HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 033 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, November 3, 2016

Vice-Chair

Mr. Joël Lightbound

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 3, 2016

● (1105)

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Good morning everyone. Welcome to the 33rd meeting of the Standing Committee on Access to Information, Privacy and Ethics.

Today we welcome Mr. Craig Forcese, professor at the Faculty of Law of the University of Ottawa, and Mr. Kent Roach, professor at the Faculty of Law and Munk School, University of Toronto, as well as Ms. Sukanya Pillay, executive director and general counsel of the Canadian Civil Liberties Association.

We thank you for being here.

I will give the floor to Mr. Forcese for 10 minutes. He will be followed by Mr. Roach and then Ms. Pillay.

Mr. Forcese, you have the floor.

[*English*]

Professor Craig Forcese (Professor, Faculty of Law, University of Ottawa, As an Individual): Thanks for having me here today.

Let me begin by noting that the topic of our conversation today, information sharing for national security purposes, is an essential one. Information sharing is essential to national security. That truth was recognized in the 9/11 commission report in the United States and it was also recognized in Canada by the Arar commission report, which was, in fact, an inquiry on how poor information sharing can precipitate human rights abuses. It was also recognized by the Air India commission, which was an inquiry into the systemic failure of information sharing.

In the presentation that Kent Roach and I have prepared, we aim to do two things. First, I'll identify the key challenges in national security information sharing. Then my colleague Kent Roach will outline suggestions on refining one core component of the governing law, specifically the Security of Canada Information Sharing Act, or the SCISA, an act that was part of Bill C-51 in 2015.

As a first point, Canadian information-sharing laws in the area of national security are a muddled patchwork. As an internal CSIS briefing note that predated Bill C-51 noted,

> Currently, departments and agencies rely on a patchwork of legislative authorities to guide information sharing....Generally, enabling legislation of most departments and agencies does not unambiguously permit the effective sharing of information for national security purposes.

The question is, however, what to do about this. The CSIS briefing note goes on to state that:

> Existing legislative authorities and information-sharing arrangements often allow for the sharing of information for national security purposes. With appropriate direction and framework in place, significant improvements are possible to encourage information sharing for national security purposes, on the basis [of] existing legislative authorities.

Instead, Bill C-51 responded to legitimate concerns about siloed information by throwing wide open the barn doors on information sharing, but in such a complex and unnuanced way that the only certain consequence will be less privacy for Canadians.

I'll enumerate now some of our concerns about the 2015 Security of Canada Information Sharing Act, the one enacted by Bill C-51.

First, the act allows those within the Government of Canada to share information about the new and vast concept of "activities that undermine the security of Canada". It is difficult to overstate how broad this definition is, even as contrasted with the existing broad national security definitions such as "threats to the security of Canada" in the CSIS Act or the national security concept in the Security of Information Act, Canada's official secrets law.

The only exemption of the SCISA definition of "activities that undermine the security of Canada" is for "advocacy, protest, dissent and artistic expression". This list was originally qualified by the word "lawful", but under pressures from civil society groups, the last Parliament deleted the word "lawful".

We were astonished by this change. We had proposed that "lawful" be dropped but then recommended the same compromise found in the definition of "terrorist activity" in the Criminal Code. We recommended excluding both lawful and unlawful protest and advocacy, but only so long as it was not tied to violence.

Violent protest or advocacy of a sufficient scale can be a national security issue, justifying information sharing. By simply dropping the word “lawful”, however, the new act seems to preclude new information-sharing powers in relation to any sort of protest, advocacy, or dissent, no matter how violent.

Government lawyers will find a way to work around this carelessly drafted exception. Indeed, the government's green paper has invented a solution. It says that the exception does not include “violent actions”. This is sensible, but it is not a standard set out in the actual law. It is a policy position, not something that is binding or in the least evident from the actual statute.

Second, the overbreadth of both the concept of security and the carve-out from it is then compounded by the operative provisions in the act.

In its key operative provision, the act contemplates that more than 100 government institutions may, unless other laws prohibit them from doing so, disclose information to 17, and potentially more, federal institutions if relevant to the receiving body's jurisdiction or responsibilities in relation to “activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption”. All these terms are not defined, even though they are capable of definition. Without definition, whether by amending the act or through regulation, there is a danger that many terms in the new act will be inconsistently applied—a danger that the Privacy Commissioner has already raised.

Third, in the absence of more carefully articulated standards, the only safeguard is that the new information-sharing power is, in subsection 5(1) of the act, “Subject to any provision of any other Act of Parliament, or of any regulation...that prohibits or restricts the disclosure of information”.

What that means is a bit unclear, but we believe that the existing act, the Security of Canada Information Sharing Act, must comply with, among other things, the Privacy Act. That is not an ideal safeguard, given the many exceptions in the Privacy Act. It is something, and yet we are not sure how to read the government's recent green paper documents. They say that because the new Security of Canada Information Sharing Act authorizes disclosure, it satisfies a lawful authority exception to the Privacy Act, effectively trumping it.

