HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 042 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, January 31, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, January 31, 2017

● (1540)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I call the meeting to order. For those of you who believe in the motto "better late than never", I am certainly glad to get this committee meeting number 42 going.

I want to welcome everybody back. I hope everybody had a great Christmas and holiday break, and I wish everyone a healthy and happy new year. It's great to see familiar faces, not only those around this table but of course those of all the folks who sit in the wings and support us as well. It's great to see all of you.

We have a continuation of our study on the Security of Canada Information Sharing Act, more affectionately known as SCISA. Today we have with us witnesses who have been waiting very patiently. On behalf of my colleagues, I just want to say that it's very understandable why there's a bit of delay today. A couple of seasoned colleagues in the House of Commons are doing their farewell speeches. I think members were sticking around for that. We can't fault them for that. There are a lot of friendships and good relations across party lines for those kinds of things here.

Without further ado, I will introduce our three witnesses. I'd ask you to give your testimony in the order in which I introduce you. You have up to 10 minutes for your opening remarks. Then we'll immediately proceed to questions and answers.

From OpenMedia, we are joined by video conference by Ms. Laura Tribe, who is the executive director. Welcome.

From the Canadian Bar Association, we have Mr. David Elder, executive member of the privacy and access law section. Also, of course, as an individual, we have Mr. David Fraser, who is a partner at McInnes Cooper.

Ms. Tribe, the floor is yours for up to 10 minutes please.

Ms. Laura Tribe (Executive Director, OpenMedia): Thank you.

Good afternoon. My name is Laura Tribe, and I am the executive director of OpenMedia. We are a digital rights organization that works to keep the Internet open, affordable, and surveillance-free. Given our work, it seems pretty fitting that I'm joining you by digital link from Vancouver this afternoon.

Since Bill C-51 was first announced, OpenMedia has been actively campaigning alongside many other groups against this reckless, dangerous, and ineffective legislation. We believe Bill C-51 should be repealed in its entirety, and that the Security of Canada Information Sharing Act, or SCISA, is one of the most problematic components within Bill C-51.

OpenMedia and our community believe that when the previous federal government passed SCISA, it weakened the privacy rules that keep us all safe. SCISA contributes to an alarming privacy deficit that makes all Canadians less secure. This privacy deficit is dangerous and will have lasting consequences for the health of our democracy, for our liberty, and for our daily lives.

I want to begin by commending this committee's recently published recommendations on reforms to the Privacy Act. As you are all aware, the Privacy Act has not been meaningfully updated since its introduction in the 1980s, and OpenMedia agrees whole-heartedly with this committee and the federal Privacy Commissioner that the Privacy Act must be brought into the digital age with the addition of strong, meaningful, and modern protections.

Specifically, we support your recommendations that the Privacy Act be strengthened to require that government activities related to the collection and sharing of information be necessary and proportionate.

We also strongly support your call to impose overarching limitations on the retention of data and to strengthen transparency reporting requirements for government institutions.

We believe the recommendations set out in your December report will substantively improve privacy protection and have the potential to help mitigate at least some of the serious problems with SCISA.

As you know, the government recently concluded the public phase of its consultation into a range of national security issues, including Bill C-51 and SCISA. Unfortunately, the green paper that was published at the outset of the public consultation focused far more on the desires of police than on the privacy needs of Canadians, with many issues, including those around information sharing, being framed in a highly one-sided way that ignores the reasons the public is so concerned in the first place.

Despite the misleadingly benign portrait of SCISA painted by this green paper, from a privacy perspective there are very serious problems with this legislation. Today I will be speaking to the three main concerns brought forward by the OpenMedia community.

OpenMedia's first concern is that SCISA enables domestic dragnet information sharing that security experts warn is counterproductive. As you know, SCISA authorizes all federal institutions to disclose Canadians' private information to no fewer than 17 separate government agencies.

Anything that relates to the sweepingly broad definition of "activities that undermine the security of Canada" can be disclosed. I echo the concerns of the BCCLA's Micheal Vonn that not only does SCISA have, and I quote, "no requirement for individualized grounds for data collection", but that it seems "likely it was enacted precisely for the purposes of bulk data acquisition."

This is deeply problematic. To participate in modern life, citizens must share lots of information with our government. This information should not be repurposed into an open-ended intelligence dragnet.

Previous witnesses have raised specific examples that shed light on just how problematic the type of information sharing facilitated by SCISA can be: CIPPIC's Tamir Israel cited recent examples of government targeting journalists and peaceful indigenous activists and expressed concern that SCISA could be leveraged to share information about their activities in spite of the supposed exception for activities of "advocacy, protest, dissent and artistic expression", and the BCCLA's Micheal Vonn pointed to the extraordinary data collection powers of FINTRAC and how its counterbalancing privacy protections have been "decidedly unsettled by SCISA to the point where its constitutionality may be at issue."

OpenMedia believes the principles of necessity and proportionality are workable mechanisms for sharing or receiving threat data, and there is no need for SCISA's expanded definitions of security in this context.

To safeguard Canadians, information sharing of data entrusted to government agencies should only occur in narrow circumstances, and the Privacy Commissioner must be empowered to assess the overall necessity and proportionality of any and all information-sharing activities.

Additionally, all government institutions should be required to keep thorough records of when they disclose our private information, including to foreign governments, and information sharing in general should only occur subject to formalized agreements.

OpenMedia's second major concern with SCISA is that inappropriate information sharing with foreign governments can have a devastating impact on the lives of individual Canadians. In recent years, over 200 Canadians have publicly come forward to say their personal or professional lives have been ruined due to information disclosures with foreign governments, despite never having broken the law, and we'll never know how many others who have been impacted have chosen to stay silent.

● (1545)

Some have faced career limitations, while others have had to deal with travel restrictions. False charges that were subsequently dropped or dismissed, never resulting in criminal records, or even brief contact with the mental health system can create flags with life-changing consequences. These stories underline a very real threat regarding the government's handling of our sensitive data: that without safeguards in place, government bureaucrats will simply act recklessly and make life-impacting mistakes.

Canada's security agencies, the designated recipients of information under SCISA, routinely and on a large scale share information with their counterparts in the U.S. When mistakes are made, the impact on individual Canadians can be profoundly damaging. We need look no further than the case of Maher Arar to see that. These long-standing problems have been exacerbated by the Trump administration's recent decision to eliminate all U.S. Privacy Act protections for foreigners, including Canadians. As Professor Michael Geist points out,

> the order should raise significant concerns about government data shared with U.S. authorities as well as the collection of Canadian personal information by U.S. agencies. Given the close integration between U.S. and Canadian agencies—as well as the fact that Canadian Internet traffic frequently traverses into the U.S.—there are serious implications for Canadian privacy.

These concerns are compounded by the Trump administration's expressed openness to returning to torture policies that were largely discontinued by the previous administration. Sadly, should SCISA remain in place, more examples like that of Maher Arar are not unlikely.

OpenMedia's third concern is the way that reckless information sharing harms our digital economy. Leading Canadian business figures, including the heads of Hootsuite, Slack, Shopify, and OpenText, have warned that the information-sharing provisions of SCISA will harm the Canadian economy by undermining trust in our commerce and trade. In an open letter published shortly after Bill C-51 was first proposed, these business leaders had this warning:

> The data disclosures on innocent Canadians and those travelling to Canada for business or recreation could make our clients leave us for European shores, where privacy is valued. Duplicated data flowing between multiple unsecured federal government and foreign government databases leaves Canadians and Canadian businesses even more open to being victimized by data breaches, cyber criminals and identity theft.

A second letter from the business community, published last month in response to the government's national security consultation, reiterated these concerns and called for the legislation to be fully scrapped, saying:

> We hope your government will listen to Canadians, the business community and experts by starting over with new legislation that respects our collective desire for security overall. Privacy and data integrity safeguards represent security in its most clear and basic sense. Let’s start with this understanding and work from there.

