review the government's response.

We're looking at the PIPEDA on February 14, 16, 21, and 23 for considering the draft report. We then have available dates in March, and moving into April as well. I would propose that we have a more fulsome discussion, where people have turned their minds to what should be on that calendar, and so renew this discussion and come to a decision on the ninth as well.

The Chair: We have until April 4, according to the Standing Orders 110 and 111. I just wanted to bring that to your attention.

At this point in time, we have no objections; we have some who wish to.... Do you want to table this until another committee business time? Is that what I'm hearing?

Mr. Nathaniel Erskine-Smith: Yes.

The Chair: All right. That's what we'll do.

We still have some motions that are before the committee, and we have to decide how we're going to dispense with those at some point in time.

If there's no need to dispense with any of those motions at this point, then we're done.

Very good, colleagues. The meeting is adjourned.