The bottom line is that the new act's entire architecture creates confusion and uncertainty, and this requires a remedy.

My colleague Kent Roach will discuss some of our proposals.

● (1110)

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

Mr. Roach, if you can hear us, could you please proceed?

Professor Kent Roach (Professor, Faculty of Law and Munk School University of Toronto, As an Individual): I'd like to thank the committee for inviting us and for allowing me to appear remotely. I realize this isn't ideal.

First of all, as someone who worked on both the Arar and Air India commissions, I want to underline what my colleague said. We need to get information sharing right, and this act, which was hastily and very poorly drafted, does not get information sharing right.

With the Arar saga we see the dangers of sharing information that is not reliable and is not strictly necessary for the mandate of a receiving institution. That underlines the extreme dangers that can come from too much or inappropriate information sharing.

Just as importantly, however, the Air India commission showed the dangers of not sharing enough information. Indeed, one of things that is absent from this act was a recommendation by Justice Major that there be mandatory information sharing by CSIS about specific information relevant to the prosecution of terrorism offences.

Rather than devising a system that focuses on a particular form of information sharing, what we see in the Security of Canada Information Sharing Act is section 2, which is a radical departure even from the broad definition of threats to the security of Canada under the CSIS Act, which has been with us since 1984. In terms of amendments, one of the first things that should be looked at is trimming the overly broad definition of section 2.

I would underline that for Canadians to have confidence in this information sharing, there need to be more limits in the legislation and also more transparency about the information sharing, because as my colleague has pointed out, if over 100 departments can potentially share information under this act with 17 or more recipient institutions, all of this is done through legal interpretations that the public has no access to. It's very difficult to ask civil society and the public not to have concerns, and indeed suspicions, about information sharing when we have such a radical, broad definition of “activities that undermine the security of Canada”, including not only legitimate topics like terrorism but also, for example, an activity that takes place in Canada and undermines the security of another state. In my view, it's very important to go back to section 2.

Section 4 of the act has a number of guiding principles, and these guiding principles are fine as far as they go, although I would like to see more emphasis put on the reliability of the information that is shared. Justice O'Connor in the Arar commission report stressed that there need to be assurances that the reliability of the information is discussed, and also the respect for caveats, which is mentioned in section 4.

The problem with section 4 right now is simply that principles are placed out there, but there are no teeth, unless there's a requirement for protocols through regulations or through amendments of the statutes. The Privacy Commissioner has also noted this.

As my colleague has noted, sections 5 and 6 are extremely poorly drafted. They need to be made precisely clear, because unfortunately the green paper reflects a fundamental ambiguity in how this act is going to be interpreted.

● (1115)

Certainly the interpretation that we thought was the viable one and the preferential one, which was that this act did not have an independent trumping force over the Privacy Act, is partly negated in the green paper. The green paper gives us some idea of how government lawyers are interpreting this legislation, and unfortunately the interpretation, like section 5 and section 6, is about as clear as mud, so it is very, very important to address those two very fundamental sections.

Also, we would support what the Privacy Commissioner has said, which was that the issue should not simply be sharing of all relevant information but that there should be some requirement of necessity. We would just add that Supreme Court jurisprudence, like the jurisprudence in Wakeling, suggests that information sharing—not simply information acquisition, but information sharing, such as is authorized by this legislation—is subject to the charter, and so a standard of necessity or proportionality would be much more likely to withstand charter scrutiny than one of mere relevance.

I would also underline again why this provision and the CSIS threat disruption are probably the two most controversial parts of Bill C-51 in their reference not only to detection, identification, and analysis but also to prevention or disruption, so I think it has to be made clearer that this does not expand the mandates of all of the recipient institutions.

In addition, again on the theme of why so many people in civil society are rightly suspicious about this act, section 9 provides a very broad immunity from civil consequences. Not only does this raise the spectre of allowing the sort of information sharing that harmed Maher Arar and many other people, but it also puts yet another barrier to getting civil compensation should information sharing—and in particular I would stress information sharing about security threats—impose harm on people who may very well want to seek compensation for it and who may very well want to restore their reputation.

Just because Mr. Arar's reputation, at least in Canada, has been restored, we should not forget that this was because of the extraordinary event of a public inquiry. Perhaps one of the most objectionable parts of Bill C-51 is that it allows a very broad, overly broad, permissive regime for information sharing. It does so in an unclear, poorly drafted manner, and it does not ensure that there be mandatory information sharing about that information that is most relevant to direct threats to the real security interests of people in Canada.

Thank you very much.

● (1120)

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Roach.

We'll now move to Madame Sukanya Pillay for 10 minutes.

Ms. Sukanya Pillay (Executive Director and General Counsel, Canadian Civil Liberties Association): Thank you for the opportunity to be here today.