For all these reasons, OpenMedia believes that the Security of Canada Information Sharing Act should be completely repealed, alongside the rest of Bill C-51. As one of our community members told us recently:

> Repeal it completely and do it now. If the Liberal government believes some sort of bill is needed, then write a new bill from scratch only after thorough consultations with legal experts and citizens to ensure Canadian rights and freedom are preserved.

Strong privacy rights need to be at the heart of any healthy democracy because they are the foundation of many other democratic rights we hold dear. We all deserve effective legal measures to protect the privacy of every resident of Canada against intrusion by government entities or malicious actors and abuse by law enforcement. Canadians deserve at least the same high level of privacy safeguards for our digital homes as we do for our brick-and-mortar homes, if not higher, given the highly sensitive data stores and interactions that are increasingly housed online.

For many Canadians, security is privacy, in the most human sense of that word. Repeated revelations of intrusive government surveillance, whether that be spying by CSE, the new powers in SCISA, or other elements of Bill C-51, have left Canadians fearful for their personal security. This committee's work can play a significant role in ensuring that Canada can address those fears and become a global leader in reining in excessive digital surveillance practices. Let's lead by example and help set a new global standard for privacy protection in a digital age.

Thank you.

● (1550)

The Chair: Thank you very much.

We now move to Mr. Elder, from the the Canadian Bar Association. You have up to 10 minutes, please.

Mr. David Elder (Executive Member, Privacy and Access Law Section, Canadian Bar Association): Thanks very much, and good afternoon, Mr. Chair and members of the committee.

My name is David Elder. I am an executive committee member of the privacy and access law section of the Canadian Bar Association. I also co-lead the privacy and data protection practice at Stikeman Elliott LLP. I was formerly the chief privacy officer for a major Canadian telecommunications company, and I have been practising privacy law for over 20 years.

Thank you for the invitation to present the CBA's view on the Security of Canada Information Sharing Act.

The CBA is a national association of over 36,000 lawyers, law students, notaries, and academics. An important aspect of the CBA's mandate is seeking improvements in the law and the administration of justice, and it is that perspective that brings us to appear before you today.

Our submission to the committee on SCISA was prepared by a CBA national security working group, with contributions from the privacy and access law section as well as other sections. The section's membership represents lawyers with in-depth knowledge in the areas of privacy law and access to information from every part of the country, drawn from private practice, industry, and government sectors.

Our section also worked on the CBA submission this past fall in response to the government's national security green paper, and the year before that on the CBA submission to the public safety and national security committee respecting Bill C-51, part of which contains SCISA.

I'll now address the substance of our submission.

The CBA supports information sharing for the purpose of national security when that sharing is necessary, proportionate, and accompanied by adequate measures against potential abuse. However, sharing too much information or sharing information for unrestricted purposes can lead to harmful consequences. Moreover, such oversharing is contrary to the principles underlying privacy laws in Canada.

SCISA has significantly expanded intragovernmental information sharing for national security purposes in Canada, including the sharing of potentially sensitive personal information, without precise definitions, basic privacy protections, or clear limitations on the purposes for sharing. While some helpful changes were made to SCISA before its final passage into law in 2015, the statute still causes concern on several fronts.

The CBA has four main concerns with the law as enacted.

The first is independent oversight. SCISA includes a number of useful guiding principles for information sharing, including the principle that originators should retain control over shared information and the principle that information should be disclosed under the act only to institutions carrying out responsibilities in respect of activities that undermine the security of Canada.

However, to be meaningful, SCISA must include a robust oversight and accountability mechanism to enforce these principles. In the CBA's view, any oversight body should have independence from the government institutions that will be sharing information under the act in order to avoid any potential conflicts of interest.

There may be several oversight models that could work in this regard. The committee of parliamentarians that was proposed in Bill C-22 could be one such option. Existing institutions, such as the Office of the Privacy Commissioner of Canada, might also work.

Whatever oversight mechanism is pursued, in order to better facilitate the review of activities carried out under SCISA, the CBA submits that regulations should be introduced requiring disclosing institutions to keep a record of all disclosures made under SCISA and requiring receiving institutions to maintain records of subsequent use and disclosure of information received pursuant to SCISA. If such records do not exist, it will be nearly impossible for any oversight body to determine whether the guiding principles of the act are indeed being respected.

The second concern is balanced information sharing.

The CBA notes that subsection 5(1) of SCISA permits disclosure among the 17 government institutions listed in the schedules of the act if the information is relevant to the recipient institution's jurisdiction or responsibilities under an act of Parliament or another lawful authority respecting national security. In the CBA's view, mere relevance is a very low standard for what should be an exceptional sharing of information between government institutions, and this could allow for unnecessary and overbroad sharing of information, undermining the privacy rights of Canadians. The CBA agrees with the previous submissions of the Privacy Commissioner of Canada and others that a test of necessity would better balance the objectives of SCISA with privacy rights and principles. In other words, in order for information to be shared with another institution, such sharing must not only be relevant to the receiving institution's mandate respecting national security, but also have to be necessary in order to allow the receiving institution to fulfill that mandate.

● (1555)

The CBA is also of the view that the existing schedule 3 to SCISA, which lists the institutions with which information may be shared under the act, should be expanded to include references to the specific sections of the statute supervised or implemented by those institutions that might relate to national security concerns. Greater specificity would assist both disclosing and receiving institutions, as well as any oversight body, in assessing whether disclosure to another institution might be appropriate.

Our third concern with SCISA is the lack of restrictions around subsequent use and disclosure of information disclosed to an institution under section 5 of SCISA. More specifically, the current provision seems to allow for the subsequent disclosure by a recipient institution to other non-designated government institutions, to individuals, to foreign governments, or even to the private sector, and for purposes unrelated to national security.

In the CBA's view, the information sharing between government institutions contemplated by SCISA should be seen as an extraordinary measure designed to fulfill an explicit narrow purpose. Accordingly, SCISA must be designed to eliminate what is sometimes called “purpose creep”, including potential disclosure to third parties.

The CBA is particularly concerned about subsequent use and further disclosures by a receiving institution when the information has been obtained by the disclosing institution through the exercise of extraordinary powers, such as powers to compel production of information or enter premises. It would be inappropriate for a receiving institution to be able to leverage, for purposes unrelated to national security, any investigation and enforcement powers not conferred on the receiving institution by Parliament. SCISA should not allow receiving institutions to obtain indirectly that which they cannot obtain directly.

Fourth, the CBA is concerned about reliability of information.

The CBA is concerned that SCISA includes few effective checks and balances on information sharing or safeguards to ensure that shared information is reliable. The Arar commission stressed the importance of precautions to ensure that information is accurate and reliable before it is shared. Omitting safeguards in SCISA ignores lessons learned through the Arar saga and the recommendations of the Arar commission, and risks repeating the same mistakes.

In conclusion, once again the CBA appreciates the opportunity to share our views on SCISA. We support balanced information sharing for the purpose of national security when it is necessary and proportionate, and is accompanied by safeguards that are adequate to protect individual privacy rights and to ensure the reliability of any information shared pursuant to the act.

I'd be pleased to respond to any questions the committee members may have.

● (1600)

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

Our last presentation is going to be from Mr. Fraser as an individual, but he's a partner from McInnes Cooper.

Mr. Fraser, the floor is yours.

Mr. David Fraser (Partner, McInnes Cooper, As an Individual): Thank you very much.

Thank you very much to the committee and to the chair for the opportunity to speak with you today about this very important subject.

I will introduce myself. I am a privacy lawyer practising with McInnes Cooper in Halifax. I've been practising law in this area for more than 15 years, and in that time I've had the benefit of advising clients on a full range of privacy, access to information, and technology issues. I've worked with clients who regularly have contact with the police and with the national security authorities looking for information, both through regular lawful channels and, shall we say, informal channels.

I am here in my personal capacity, so I'm not speaking on behalf of any of my clients or any of the associations that I am a member of —I'm a proud CBA member—nor am I speaking on behalf of my firm. This is just me.

This committee has a very important opportunity, and I think we are at a turning point in global history. We have the chance, right now, to take a deep breath, take a step back, and ask some very important questions: who are we as Canadians, and what do we want to be? What kind of country do we want to live in, and are we taking positive steps to make that happen?

Looking south of the border, I am very mindful of a phrase that I first heard said by William Binney, who was one of the first whistleblowers from the U.S. National Security Agency. He left because he was afraid that what he was being asked to create within that organization was something he called “turnkey totalitarianism”.

If you build an intrusive tool for the most benevolent institution, you can have faith in the people for whom you build it, but you can't be sure that it won't fall into the wrong hands. Setting aside the cynicism I've developed over the last dozen years, even if you absolutely believe what the leaders of our national security and policing agencies say to you—and I understand there will be further testimony from them—you can't be sure that their replacements will necessarily have the same good faith and concern about the rights of citizens. You can't be sure about the good faith and commitment to Canadian values of the next government.

The new U.S. administration has at its disposal the most significant surveillance apparatus ever assembled, and it's being built with Canadian collaboration. This committee needs to look at the here and now, but also look over the horizon for what may come next. The Anti-terrorism Act of 2001 and the Anti-terrorism Act of 2015 are, or could be, the foundation of what could become a massive abuse of Canadian rights.

We also need to look at whether any of this is really necessary or proportional in the first place. We need to look at what we have here and what is going on. On the one hand, recently we've seen that CSIS, with the assistance of Department of Justice lawyers, has lied to courts in order to feed CSIS databases. We've also seen that CSIS has refused to delete the information that it unlawfully retains. Most recently, we've seen that CSIS has been working within government to try to justify its data mining practices and has actually been looking to get more data to put into its massive databases.

Then we have the Security of Canada Information Sharing Act, which is, in my view, a privacy disaster. The privacy of Canadians was previously connected by information silos. Departments could collect information that was reasonably necessary for their purposes. They could share it with other departments for purposes that were consistent with those purposes, and they could share it with law enforcement in other circumstances. There were rules around that. You knew that the information about your Canada Pension Plan contributions or EI claims would not be used for any other purpose, unless the relatively weak hurdles of the Privacy Act—with which everybody here is familiar—were complied with, or unless a judge determined that it was appropriate in those circumstances that the public interest in disclosure outweighed the privacy interest.

Now we have a system whereby CSIS can ask any government department for virtually any data, as long as they think it's relevant to their task. You can try to get insight into how they would calculate that; I'm not sure. They can then get it, and it is no longer covered by the privacy protection of the originating institution.

They might think, for example, that people who visit bad guys are probably bad guys themselves, so let's get all the visitor logs from Correctional Service of Canada and then let's match that up against the Canada Border Services Agency records of people leaving and returning to Canada, and passport applications—and why not all the records of people receiving EI, and then everyone else's tax returns to see who has donated to Muslim charities? This law would allow CSIS or the RCMP to collect, in one massive database, all the information that every other government department has about you, based on the linchpin of that extremely low threshold of relevance.

SCISA does not contain any limit on what organizations like CSIS or the RCMP can do once they build those databases. There is nothing built into SCISA that does that. There is also no internal limit on how much information can be transferred between any government department and any of those institutions listed in the schedule to the act. On top of this, all of this happens in the shadows: there is no oversight within this statute.

● (1605)

As parliamentarians, all you know are the evasive non-answers given to you. There is no oversight, no accountability within this framework. This is essentially a blank cheque giving national security agencies access to some of the most sensitive personal information about Canadians. This is a real problem, and the act should be repealed.

In closing, I would also highlight the presence of section 9 in the statute. It should raise a flag. It should raise a flag very high. It says, “No civil proceedings lie against any person for their disclosure in good faith of information under this Act.”

If a statute has to provide immunity for otherwise unlawful conduct, we should be very careful about authorizing that conduct in the first place and we should be very careful about granting that immunity.

Thank you very much again for this opportunity. I very much look forward to the discussion.

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

We've had some great testimony from our witnesses, and I'm sure we'll have some very interesting questions from somebody over here.

Mr. Long, why don't you start us off for seven minutes?

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

I want to welcome my colleagues all back to Ottawa. There's nice cold weather out there to keep everybody sharp. I thank our presenters for their very interesting presentations.

Mr. Fraser, welcome back.

Mr. David Fraser: Thank you very much.

Mr. Wayne Long: He's another Atlantic Canadian.

I just want to get your comments. Obviously in this committee we're very busy. With this issue of activity that undermines the security of Canada, we want to make sure that people have the leeway and right to investigate, but we also want to balance that with people's privacy, and I think you have all spoken to that, so I'm going to wave my magic wand and make you part of our government.

It's so easy for people to say we're going to scrap it. I would like to know what you would suggest. What would be the first things you would do? Would you absolutely scrap it, and what would you replace it with, or what would you implement?

Mr. David Fraser: I'm not sure that we've necessarily seen that there was such a problem in the previous regime that it needed to be completely thrown out with a blank cheque handed to these authorities, but—

Mr. Wayne Long: Could you say that again?

Mr. David Fraser: I'm not sure that it was proven, when the statute was originally introduced, that it was so necessary, that there was something so wrong with the way that the Privacy Act worked in allowing information sharing among government departments.

We've certainly seen evidence of, and royal commissions referring to, the challenges of information sharing between government departments that exist and national security agencies. If you accept that as a premise, then the challenge is to come up with the appropriate tool. I think one of the big problems that we have overall is that this is using a sledgehammer when perhaps a ball-peen hammer or something more precise would do.

This statute provides licence for bulk data movement from one department to another. I don't have any concern, when it's justifiable and proportionate in the circumstances, with the RCMP and CSIS working on exactly the same file. I don't have a problem if, let's say, the employment insurance folks have reason to suspect that there is something sketchy going on, and they provide that information to the RCMP when it relates to national security. What I find particularly problematic is the scale at which information movement could take place, and the lack of accountability.

Mr. Wayne Long: Continue on, Mr. Fraser.

There are 17 organizations under the act privy to information sharing. Can you comment on the need for some of these organizations to have access to information? Are all required for national security?

● (1610)

Mr. David Fraser: I'm not sure. Certainly since 2001—

Mr. Wayne Long: Sorry. I'll just jump in again.

One of the organizations, say, is the Department of Health. Can you comment on what they would need that would pertain to national security?

Mr. David Fraser: I would simply be speculating, but I would assume it would relate to pandemics.

Mr. Wayne Long: Then what about the 17 organizations?

Mr. David Fraser: It seems like a longer list than is necessary. I would think that Canada should be focusing its efforts with respect to national security, rather than diffusing them across a whole bunch of organizations.

Mr. Wayne Long: Again, you've said technically that government has taken a sledgehammer to a problem that needed a mallet. Just so I'm clear, what would you suggest? Would you suggest we scrap it, or would you suggest we keep it and step back a bit?

Mr. David Fraser: I think my first suggestion would be to scrap it.

Mr. Wayne Long: Just outright scrap it.

Mr. David Fraser: It would be to scrap this statute, SCISA, and take a look at what is already in the Privacy Act, because every one of these organizations is subject to the Privacy Act, and the Privacy Act already has a scheme that allows one government institution to disclose information to another government institution, and it would naturally fall into that. If it needs to be tweaked, I think there probably are some places where it could be tweaked, but I think there is so much that is negative in this statute that we would be better off to do without it than to tinker with it.

Mr. Wayne Long: You would say right now that basically we are out of balance.

Mr. David Fraser: Yes.

Mr. Wayne Long: Do you have examples of where you think it's gone too far?

Mr. David Fraser: I don't think we've heard anything about what is going on in the background or between these organizations, and I don't think we are likely to hear about it. That's one of the problems. If there were oversight and accountability and we could actually get a line of sight into what was going on, if they had an obligation to publish in the *Canada Gazette* all the information-sharing agreements and the magnitude of them, and if they had to report in Parliament every year—as is required for wiretap warrants, for example—then we would have some insight, but as a lawyer, when I look at this and read the statute, I wonder what could go on in here. I think that a whole lot of mischief could go on within the ambit of this statute. I think we need to make sure we're putting appropriate fences around that information.

As I said in my comments, our information and our privacy within government has actually been protected by the existence of those silos, and when it comes to these most intrusive institutions of government, those silos have been broken down.