The Canadian Civil Liberties Association is a non-partisan, independent, non-governmental organization that for 52 years has worked to protect rights and liberties and particularly to fight against injustice and wrongdoing. We support constitutionally compliant government action that provides effective security. I feel that this is an important context in which to begin my comments today.

We have serious concerns about the Security of Canada Information Sharing Act, which I will refer to as SCISA, and we are concerned by further confusions introduced by the green paper. I will outline five considerations here today.

First, information sharing is a critical component in countering terrorist activities, but such information sharing must be effective. This means that the information collected must be reliable and subject to constitutional requirements of necessity and proportionality and constitutional safeguards including caveats on use, retention, access, and dissemination. All of these, and legally enforceable provisions, are missing in the SCISA.

The scope of permitted information sharing is drawn from the definition in the act of “activities that undermine the security of Canada”, which we find to be astoundingly overbroad and which can capture all sorts of unnecessary and disproportionate information on legitimate activities, thereby effectively relegating Canadians to being potential suspects.

Further, the information sharing scheme superimposes vast information sharing on top of imperfect information-sharing structures already existent in Canada. In effect, there are 17 agencies, only three of which have any review structures, in over 100 departments. Again, this is information sharing with inadequate or non-existent review structures.

While we understand that the SCISA may have introduced some clarity for hesitating zealous officials who will now feel they have a green light to go ahead and share certain information, the scheme does absolutely nothing to ensure the reliability of the information or to ensure that constitutional principles of necessity and proportionality and the safeguards of caveats are observed.

Third, increased and integrated information collection and sharing powers are not matched in this act by increased and integrated review structures, and this is a serious concern for CCLA. Our country has witnessed the severe injustices of mistaken and faulty and even failed information sharing. Three federal commissions of inquiry—Arar, Iacobucci, and Air India—have provided observations and lessons that are not implemented or even, it seems, reflected in SCISA.

My second-last point is that SCISA engages section 7 of the charter rights of individuals. The definition of activities that undermine the security of Canada is unconstitutionally vague and can impact the security and liberty rights of individuals as found in section 7.

As the scheme is structured, violations can occur without the knowledge of an affected person, and even if there is knowledge, without an appropriate review structure there's nowhere to bring a complaint, given the absence of any one review structure with jurisdiction to review all the agencies empowered to share information.

In the past, government has stated that the Privacy Commissioner and the Auditor General have review powers, but their mandates and resources do not provide the jurisdiction and powers that would be required to properly review the information sharing that exists under the SCISA.

As CCLA has observed in its application, which is on hold before the courts, even the three existing review bodies for CSIS, the CSE, and the RCMP have no powers to compel the government to follow specific interpretations of the law. Further, the secrecy under which the sharing occurs renders any defence against illegal sharing illusory.

Finally, CCLA is seriously concerned that information sharing implicates section 8 of the charter as set out by the Supreme Court of Canada in its interpretations in Wakeling. SCISA permits a form of disclosure of information that is unreasonable within the meaning of section 8, and there are no checks and balances on such sharing.

Thank you.

● (1125)

The Vice-Chair (Mr. Joël Lightbound): Thank you very much to the three of you.

We'll now begin our first round of questioning for seven minutes, starting with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much to all of you for being here today.

Unfortunately, I only have seven minutes. I think I could use seven hours to ask the questions that I want to ask.

Let's start with something simple. This is for you, Mr. Forcese.

I read the paper that you and Mr. Roach wrote together, and I wonder if you could explain to me the difference between necessity, relevance, and proportionality. Could you highlight the differences and explain why you believe there should be a necessity test?

Prof. Craig Forcese: Relevance is the broadest concept, in the sense that information can be relevant but at the end of the day prove not to be material or tremendously useful. It's a broad concept. It's roughly analogous to the disclosure standards we demand of the crown for purposes of criminal prosecution.

Necessity dictates that you ask yourself whether the information that you're proposing be shared meets a materiality threshold. Is it material for the purpose of addressing this particular security concern? There's a more direct link, in other words, between the information and the security issue that you're trying to resolve.

At the end of the day—and this might be one of the concerns one has about these legal terms—these legal terms are subject to interpretation and construal within government. While we advance the idea and agree with the privacy commissioner that it's important to have more robust terminology that government lawyers and officials will interpret, at the end of the day it's also vital that there be an independent third party that is capable of scrutinizing the actual application. That would raise some of the issues that Ms. Pillay mentioned in terms of the accountability structure and review bodies.

Mr. Raj Saini: The second question I have—and I think all of you raised this point—is about the information being shared among 17 organizations and 100 different departments. You wrote about what you called the “privacy virus”, about how information held with one department gets spread around and then you want the information to be removed.

Can you elaborate on how we can make sure that once it has been decided that the information is no longer needed, it will be removed from all the organizations or departments that have that information? How would that work? I think that's an important concept.

Prof. Craig Forcese: It's very difficult, because information moves and is very difficult to track and can accrue in different places and different databases.