Mr. Wayne Long: Thank you.

Ms. Tribe, hello.

Ms. Laura Tribe: Hello.

Mr. Wayne Long: I want to get your opinions on that too, just to continue on my discussion with Mr. Fraser.

Are you suggesting an outright total scrapping? Would you like to see it modified? What would you do if you were us?

Ms. Laura Tribe: One of things I want to make clear is that I am speaking on behalf of the media community, not just myself.

One of the things that has been made really clear to the media throughout this entire process since Bill C-51 was first introduced with the information-sharing provisions within it is that it should be scrapped.

Any time we have talked to our community about what they would reform, we get quite a clear message that it is not worth fixing, that it is too big, that it is too broad, and that we are better off scrapping it and introducing smaller, more detailed provisions—

Mr. Wayne Long: I appreciate that and I hear you. I think we all realize we're certainly in a new era of heightened security and concern with our national security. However, one thing I continue to struggle with is that people say we need to scrap it and pull it right off the table, but what would you do in lieu of that?

Ms. Laura Tribe: To Mr. Fraser's point, I think we've seen no strong evidence that there is any problem with scrapping it. We haven't seen the evidence that it was necessary in the first place.

I think there has been a lot of information coming in. I'm very excited to see the results of the national security consultation that Public Safety Canada has conducted, as well as the findings of this committee, and to learn from law enforcement what they think they need and what they need to retain.

I think those are the elements, with more detail, that need to be reintroduced, either through updating the Privacy Act or through separate legislation, and that require proportionality when information is shared.

Really, the ultimate problem we have with what has been introduced is that, to the point about what has gone wrong so far, it could be years before we know what has gone wrong. There is no way for us, as citizens, to actually know what information is being shared about us, who it's being shared with, and whether it's even accurate.

I think it really removes people from the accuracy of their data. It removes them from having any control over their information and an understanding of where it's going, which has some really long-lasting effects, both in terms of negative ramifications and also on people's ability to express themselves.

● (1615)

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

We now move on to the next seven-minute set of questions. They will be from Mr. Jeneroux, please.

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

It's good to be back in committee with all of you.

Thank you to the three witnesses. I'm sorry we were late getting here.

I want to quickly clarify, in response to some of the comments that were made earlier in part of the presentation, that we're talking about information sharing. That's the focus of this study.

I'll quickly read into the record the purpose and principles of SCISA: SCISA is intended to protect Canadians against activities that undermine the security of Canada by encouraging and facilitating the sharing of information related to such activities among federal institutions. Some of the conversations seemed to take a bit of a different direction there.

I'll open up with my first question, which concerns the Five Eyes.

We know that it's important to the Government of Canada to have allies across the world. I would like to break it down into three separate questions for all three of you.

Do you believe these types of allied relationships better protect Canadians? If so, do you believe it is important that our national security organizations have tools similar to those of our allies? Are any of you aware of any of the information-sharing laws and oversight mechanisms of any of these allied countries?

I'll open it up to conversation.

The Chair: Who do you want to go first, Mr. Jeneroux? Who is ready to go?

Mr. Matt Jeneroux: It would be whoever is eager. Mr. Fraser looks eager to go.

Mr. David Fraser: Thank you.

Yes, I am in favour of collaboration with our allies. I think, in fact, that being a member of NATO has kept us safe since the Second World War. In this age when borders are less relevant, I think that's important when it comes to international crime, which includes terrorism. I think collaborating with our allies is important.

It's a matter of checks and balances within that. It's a matter of proportionality when it comes to intrusive measures. I think that is ultimately the key to it. I think the thing that caused.... When you cast your mind back to the kind of revelation associated with Mr. Snowden, it was not so much that the National Security Agency, the CSE, and others existed and that they were doing their published jobs related to signals intelligence; what was problematic was the bulk data collection, the collecting and analyzing of information about people for whom there was no reasonable suspicion that they were doing anything wrong.

At least for me, it's not an objection to the existence of CSIS. I think it's good. Actually, I'm glad that those powers were taken away from the RCMP following the McDonald commission. I don't have a problem with the existence of the Communications Security Establishment. It's all a matter of proportionality and keeping it all entirely within check.

When it comes to the third question that you asked with respect to information sharing, I don't think I have enough specific information to illuminate you, unfortunately.

Mr. David Elder: I'm not sure that this is a question that the CBA has addressed and come to a formal position on, so my remarks will be somewhat limited.

I would say that conceptually we would think that some level of sharing with our allies is necessary and that co-operation is in the interests of all of the agencies and all the nations concerned. We're increasingly dealing with global threats to everyone's security, and it does make some sense that we share that information.

However—and I'm not familiar with the individual rules for those foreign agencies, unfortunately—I think the position would be that any of that sharing has to continue to be proportionate and protect the privacy rights of Canadians that this country holds dear.

Ms. Laura Tribe: I think this is really not something that the OpenMedia community has discussed explicitly, but our mission and mandate is to be open and collaborative. I think that we all want to feel safe and we think that collaboration is important, so this is not to rule out working together with partners. I think this is really to echo what Mr. Fraser was saying about checks and balances.

As to your second question on whether we need similar tools, I think that to some extent it's a little problematic if it gets viewed as an arms race. If we decide that since the NSA has these tools, we need them too, it's problematic if checks and balance and proportionality are not being applied elsewhere. I think what we're really pushing for is for Canada to implement the checks and balances that we need, and then in exchange to actually ask our partners to do that as well.

Without having those checks and balances in place internally, our concern about collaboration with international partners is that the information that we might trust our partners and our own internal government agencies to use respectfully would not be treated the same way once it crossed our national borders. Having some very strict checks and balances and rules and regulations around that aspect is really important to us.

● (1620)

Mr. Matt Jeneroux: Ms. Tribe, do you think there are situations in which national security would trump the right to someone's privacy? Maybe you could elaborate on that. What situation would you see that would require protecting national security over the privacy of an individual?

Ms. Laura Tribe: I'm not a national security expert, so I can't speak to specific cases, but I think we have seen examples. That's the reason we have CSIS and the RCMP. There are very real threats to security and to our national security. In those cases, they identify potential suspects, and that is the information being shared. Bulk collection of data on everyone in Canada or everyone in the U.S., the sharing of all of the information from all the partners on any given individual, really feels like it's beyond the scope of national security. Identifying the information that is needed and how to share that is really the difference. I don't have the expertise to know exactly the information that's required and I'm not a member of law enforcement, but I think that's really the difference.

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

Mr. Blaikie, you have seven minutes, please.

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

I know we've heard pretty clearly from two of the witnesses today that the best place to start is to scrap this legislation and start anew. I was wondering, Mr. Elder, if your organization has a preference in terms of process. Does your organization think that this needs to be done away with first, and then if there are needs in terms of expanding the law for information sharing, that they be dealt with after this particular statute is out of the way, or is your organization of the view that there's enough to work with here, and it's just a matter of a suite of amendments?

Mr. David Elder: From the very beginning, back to Bill C-51, which initially proposed the SCISA framework, the CBA's approach has always been about making the necessary adjustments to that law to carry on. To the best of my knowledge, we've never addressed a question or pursued a position that would have favoured the outright removal of the legislation.

Mr. Daniel Blaikie: Given some of the risks to the privacy of Canadians that you've identified, given that it can take a long time to draft amendments, do you think there's a significant risk to the privacy of Canadians in maintaining this framework while trying to figure out what a better framework would be, and that therefore it might make sense to try to dispense with this particular bit of legislation so that the Privacy Act can do its job while government figures out how to enact other types of changes to the information-sharing regime?

Mr. David Elder: To clarify that I'm speaking on behalf of the CBA, I think it's clear that the CBA thinks there are a number of material concerns with the law as it's currently enacted and that there's potential for abuse. There's potential for information sharing that I think threatens the privacy of Canadians. If that were to continue as is for a lengthy period of time, I think it would be problematic.

Again, as an organization we haven't addressed the issue about having the law repealed, but we have put forward, both in my remarks today and in the position paper we left you, a number of places where adjustments could be made to significantly narrow the focus and the subsequent scope of use of the information.