The accrual of information in the hands of different agencies is a perennial problem, so there are safeguards. The first safeguard is on collection, in that historically, privacy has been about restricting the capacity of government to collect information in the first place. Then, once it's collected, there's the issue of retention and use, so safeguards include limitations on how long information can be retained in a given database before it must be expunged, as well as information on how it can be used, and in “use” of information, we also include sharing.

Putting in place protocols that mitigate the spread of information through government agencies is probably the best we can do, coupled with effective auditing thereafter to ensure compliance and conformity with those dictates.

I suspect Ms. Pillay may also have some views on that as well.

Ms. Sukanya Pillay: Thank you.

I agree with everything that Professor Forcese has just said.

In addition to collection and retention and use, we're also concerned about access, and we're very concerned about what happens in the absence of caveat. If there aren't any written agreements as to how this information was collected and how it should be used and if there are no limits around how it's used and who it's shared with, once that information leaves the hands of A, it's effectively out of the control of A. As I mentioned at the outset, we're very concerned about injustices that can occur when a piece of information is mistakenly shared, or when, as in the case of Maher Arar, the information that is shared is full of error and innuendo that can result in serious harm to an individual.

I also mentioned, as did Professor Roach, the many issues that came up in the Air India inquiry, namely the concerns around information that was mistakenly withheld between agencies. None of that is properly addressed or cured by SCISA, nor is any illumination provided by the green paper.

● (1130)

Mr. Raj Saini: One subject area that you all mentioned was that this proposed act was built on a very overbroad concept of activities that undermined the security of Canada. I want to ask you about one specific aspect of that act, which states: “an activity that takes place in Canada and undermines the security of another state.”

Let me give you a personal example. Sometimes in my constituency office I have people who come from other parts of the world where they have repressive regimes, and they are trying to create a sense of opposition not only in Canada but in the country of their origin. Sometimes they may send money or information over to an organization there that's fighting for civil rights or fighting for freedom or democracy in that part of the world. How will that play out in that case? If that country makes a complaint that opposition is being formed here, even though it's a repressive regime, I don't understand how that's going to fall into the act.

Can you explain how you see that happening?

Prof. Craig Forcese: Does Kent want to try that?

Prof. Kent Roach: If people can hear me, I wouldn't mind quickly addressing that and one other point that was raised.

The concern would be paragraph 2(i), where if your constituent is doing an activity that takes place in Canada and undermines the security of another state, even a repressive state, there is a possibility that the information not only will be shared, but if you look at section 5, the criteria is relevance to, among other things, detection and prevention.

One of the concerns about relevance is that it allows data mining. That relevance to detection and prevention can include a vast range of information that on its own may be innocuous, but when combined with more information that is available through computer data banks can reveal quite a bit.

The last thing I would say goes back to what my colleagues have talked about, the importance of review. I think it's very important for this committee not to just look at this act in isolation. The absence of credible review for all of the institutions, combined with the fact that the government appears in the green paper to at least be seriously considering getting more data from metadata and other things feeds into what I would say is a justifiable lack of confidence that many Canadians have about how this information, once it is collected by one part of government, is going to be shared, stored, and accessed by other parts of government.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Roach and Mr. Saini. That's all the time we have.

We'll now move to Mr. Jeneroux. I would like to remind members that due to a technical problem, Mr. Roach is on mute, so if you have questions you would like him to address specifically, it's important to mention it.

Mr. Jeneroux, you have seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you so much, Mr. Chair, and thank you to both of you for being here today, and to Mr. Roach for being here virtually. It's appreciated that you guys take the time to do this.

Quickly, have any of you participated yet in the government's consultations on national security?

Prof. Kent Roach: Yes.

Ms. Sukanya Pillay: Yes. I participated in one consultation here in Ottawa, and my colleagues participated at an open mike in Toronto.

Prof. Craig Forcese: Yes.

Prof. Kent Roach: At the Munk School we've hosted one consultation, and we will be hosting another consultation later this month.

● (1135)

Mr. Matt Jeneroux: The most important part for any government is the protection of its citizens in balancing the various domestic and foreign threats, but protection of private information is also fundamental.

To all three of you, do any of you believe that there are any situations where the need to protect our national security might supersede that right to privacy?

Prof. Kent Roach: As I said in my opening comments, and also with Justice Major's recommendations, I agree about mandatory sharing, about intelligence, and about possible terrorism offences. That would be an example of a mandatory requirement as opposed to the permissive requirement, but it's a much more narrowly focused requirement than we see in section 2 of this act.

Ms. Sukanya Pillay: I completely agree with Professor Roach. I would just add that in addition to the mandatory sharing, as recommended by Justice Major, the principles of necessity and proportionality exist to allow for sharing when it's precisely that: when it's necessary.

Prof. Craig Forcese: It becomes a question of definition. The problem with section 2 is that the definition is so sweeping that it encompasses things that aren't bona fide national security issues. Essentially, privacy then becomes superseded by more extraneous considerations.

Mr. Matt Jeneroux: Okay.