Mr. Daniel Blaikie: Ms. Tribe mentioned in her opening remarks the recent executive order by President Trump having to do with not having U.S. privacy law extend its protection to non-American citizens. From any of you who care to answer, I'm wondering if you think there is a way to work in reasonable legislative protection for information, either to this statute or to some other law governing the sharing of information practices.

If information is being shared between departments and one department doesn't have a mandate to share that information with some other country that may not have the same protection for Canadians' privacy, but a statute like SCISA allows that information to be transferred seamlessly to another department that does, do you think there are reasonable ways within the law to afford Canadians some protection from other governments with which we would want to share information for specific purposes? Once that information has left the border, so to speak—which is a funny way to speak when we're talking about technology and information sharing, because it doesn't know those borders—is there some reasonable way to try to incorporate protections for Canadian citizens into our own law, or is that information out of our hands once it is shared?

● (1625)

Mr. David Fraser: How exactly you would do that is a very complicated question. A lot of effort went into looking at what happened to Maher Arar, for example, which was triggered by the sharing of information with the United States by Canadian law enforcement and national security agencies, and the consequences of that. We've had discussions about Canada not wanting to participate in or condone information-sharing practices related to torture, for example.

That is such a big picture and such an important question. It's actually outside the scope of SCISA, because a whole lot of information sharing that happens with the United States—and our other allies; it's not just the United States—happens outside the ambit of SCISA and any particular statute. Nothing in the Privacy Act, for example, limits the disclosure for those sorts of purposes, so that would merit a study entirely of its own within this committee.

At least where it touches on SCISA, I understand as part of the study you will be hearing from folks from the RCMP and CSIS and the Communications Security Establishment. I would ask them specifically what information has been shared within departments since they've had this ability under SCISA that they couldn't share before. What amount of that information has crossed the border? Once you have that information—and as parliamentarians you can require a witness to answer such a question—you're going to be in a much better position to understand what's going on. However, I don't expect you're going to get a straight answer.

Mr. David Elder: I will jump in and add my two cents.

To build a bit on what David said, I agree that it's certainly a complicated question. I think there are inherent limitations in the ability of domestic legislation, obviously, to govern what happens to information once it's in the hands of other sovereign governments. That has always been an issue.

There are at least a couple of things that traditionally we've done. One of them David alluded to, which is being careful with who we share things with and being careful with how much we share. Part of that involves some understanding of the nature of the foreign governments, the way they operate, and the type of civil liberty protections they offer to their own citizens as well as to foreign citizens. We can be somewhat choosy in how we share, with whom, and how much.

The second thing that I think Canada has traditionally done is through the treaty process. We'll have treaties with various governments that will help govern how information is shared, pursuant to procedural safeguards, etc.

The Chair: Thank you.

Ms. Tribe, you wanted to add something.

Ms. Laura Tribe: Yes. I agree it's a huge concern, but there were very weak protections for Canadians' data that went cross-border to the U.S. in the first place. Some of the problems with that executive order actually have to do with data transmitted through the Internet that the NSA would intercept itself. It wasn't necessarily given from the Canadian government.

I think there's a much bigger question around how we work with our partners to ensure that our data and our citizens' data is protected, as well as those agreements we make up front. If we're going to enter into information sharing, what are the provisions that we need and the guarantees for our own citizens?

The Chair: Thank you very much.

We now go to Mr. Saini for the last of the seven-minute round.

Mr. Raj Saini (Kitchener Centre, Lib.): I wanted to pick up on that point of information sharing, especially with the concept that Mr. Elder raised about subsequent disclosure.

We've raised the issue about the Five Eyes. We may have bilateral agreements with certain countries about information sharing. We may even have agreements with multilateral organizations like the Five Eyes. The question I have is, what recommendation can we make for the situation that occurs if we pass on information to one of our multilateral partners with whom we have a solid agreement, but that country or that entity has an agreement with a third country that we may not have a direct contact with?

On our part with the recipient country, we have a very strict and a very coherent protocol governing how to share information. What happens if that country has an agreement with another country that we do not have an agreement with? How do we protect that information from being sent over? How would you guide us? What kind of recommendation should we make?

● (1630)

Mr. David Fraser: I would suggest it's exactly as Mr. Elder referred to. It's a matter of trusting. You're going to have to trust. If you're going to enter into these bilateral or multilateral information-sharing arrangements, you're going to have to trust.

We can also put in place general limitations on what kind of information we share. What is the nature of the information we share? Also—and this is one of the things that might sound a little bit repetitive—what's the magnitude of the information we share? If the RCMP receives a query from the Department of Homeland Security regarding an individual that they have under investigation, that's a very different thing than giving the FBI full access to the Canadian Police Information Centre, which is currently the case. They're allowed almost unsupervised access to a massive trove of data. We don't have a whole lot of insight, accountability, or oversight, or even an understanding of what is happening with that information.

If it's on a case-by-case basis so that it's much more limited or it's much more controlled, then you have a much better sense of why they're asking. What's the nature of the information? Is it particularly sensitive? Is it something that's stigmatizing? Does it relate to, for example, religion or protected expression under our charter or all these other sorts of things? Shared databases and massive troves of information seem to be the trend these days. Instead of using knowledgeable investigative insight and individuals with the proper skills, they're throwing in technology, collecting a lot of information to create a haystack as big as they can, and then using technology to go through it looking for needles.

The problem is that the haystack is information about individuals who are 99.999% innocent. Technological scanning, for example, will produce false positives, will result in individuals wrongly ending up on no-fly lists and other things, or worse, ending up being tortured in a basement somewhere. That's what we need to protect. You don't share sensitive information that could cause harm to our citizens with somebody that you don't absolutely trust in terms of what's going to happen with that information.

Unfortunately, as Mr. Elder said, no Canadian law can tie the hands of any foreign government once they have that information. It needs to be a two-way street. It needs to be a relationship built on trust, but trust that's verified. Keep an eye on their track record. Has the information gone elsewhere? Be prepared to kind of pull back on the leash if there's any sign of trouble.

Mr. David Elder: Just to add to that, I certainly think our treaty arrangements and mutual sharing agreements with foreign governments can attempt to limit what those foreign states do subsequently with the information they receive from us, specifically preventing them, for example, from disclosing information they got from us to other states without our okay, or things like that.

The only remedy we would have when those arrangements aren't followed is to pull back on future sharing, or maybe there are other diplomatic channels and consequences to that relationship. Those are really the only things we can do if things go off the rails.

Mr. Raj Saini: If a country had to share that information with a third country, would you suggest that maybe a separate request be sent to the department, stating that a third country needed certain information and stating the reasons? That department here would make another analysis or another decision as to whether the information should be shared or not. Would that be something you think would be prudent?

● (1635)

Mr. David Elder: I certainly think that is a mechanism that might help. I think, as a country, we wouldn't want information shared indirectly with countries that we wouldn't otherwise have shared with directly.

Mr. Raj Saini: The second point I want to raise, and this is part of your CBA submission, is that some of the departments that are mentioned under SCISA have the power to compel, to receive information.

What could happen—and this is where I want guidance, advice, or recommendations from all three of you—is that if you have one department that has the ability to compel information through a warrant or something else, they receive that information, and then another department that does not have that ability would ask for that information and receive it. That department would be receiving that information indirectly, as opposed to receiving it directly like the other department.

What advice would you have to make sure that this information is handled in a suitable manner?

Mr. David Elder: I guess there are two thoughts on the subject, and thank you for the question, because it is something we didn't address maybe as explicitly as we should have in the position paper.

I don't think that CBA was ever considering a situation in which another department would ask for it. I would say that right from the get-go, there should be a restriction on that. If you're a department asking another institution for information that they've obtained through extraordinary powers, I don't think that should be permitted.

I think our comment was more on the other scenario, in which the institution that has those powers gets information that they believe would be relevant to another institution. Our submission was that the information should only be handed over to that other institution if it's very clearly necessary to allow that other institution to fulfill its functions that relate specifically to national security.