The Government of Canada is a member of what's called the Five Eyes. Around the world, they work with these like-minded countries to thwart threats to collective national security. Do you believe these types of relationships are important to better protect Canadians?

Prof. Craig Forcese: Yes, absolutely. We're a net beneficiary of intelligence sharing. At one point, the RCMP was saying that it was receiving 75 times more information from allied services than it was sending out. We have to be cognizant of our place in the international information-sharing infrastructure.

These, in part, are some of the drivers around some of the other concerns that have been raised in other contexts about how we manage the flow of intelligence into, say, the court system, but that's a big, long story. The bottom line is that it's essential for us to be an active participant in that consortium.

Ms. Sukanya Pillay: Yes, I completely agree.

I would also point out that after the 9/11 attacks, the international community recognized that this needed to be done. In Canada, as Professor Forcese has just said, we have a certain place. We are a net recipient of this information, and it's important for us to rely upon it.

Having said that, we also know that there have to be checks and balances with respect to Canada's role in the Five Eyes, what it tasks its partners to do, and what it says it's doing here in Canada versus what's actually happening in terms of the relationship with the Five Eyes partners.

Prof. Kent Roach: As Ms. Pillay has said, information sharing is a modern reality. We should participate in it, but we need checks and balances in the form of an adequate review structure. Although the Privacy Commissioner obviously has some role here, if we had a dedicated national security review—if the activities of, say, SIRC, the Security Intelligence Review Committee, were expanded, as Justice O'Connor recommended in Arar—we would have greater confidence that the information sharing that must take place with our allies, both in and out, is done in as responsible a manner as possible.

The problem is that this act is silent about foreign information sharing. Even its operative principles do not actualize what Justice O'Connor said was important, which was that when we share information or receive information from allies, we should be cognizant of the reliability, lack of reliability, or, as is often the case with intelligence, unknown reliability of that information.

● (1140)

Mr. Matt Jeneroux: Are you three aware of the information sharing laws of our allies? Are there some that you have particular comments on?

Prof. Craig Forcese: Only in the broadest sense. The privacy rules in different jurisdictions are quite variable.

In relation to international information sharing, which was your prior question about Five Eyes, for the most part, there's relatively little law that I'm aware of within the Five Eyes that would govern that carefully and thoroughly.

On the other hand, one of the differences is that for the most part, the Five Eyes allies have more robust review and more comprehensive review. When you talk about international information sharing, the difficulty is always reconciling domestic review by domestic review bodies with an internationalized process that might implicate the interests of foreign states. I'm not sure that anyone has yet derived a perfect solution to that conundrum.

In terms of domestic privacy laws, they're quite variable. I would say that Canada, relative to some of the Five Eyes, has quite robust domestic privacy laws.

Ms. Sukanya Pillay: This is not just a plug, but based on your question, we have released just this week, with our international partners, a report on information sharing and surveillance. The CCLA has included a chapter in that report on the Re (X) case. The other partners who have written include information sharing laws in the United States, Russia, Kenya, South Africa, and India. We'd be happy to make that report available to you.

Mr. Matt Jeneroux: None of those countries is part of Five Eyes, though.

Ms. Sukanya Pillay: The U.S. is part of the Five Eyes.

Mr. Matt Jeneroux: Okay, I appreciate that.

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

That completes our seven minutes for Mr. Jeneroux. Now we'll go for seven minutes to Mr. Dusseault.

[*Translation*]

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

I thank the witnesses for being here with us today.

I'd like to go back to a point raised by Mr. Saini. He spoke about the possibility of sending information to foreign countries, which could in some situations compromise the safety of persons living in a country governed by a repressive regime.

Could there be some kind of safeguard for that type of situation? I am thinking for instance of information sent to Saudi Arabia by a Canadian who communicates with someone in that country. The safety of the person living on Saudi territory could be jeopardized if the leaders became aware of it.

Is there some type of mechanism that could prevent information being shared when it could endanger people in certain countries?

Mr. Forcese, what do you think?

[*English*]

Prof. Craig Forcese: I would say, in part, as I've noted, there isn't specific statutory law that would govern that sort of arrangement, and the current act that is the subject matter of today's hearing doesn't deal with international information sharing on its face.

As you may be aware, there are ministerial directives from the Minister of Public Safety dating from 2011 and directed at the Canada Border Services Agency, CSIS, and the RCMP that are designed to govern circumstances where there is a prospect that outbound information sharing could induce maltreatment or torture, and they also try to grapple with the prospect that inbound information sharing may be the product of torture.

The bottom line is that the ministerial directives put in place protocols to minimize those risks, but in truth, at the end of the day, the ministerial directives also leave the door open in the most dire circumstances to sharing if, at least in the views of the responsible officials, the risk of torture can somehow be mitigated.