Mr. David Fraser: I think it's a very interesting question. It raises the spectre that I didn't even think of as well, which is essentially information laundering. I'm actually a little ashamed, because I'm usually pretty good at worst-case scenarios.

In an example like this you could—I don't know, but maybe this is one of those movie plot theories—imagine a scenario in which, for example, CSIS goes to the RCMP and says they would like to have all the recordings the RCMP have made of communications they intercepted with a warrant. Now, the RCMP can't make collateral use of that, likely because of the conditions in the warrant. However, as soon as CSIS has it, which they can do under SCISA, they're not subject to those restrictions; they're subject to their own kind of restrictions.

You could, in fact, by moving information from one department to another—which is completely allowed under this—change the nature of the protection of that information or lift those protections. That section 9 that I referred to would remove any civil liability for doing that, and that could be troubling.

Yes, I'm going to lose sleep over that.

The Chair: All right. We'll get on with the meeting, then, so that we can get to bed earlier.

Go ahead, Mr. Kelly.

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

I'd like to continue with you, Mr. Fraser, and maybe get some further clarification of what you discussed in your opening remarks, and maybe even in your answer to Mr. Saini's question.

You've characterized SCISA as a blank cheque facilitating the collection of bulk data and the exchange of bulk data, seemingly without any limitation. We've had a lot of discussion about the correct threshold for information sharing, and the criticism of SCISA that many have raised is that conduct that undermines the security of Canada is too low a threshold and that the bar ought to be set higher. It is, nevertheless, a bar.

You gave hypothetical scenarios in which people's charitable donations to religious communities were combined with who visits prisons and who crosses borders. None of that sounds like anything that would meet the stated threshold of undermining the security of Canada. Explain how SCISA, with such a threshold built into it—whether too high or too low, it is, nevertheless, a threshold—really is this sort of blank cheque to collect any and all data in bulk and to transmit it to any of these 17 organizations.

● (1640)

Mr. David Fraser: I'm happy to answer that.

Part of it relates to the question of relevance: what is relevant to investigations related to activities that undermine the security of Canada? Relevance is a very low threshold. If you're going to tinker with it, I would adopt “necessary”, because that's stricter.

Another problem is going to be that there's no oversight. There's no mechanism by which you can test whether or not something is, in fact, reasonable; reasonable is in the eye of the beholder.

Then also, we're now in the 21st century, when investigative means aren't simply following up leads but are analyzing databases and taking massive amounts of information and running them against algorithms in order to try to make information surface. If you are investigating to try to find the next person who's going to commit murder in a mosque, for example, if you have the mindset that the best way to do that is to analyze massive data sets because doing that is relevant to dealing with situations that would undermine the security of Canada, you can justify that in that sort of circumstance. When your mindset is that you operate by analyzing bulk data sets, then you can very easily see and connect those dots and take something that way. It might not have been the intention, but in this day and age, that is how a lot of investigations and a lot of intelligence work are being done, so we need to have the limitations that are in it.

As I said, I'd be happy to have the whole thing thrown out and rewritten and to have these things dealt with in the Privacy Act. The four recommendations made by the Canadian Bar Association would dramatically improve it, but we need to have the proportionality in it. It's the use of bulk data that troubles me the most.

Mr. Pat Kelly: I understand that two of you have quite clearly recommended scrapping it. I'll ask a question that may be aimed more at tweaking than scrapping.

Mr. Elder, how do you think oversight would work? The commissioner's recommendation is for independent oversight for all government bodies that receive information under SCISA. What do you think that would look like? Comment on the cost and manageability of workload. What would a proper body to oversee the listed recipients look like if we were to continue to have an information-sharing system similar to SCISA?

Mr. David Elder: Well, I can say we haven't done a full budgeting workup of what that would look like or those costs, so I'm not in a position to tell you today that it's going to require so many employees or that there's going to be an annual budget.

What I can say is that I think for that to work, a couple of things have to happen. One, as we said in our submission, is that it's really important that the institutions involved in information sharing—both those disclosing and those receiving—have to keep records of what's going on. I think it would be desirable for there to be some kind of regular reporting function between those institutions and whatever governing body or oversight body is created. I think it makes sense that the oversight body would have powers to investigate and compel production of information, potentially audit-like powers.

That's probably all I'll offer you at the moment. I'm sorry I don't have further information.

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

We'll go to a five-minute round now, beginning with Mr. Dubourg.

[*Translation*]

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

This is the first time I've been on the Standing Committee on Access to Information, Privacy and Ethics. Let me salute the members of the committee and tell them that I'm very pleased to be here and to work with them. I also acknowledge the witnesses who are here with us. My apologies for being late for the meeting.

I'm very interested in this topic, so I have a number of questions that I would like to just throw at several of you.

My first question is for you, Mr. Elder.

I looked at the brief that was submitted. Schedule 3 of the Security of Canada Information Sharing Act lists 17 federal institutions that are authorized to exchange information. Pursuant to which section of the legislation, should we allow the information sharing between those institutions? In your view, are there too many authorized institutions? Can you also tell me which aspect of national security comes into play for each institution? What do you suggest that we correct to ensure that only the institutions mandated to receive that type of information are authorized to do so?

● (1645)

[*English*]

Mr. David Elder: Thank you very much for your questions.

To your first question, on whether there are too many, I think part of the issue is that we don't really know. That's because for a number of these listed institutions, it's not obvious—to me, anyway—exactly what their responsibilities and authorities that relate to national security are. For some of them it's a bit more obvious; for some of them it's not obvious at all.

That's exactly why we recommended that as part of this you not only identify the institution but you also explicitly identify the sections of their legislative mandate that would clearly relate to some authority over the protection of national security.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

At one point, you talked about the reliability of the disclosed information that an agency can gather. What did you mean by that?

[*English*]

Mr. David Elder: I guess what we're really talking about is accuracy. There are general provisions right now in the Privacy Act for all government departments that any information they're collecting, using, or disclosing should be reasonably accurate and that they should take steps to ensure that it is.

Our particular concern stems from the tragic case of Maher Arar. From information that turned out to be inaccurate and that may not have been adequately vetted before being handed off to foreign governments, we wound up with a Canadian citizen being detained and tortured, with all kinds of horrible things. That's really the worst-case scenario, and it's a great reason for being really careful with the information we're sharing, particularly when it is being shared with a foreign power.

[*Translation*]

Mr. Emmanuel Dubourg: I have one last question, and it's still for you, Mr. Elder.

Do you think there should be records of all the information sharing between those agencies? Also, should parliamentarians have access to those records?

[*English*]

Mr. David Elder: Well, definitely, in accordance with our position, we think those records should definitely exist, because without those records it's very difficult for anybody to have any kind of oversight to check up on exactly how the law is being implemented and what information is being shared.

In terms of access, certainly they should be accessible by whatever oversight body is tasked with that oversight. As to whether they should be generally available to all parliamentarians, I think that is a more difficult question that I'm not sure I can answer now. Obviously there will be puts and takes to that. On the one hand, it will be extremely sensitive information, in many cases. You'd need to have very clear security protocols and clearances and that sort of thing.

● (1650)

The Chair: You can come back if we have more time, Mr. Dubourg. We're over the five minutes.

Mr. Emmanuel Dubourg: It's so quick.

The Chair: Things happen fast at this committee, sir.

Mr. Kelly, you have five minutes, please.

Mr. Pat Kelly: Thank you.

We had discussion earlier about Canada's relationship with its partners and allies. I heard agreement about from all of our witnesses that it is necessary to share information with allies, that the security needs of Canada require us to share information. It had been reported in earlier testimony at committee that Canada is by far a net importer of information. I don't remember the exact number, but the researchers would have record of it. I think it was something like a factor of 100 to one in terms of information that Canada receives in its sharing agreements.

To go back to this question of appropriate levels, I would assume it's reasonable to expect that Canada would have information-sharing agreements within government that are somewhat approximate to those that we rely on for information sharing in other countries.

Perhaps each witness could comment a bit on the reciprocal nature of sharing information with our international partners.