The problem, of course, in all those circumstances is that you can't necessarily control what will happen in response to the information once it's shared. The Arar commission report took the view that even when there's a bona fide security reason, there will be circumstances when you have to decline to share, and that's probably the honest truth of the matter. It is an enormous moral and ethical dilemma that the law has difficulty reconciling.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you for that enlightening answer.

I'll stay with you, Mr. Forcese. Do you think that the Security of Canada Information Sharing Act was really necessary? The laws we had before, which are still in effect, such as the Privacy Act—were they effective enough to protect national security when information is shared?

Was this new law really necessary, or were things working well before?

● (1145)

[*English*]

Prof. Craig Forcese: I would describe the new law as an effort to wallpaper cracks in the roof. In other words, it superimposes a new legal regime on existing legal rules that are themselves an arcane patchwork and difficult to construe.

Just to give you one example, CBSA, the Border Services Agency, implements several statutes as part of its mandate, and these statutes each have provisions on information sharing in the interest of national security, broadly defined. However, they all use different terms and are drafted in different ways, so the same agency is applying different standards under different statutes.

If I were to make an overarching recommendation, it wouldn't be to create a Security of Canada Information Sharing Act that papers over all these cracks. It would be to go into the statute books of all these agencies and clean up all the differential rules that apply to govern information sharing.

I would also add that the Privacy Act itself has a number of exceptions that allow private information to be shared, including a public interest override. In circumstances where the agency takes the view that there's public interest in information sharing that supersedes the privacy interests of the individual, it can be shared.

In sum, it's not entirely clear to me what problem this act was trying to solve, other than to signal to government that we're going to share more.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you.

My question is for Ms. Pillay.

Regarding the issue of monitoring shared information, would it be appropriate to have more mechanisms for the surveillance of shared information? This is already being done, but could we do more to ensure that surveillance?

Could we do more to monitor the sharing of information, in order to ensure that government institutions respect the law as they should?

[*English*]

Ms. Sukanya Pillay: Thank you for the question.

I would absolutely say that more needs to be done, and obviously my two fellow witnesses are experts on talking about what can be done.

In short, as I've mentioned, we've called for an integrated review. A review would be different from oversight, as Professor Forcese has often said. The review comes after the fact, but it provides an accountability that's currently missing, and given that we have many of these agencies now working, as I mentioned already, in an increasingly integrated fashion, we need some sort of structure that can work in an integrated fashion to provide that review.

Then within agencies, I personally think that there ought to be some sort of—the translator's word was “monitoring”. There ought to be some sort of monitoring mechanism. There would have to be some protocols in place to govern what is being shared, and when, and why.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you.

If I have a few minutes left, I am going to speak to Mr. Roach.

On the issue of damages that could be paid to citizens who were adversely affected by an exchange of information, would it be appropriate to include a mechanism in our act, or a regulation or sections in the act clearly establishing that a citizen whose privacy was violated could be compensated?

[*English*]

Prof. Kent Roach: Thank you very much for the question.

I think this is an area that we should probably just leave to the courts, and I would favour simply deleting section 9 of SCISA. The Supreme Court is now developing jurisprudence with respect to charter damages, which would include damages for violation of rights of privacy. The court has done so in a way that recognizes a broad range of reasons for awarding damages, compensation for pecuniary and non-pecuniary losses, vindication, and deterrence, but is also respectful of governmental justifications. What the court says is that once you have established an entitlement to damages, it is up to the government to justify why damages would be inappropriate or why some alternative remedy would be better. In my view, subsection 24(1) of the charter provides a more flexible mechanism for responding to damages.

Having said that, I would also add that damages cannot be a substitute for effective review, because as Justice O'Connor stressed, most people do not know if information is being shared about them. Mr. Arar and other Canadians who were tortured in Syria, in part because of Canadian information sharing, knew because of the devastating consequences that they experienced, but you or I would not know right now if information about us is being shared, so although damages should be available, we should not rely upon damages, and we need a better review structure to do independent audits of information sharing practices.

● (1150)

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Dusseault and Mr. Roach.

We went considerably over our seven minutes, but it was very interesting.

I will now yield the floor to Mr. Erskine-Smith for seven minutes.

[*English*]

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

I'd like to start with replacing the overbroad definition of activities that undermine the security of Canada. Just very simply, to your knowledge, was there any adequate reason or justification put forward for why we moved away from the definition in the CSIS Act to begin with?

Prof. Craig Forcese: The only persuasive position I heard during the Bill C-51 debates was in relation, say, to weapons proliferation, weapons of mass destruction. Those sorts of matters could fall outside the scope of the threat to the security of Canada definition within the CSIS Act, so you would want to have a slightly broader definition to encompass those sorts of issues.

You could come up with something that's not as sweeping as the present definition in proposed section 2 that would address those sorts of bona fide concerns.

Mr. Nathaniel Erskine-Smith: Apart from that, if we limit it to threats to the security of Canada, that would be satisfactory, and perhaps we will want to add something specific to that concern. Okay, that's fair.