Mr. David Fraser: One of the challenges we are going to face, particularly when you look at the Five Eyes, is that Canada is one of five countries that are part of this. I think it will be politically difficult for Canada to act alone, because it ultimately depends on reciprocal information flows.

Mr. Pat Kelly: It would be inefficient, I would say, to act alone.

Mr. David Fraser: Well, certainly, and we would lose the advantage. For example, if Canada were to adopt a position that we were not going to play the bulk collection game and would instead play the targeted collection game so that we're not hoovering up massive amounts of information that's irrelevant or is about innocent people, and then the other four countries didn't play along, then I think that would be difficult. However, I do think the growing international consensus outside of the national security complex is that this is the appropriate thing to do.

I don't have any problem with police and national security agencies doing the things they do. I don't have a problem with the fact that CSIS can get a warrant in a federal court with a designated judge that can allow a CSIS agent to break into a house and secretly and covertly install bugs and things like that. They absolutely need those powers to deal with the sorts of situations they deal with. The concern is the disproportionality in the technological collection of massive amounts of information.

We're very much joined at the hip with our Five Eyes partners, but I think it makes sense for Canada to take a stand.

Mr. Pat Kelly: I'd like to give each witness a chance to comment.

Mr. David Elder: I want to make sure I understand your question. Are you asking if it's desirable that we have clear agreements with each of these international partners?

Mr. Pat Kelly: I didn't phrase it in the form of a question so much as giving each of you the opportunity to comment on the reciprocal nature of information sharing with our partners, and the necessity of it being a two-way street and having similar arrangements internally that our partners would have. I would guess that's an expectation that our partners would have.

Mr. David Elder: Yes, I would think so. We may be a smaller player within the Five Eyes in terms of our intelligence, but I don't think that means we lack any bargaining power and I don't think it means that we sign on to whatever the largest members of Five Eyes do and agree to all those procedures. However, I do certainly think it would be unrealistic to expect that whatever arrangements we agree to would not be mutual. That just seems unfair as a starting point.

Ms. Laura Tribe: On the reciprocal nature, with regard to Canada being a net importer of information, we're dealing with, for starters, four other countries giving us information and our putting out just this one country's worth of information. Just by the very arrangement of the Five Eyes alone, we will be importing more data than we're exporting.

In terms of the reciprocal nature, there are the realistic expectations of what we can get and then there are the reasonable expectations of what we should actually be expecting and demanding. They're not always easy or convenient conversations to have, but just because we're able to get an incredible volume of information from the NSA, from the U.S., doesn't mean that we should be returning in kind just because that's the expectation that has been set for us.

I think there's a really principled stand that we keep hearing our community saying is really of concern.

● (1655)

The Chair: Thank you very much, Ms. Tribe.

We now move on to Mr. Erskine-Smith, please.

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

I want to start with the definition of "activity that undermines the security of Canada" and get your views on whether we ought to maintain that definition or have a stricter definition.

I'll start with Mr. Fraser.

Mr. David Fraser: When you look through each of the individual clauses, it makes a whole lot of sense and hangs together, and certainly—

Mr. Nathaniel Erskine-Smith: It wouldn't be of concern that it's non-exhaustive?

Mr. David Fraser: I think that's something to be mindful of, and there are other kinds of limitations that talk about and are related to protected expression and things like that, so certainly it fits and is consistent within the whole scheme of the statute. I would identify the defects as being with the statute as a whole, rather than with just that particular provision.

Mr. Nathaniel Erskine-Smith: That provision is an incredibly important threshold, though, for information sharing, so it's actually, in my view, the only real protection we have, other than the relevance threshold.

Mr. David Elder: I don't think we have a particular issue with the scope of that section as drafted. To your question about it being non-exhaustive, I think it would be much more problematic if it were non-exhaustive, if it was just "including the following things" as an open-ended definition—

Mr. Nathaniel Erskine-Smith: That's what I mean. It is open.

Mr. David Elder: Well, I don't think it is; it's of these 10 or so factors.

Mr. Nathaniel Erskine-Smith: No, it's including these factors.

In any event, Ms. Tribe, do you have a view on this aspect?

Ms. Laura Tribe: We think the threshold of "undermines the security of Canada" leaves it open for a huge amount of interpretation. I know that there's a lot of talk about how things like protests and activism are excluded, but when you look at things.... In B.C., we're looking at pipeline protests, and that's the economic security of Canada. Does that count? If that threatens the idea of the security of Canada, whose interpretation is that? I think we're seeing a lot of people who are feeling quite silenced by this provision and think that the provision is not accurately worded in a way that protects us or our privacy.

Mr. Nathaniel Erskine-Smith: Getting to the other protection, which is the threshold of relevance versus necessity, Mr. Fraser, you indicated that maybe the government hasn't made its case.

We had an official before us who said there was a problem they were trying to tackle that was referenced in a 2009 Auditor General's report, which was that departments had information they thought might be relevant, but they were hesitant to disclose the information, perhaps, because it wasn't clear to them that it was necessary.

They reiterated—and perhaps the legislation should be a lot clearer—that the recipient institutions remain subject to their own rules. In the case of CSIS, for example, they remain subject strictly to a test of necessity, and it's only the disclosing institutions that are subject to relevance. Is that something we ought to make crystal clear in the law, given that there seems to be a lot of confusion?

Mr. David Fraser: Certainly certainty is a whole lot better than confusion, both in the way you referred to and in the example you gave of hesitation in handing it over when they probably were lawfully able to do that in the first place, and also in the possible broad interpretation of relevance.

For example, CSIS might have limitations in some of its provisions related to "as necessary". We've certainly seen how they interpreted that in the recent cases that have come out of the Federal Court. The RCMP doesn't have those sorts of limitations, and we have 14 other institutions , I guess, that are referred to in the act that would have different sorts of rules as well.

I do think that if you think necessity is too high a threshold, relevance is too low a threshold, and some—

Mr. Nathaniel Erskine-Smith: No, no. I'll cut you off just to maybe be clear about a proposal—not necessarily my proposal, but perhaps a proposal to fix this. If we clarify that the necessity standard is on recipient institutions, that the relevance standard is to disclosing institutions, and that when an institution receives relevant information that is not necessary to their mandate, they must destroy it immediately, would that be a fix that you would be comfortable with?

● (1700)

Mr. David Fraser: It's an interesting one. It is, I think, worth further discussion.

For the recipient organization, I think they should collect only the information that's necessary for their operations, the information that relates to their statutory obligations related to threats to the security of Canada. As an example, if there was a written request for particular information and the head of that institution, which is listed in schedule 3 of the act, certified that the information was necessary for their lawful activities, and each request was subject to scrutiny and oversight, it would be a very significant improvement on the act.

Mr. David Elder: I think it's particularly useful if it is restricted to just the head of the particular institution, and only that. The head of the institution has access to the information and makes the call.

The Chair: Okay, good.

Mr. Erskine-Smith, your time is up.

The last question of the official round goes to Mr. Blaikie, and Mr. Bratina would like to use up some spare time if we have any, and Ms. Shanahan as well.

We'll have Mr. Blaikie, and then we'll go to anybody else who would like to ask questions.

Mr. Daniel Blaikie: Mr. Elder has already weighed in somewhat on the question of what an appropriate oversight body might look like. It seems to me that's the linchpin for whether we stick with SCISA and change it somehow or throw it out. There will continue to be information sharing between departments, and the legislation that currently governs that might even be modified.

I'm wondering if the other two witnesses, Mr. Fraser and Ms. Tribe, want to weigh in on an adequate oversight regime for information sharing between departments.

Mr. David Fraser: I'll try to be brief, which is uncharacteristic.

Consistent with the other efforts that are going on related to oversight of national security generally and across the board, there is no common oversight of any of these 17 organizations, and all of them, apparently, are instrumental in our national security. All those functions should be overseen, probably by a parliamentary committee that has the ability to summon any information they want, and that committee should have absolute visibility into this. There should probably also be an additional committee, like the Security Intelligence Review Committee currently, that has the ability to go in and routinely do audits. It goes in and double-checks that all this is being done, because a parliamentary committee doesn't necessarily have the manpower to do that on a regular basis.

That would be my suggestion.

Ms. Laura Tribe: Can I add a plus one to that?

This really does exist in the bigger context of what's going on. I think it is really critical to have oversight over information sharing. The activities of each of those agencies is also something that.... What they do with that data once they have it, even if they collect it themselves, is something that we're really concerned about. That gets into things like the notion of "super-SIRC", which is beyond just the mandate of the Privacy Commissioner. It's great to have those SIRC reviews come through, but they're so far behind the actual activities as they're taking place that the amount of resources that need to be put into place for checking in and auditing those proactively and on an ongoing, regular basis, as Mr. Fraser was saying, is really critical. Finding out three years later that the CSE was giving away metadata of Canadians is too late. Being able to weigh in at the appropriate time or in a more timely fashion is really important.

Mr. Daniel Blaikie: Thank you very much.

The Chair: Colleagues, as per usual, we have a bit of time left over at the meeting, so I'll give priority to any MP who hasn't had a chance to ask a question.

I have Mr. Bratina.

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

Item six on the recommendations from the CBA is clarifying the interaction of the Privacy Act in SCISA. How about clarifying item six? Is it that the CBA thinks the Privacy Act should dominate? What are your views on that? What's the problem with how it's written within SCISA?

Mr. David Elder: Yes, we like the Privacy Act and the controls that are in place there, and I guess there seems to be a bit of confusion about how the two interrelate. The Privacy Act would generally be presumed to govern, but the Privacy Act has explicit exceptions for situations in which another law is applicable.

As well, you have section 6 in SCISA, which I call the “not my job” paragraph, because it really says nothing is either authorized or prohibited by this act, so you're left with this sort of tautology that, I think, would be beneficial to clarify.

● (1705)

Mr. Bob Bratina: Would you anticipate a problem in clarifying in terms of imminent national security issues if information is flying around because something bad may be happening and so nobody phones up the Privacy Commissioner?

Mr. David Elder: The concern here is that anything set out in the act in terms of the use of information can be covered off within the act. I think the main concern about the Privacy Act would be about further uses and disclosure, for which there aren't any restrictions in the law. You may have something that's disclosed legitimately in the interests of protecting national security, but it could be used for any other collateral purpose. I think that's why we really want to have the Privacy Act trump SCISA.

Mr. Bob Bratina: The government of the day was facing serious issues and created Bill C-51 and SCISA. Was it a rush draft in the fog of war? In evaluating the drafting of this legislation, I know we've heard many people say we should just get rid of the whole thing, but could it be worked on, from CBA's perspective?

Mr. David Elder: I won't speculate on how it came to be, but certainly from CBA's perspective, it could be worked on. It could be made a lot better in a way that would much better protect the privacy rights of Canadians.

Mr. Bob Bratina: Safeguards to ensure that any shared information is reliable are problematic for me, because.... Colin Powell said there were weapons of mass destruction. How would you envision the reliability being vetted?

Mr. David Elder: I guess that there is some vetting and that we're not passing on information that is rumours or hearsay. We're not repeating or forwarding fake news. We're doing some analysis and some checking on our own to make sure we're reasonably sure this is accurate information.

Mr. Bob Bratina: Thank you.

Thanks, Chair.

The Chair: Thank you, Mr. Bratina.

Mrs. Shanahan, welcome to the committee.

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you very much, Chair.

Thank you very much to the witnesses for appearing today. It's my first time on this committee, and it's always a good opportunity for us new MPs to learn about a subject that we haven't had much exposure to, except of course in the general media and the news.

One thing that does concern me is the notion of oversight and how that would take place. I think it came up in all three presentations that the key is how this information.... There is an acceptance by Canadians, and certainly I hear from my constituents that they're ready to share some information, as necessary, for national security, but who is going to be responsible for making sure that it's used responsibly?

The Office of the Privacy Commissioner brought up some concerns in its report in March 2015 with regard to some of the agencies listed having some oversight, while others did not. Can you share with me some more ideas that you have about what that oversight body should look like? Should it be in each of the agencies? Should there be one overall oversight body? What would that look like?

Mr. David Fraser: I would be broadly in favour of oversight over the entire national security and intelligence functions within the Government of Canada, which would include the law enforcement components as well. What we're seeing is that they all work as a group. When we have 17 organizations, some of which you'd think would have no national security role whatsoever, somebody has to have oversight over that.

I think that's absolutely critical, because most national security and intelligence activities are obviously top secret. Obviously they can't put all the information about what they're doing on their website. Because they are in the shadows, the only way you can make sure they conduct themselves in accordance with our expectations in a democratic society is to have confidence in the oversight, confidence that somebody is watching and keeping an eye on them, somebody who can keep the secrets but who can also blow the whistle when necessary.

I would suggest that it should be an officer of Parliament who has oversight and virtually unlimited powers of investigation, of her own initiative or in response to complaints, to deal with whistle-blowers and all that other sort of stuff over the entire apparatus. What's happened previously—and I think this is all part of the overarching discussion we're having on the green paper and everything else—is that, for example, the RCMP has been subject to one level of accountability, CSIS is subject to a different level of accountability, and CSE is subject to a different one, and I've no idea what's happening in some of these other departments. Nobody has a line of sight into the overall big picture other than perhaps the Minister of Public Safety, but even then, perhaps not. Somebody needs to be able to keep an eye on this.

The only way we can have confidence in it is by having confidence in the overseer. We have to trust that the overseer is acting on our behalf, because we, as citizens, can't have visibility into all of these things that really have to happen in the shadows. We're making a leap of faith, but we have to trust the supervisor.

● (1710)

Mrs. Brenda Shanahan: I thank you for that.

I saw Ms. Tribe nodding at certain points. Certainly with the new technology, it is a whole new world. Can you share with us some of your ideas about what that oversight body would look like?

Ms. Laura Tribe: OpenMedia hasn't put forward a formal proposal on what we think the oversight mechanisms should look like. The reason I'm nodding is that the real challenge we've seen is that having these disparate systems of oversight means there are different standards and tests and rules, depending on the department you work in.

We're starting to have the possibility for information to flow more freely among these departments. Having that bird's-eye view of everything that's happening and making sure that what is going where and the processes with which that's happening are really clear and having those checks and balances are really important.

To your question of whether there should be oversight within each individual agency, I think there can be that as well in making sure that each department is operating within its purview and making sure the information it receives and shares is being handled appropriately. There is a bigger picture, which Mr. Elder is getting to, which is understanding the big picture and how they all work together, particularly with such top secret information being shared.

Mrs. Brenda Shanahan: Thank you very much.

Is there time for Mr. Elder?

Mr. David Elder: I generally echo those comments.

At least from a SCISA perspective, for the 17 institutions that are listed—and for many more, because if put on the disclosing end, it could be any institution that is permitted under SCISA to disclose—I think there needs to be a single body that looks at all of that. I don't think that takes away from responsibilities within each of those institutions, however. I think there still has to be a clear accountability within each of those institutions to comply as well. We do need an oversight body that can look at the whole picture.

Mrs. Brenda Shanahan: Thank you very much.

The Chair: Thank you very much, colleagues.

Seeing no other questions arising from the members here at the committee, I just want to say thank you very much to our witnesses. This is very important testimony. This committee has been working very diligently on reviewing numerous pieces of legislation, and we've been working together very constructively and fruitfully. We've had two consensus reports already put before Parliament, and we're hoping that we can put forward another. Your testimony is very helpful in doing that. We appreciate your patience at the start of the meeting. We wish you well. If we need to get back in touch with you for further clarification, we know you stand ready to do so.

Colleagues, we're having a meeting again on Thursday, when we'll have more witnesses on this particular matter. I remind colleagues that I've allocated about 10 or 15 minutes at the end of that meeting just to have a brief chat about where we're going to go after that. We have witnesses with SCISA the following week as well, but we have to make some decisions about how far we want to take this and how much longer we want to continue with this study. Just keep that in mind, colleagues.

Thank you very much. We'll see you on Thursday

The meeting is adjourned.