Ms. Pillay, just to go through Mr. Roach's and Mr. Forcese's recommendation with respect to mirroring the exemptions to the information-sharing regime in subitem 83.01(1)(b)(ii)(E) of the Criminal Code, the previous government removed the word "lawful". The proposal is that the exemption be expanded. Essentially with respect to advocacy, it would exempt anything not intended to endanger life, health, or safety. Would you be comfortable with that?

Ms. Sukanya Pillay: I think that I would probably share what I heard Professor Forcese say at the outset. We were very concerned when the word "lawful" existed, but then we were also concerned when it was withdrawn, because of the implications. At first we welcomed it, but then we were concerned about what the implications might be.

Mr. Nathaniel Erskine-Smith: Then we're generally on the same page there.

Walking through section 5, which is more complicated, as I understand it, it reads that a Government of Canada institution may disclose information if it "is relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament". First we would remove "relevant" and make it "necessary and proportionate". Would that be the idea?

Prof. Craig Forcese: Yes, and that, I believe, is the Privacy Commissioner's recommendation as well.

Mr. Nathaniel Erskine-Smith: Then we'd move to "or another lawful authority in respect of activities that undermine the security of Canada". That we would have already fixed with respect to section 2, and then, "including in respect of their detection, identification, analysis, prevention, investigation or disruption."

Mr. Roach, you'd mentioned clarifying section 5 to ensure that it must operate within its existing mandate. I wonder, are we worried about changing that specific language of "detection, identification, analysis, prevention, investigation or disruption", or would we add a subsection, a "for greater certainty" sort of thing?

Prof. Kent Roach: I guess my understanding of "detection, identification, analysis, prevention, investigation or disruption" is that they're trying to include every possible activity that at least the 17 recipient institutions engage in. Perhaps with the change to necessity and proportionality, there will be a bit more rigour here, but the outer reach, as I understand section 5, is really supposed to be defined by the enabling framework for each agency.

I think this goes back to what my colleague Professor Forcese said, which was that rather than trying to paper over and provide a one-size-fits-all solution in the act, in some cases it may be necessary to go back to the enabling statute. For example, if you believe—as I do—that the case has not been made for CSIS to have disruption powers, then that might influence how you would go about structuring that final clause in section 5.

● (1155)

Mr. Nathaniel Erskine-Smith: But faced with this particular act, if we add a “for greater certainty” clause, that might be sufficient if we're just looking to cure this particular act and the deficiency that you noted with respect to the existing mandates of the government institutions.

Prof. Kent Roach: Yes, that's true, but what I would say is we already have a “greater certainty” provision in section 6, which says, “For greater certainty, the use and further disclosure, other than under this Act,”—

Mr. Nathaniel Erskine-Smith: Yes, fair enough, so you may as well just delete—

Prof. Kent Roach: —and it hasn't exactly increased certainty, because Professor Forcese and I were a bit baffled and surprised when we read the green paper. This goes back to the fact that this act has been so poorly drafted that we need a more fundamental reworking of it.

Mr. Nathaniel Erskine-Smith: With regard to reviewing information sharing—all witnesses mentioned this—we don't have a particularly adequate review body to review information sharing between agencies.

Mr. Forcese, you mentioned the siloed nature of the three existing review bodies that we have.

In the previous Bill C-51 debate, my understanding is that an amendment had been put forward that would allow all information sharing to be submitted to the Privacy Commissioner for review. The Privacy Commissioner would issue an annual report to Parliament as to whether the information sharing was acceptable. I wonder if you'd comment on whether that proposal is adequate.

Prof. Kent Roach: If that's addressed to me, obviously the Privacy Commissioner needs and has said that he needs more powers.

One of the reasons we mentioned dedicated national security review is that, particularly with the foreign information sharing and also with the evolving nature of security threats, you need to have some specialized expertise to really judge the information sharing.

One of the Arar commission's recommendations was that some of the people in the RCMP who were sharing information were not adequately trained in national security. If the Privacy Commissioner were to be the sole reviewer of the information sharing, I would also want to see the Privacy Commissioner develop expertise in the particularities of national security sharing, particularly its foreign dimension.

Prof. Craig Forcese: I would agree with that.

The problem we have right now with our current review structure is that we have three specialized national security bodies that are stovepiped to three different agencies that are constrained in their ability to coordinate. Then we have the Privacy Commissioner, who has a limited subject matter jurisdiction across all of government. Trying to get those bodies to work together would require some substantial reweaving of the existing law, but more than that, we have to ask what we would accomplish at the end if we empowered the Privacy Commissioner to perform this siloed subject matter jurisdiction in relation to simply information sharing.

I would echo Professor Roach's comment that information sharing is going to be intertwined with operational considerations that are specific to national security, and having a dedicated national security reviewer looking at the information sharing probably is more advantageous than using the Privacy Commissioner.

Ms. Sukanya Pillay: I completely agree with that, and I think I said in my comments at the outset that the current mandate of the Privacy Commissioner, while extremely laudable, means that he is constrained, and there is only so much that he can do. To change that mandate would have other implications, and I would rather see an independent reviewer.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Vice-Chair (Mr. Joël Lightbound): That does conclude our seven-minute round, and we'll now move to the five-minute round with Mr. Kelly

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

I was surprised, and I didn't know quite what to make of the comment that came after an earlier question about the information sharing between the Five Eyes, as well as the statistic mentioned about the RCMP receiving 75 times more information than it shares outwardly.

It wouldn't have occurred to me to think of whether these sharing arrangements are beneficial to Canada, based on whether it's a net positive inflow to Canada or not. It made me think and wonder whether our allies, with whom we co-operate on law enforcement and national security matters, are concerned that Canadian security organizations don't share enough. Is that a concern that's been raised, or a concern that we should have?

● (1200)

Prof. Craig Forcese: That's probably a question that's best asked of people within government. I haven't heard that in my travels.

The relative volume also has a lot to do with the relative size and scope of the security intelligence community within Canada. That 75-times figure that I gave you earlier was an RCMP figure from an affidavit filed in a federal court case decades ago, so if anything, that number is probably bigger now. That wasn't with just the Five Eyes; it was more generically.

My sense is that Canada is a valued member of the Five Eyes. We leverage certain skills, aptitudes, and assets, and we make a contribution. The contribution isn't necessarily measured in absolute volumes. As to how we're perceived by partners, that's probably a question best asked of government.

That's the best I can do. I'm sorry.

Mr. Pat Kelly: Professor Forcese, in response to Mr. Dusseault's question about the necessity of the provisions of Bill C-51, were these necessary, or were existing laws in effect that were sufficient and allowed for sufficient sharing?

You mentioned the general override under privacy law, yet when a catastrophic crime such as Air India took place—and this was 30 years ago now—after the subsequent inquiries identified the failure in sharing between institutions, there was substantial outcry. In the event of a future crime of that scale, if it were discovered that law enforcement agencies had information in their possession but were unable or unwilling to share it, or feared to share it, I can only imagine the public outcry.

Sure, the public values privacy. We know that. We've heard that at this committee, and rightly so, yet the thought of law enforcement possessing information and failing to act on it would also be very upsetting to Canadians. If the override were good enough, I am not sure Canadians would agree with that. That act existed even 30 years ago.

Prof. Craig Forcese: The story behind the Air India issue wasn't about inadequate law but about operational practices.

As for the resistance to information sharing, first of all, the RCMP and CSIS are not really affected by the new act in terms of information sharing. Existing provisions that have existed for 30 years, as you indicated, allow for sharing information between those bodies. Frankly, this act does nothing to enhance or moderate or do anything for the information sharing between the RCMP and CSIS.

The question that is raised by your comments is why CSIS would resist sharing information with the RCMP, which has been a recurring issue as recently as the Toronto 18. That has to do with what is known as “intelligence to evidence”. CSIS is concerned that if it shares information with the RCMP, that sensitive information will be disclosable in court because of the scope of our Criminal Code and charter disclosure rules. It has nothing to do with this law. It has to do with the way we've structured this intelligence-to-evidence conundrum.

That is the reason the Air India commission recommended that there be a proviso putting in place a system for CSIS to disclose to a third party—they proposed a national security adviser—who would decide whether that information should be prioritized for intelligence purposes or for evidentiary purposes in a criminal trial. CSIS would not be making the decision at the end of the day. Someone outside CSIS would ensure that if there was a need for use in a criminal trial, it would be available.

This is Kent's area more than mine, so perhaps I'll leave him some room to talk too.

● (1205)

Prof. Kent Roach: Nothing in the Security of Canada Information Sharing Act requires CSIS, or indeed any other agency, to share information. This is a permissive regime. Without getting to the organizational, cultural, and legal difficulties that Professor Forcese has talked about, this is not going to guarantee, for a variety of reasons, that CSIS or CSE does share information that could prevent a potentially catastrophic act of terrorism. The government knew about Justice Major's very specific recommendation with respect to mandatory sharing, and that is nowhere reflected in this act.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Roach.

We'll move to Mr. Bratina for five minutes.

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

I've been going over the Chilcot report recently on the war in Iraq. In relation to information, it seems as if the old garbage-in, garbage-out regime existed and probably continues to exist. Is there anything in all the laws that we have, or in Bill C-51, that addresses the integrity of the information?

Prof. Kent Roach: The closest in this act would be section 4, which provides non-enforceable guiding principles. As I said in my original statement, it does not address the issue of the reliability of the information, which I think is what you are getting at with the reference to “garbage in, garbage out”.

Mr. Bob Bratina: Exactly. This seems to be the problem. However, the government of the day, in fairness, needed to respond to a public demand for a sense of more protection from things that were happening. We had the sad occasion at the National War Memorial as an example.

Mr. Forcese, in thinking over the actions of that day, is there anything within the legislation that we have or that is proposed that would have enabled a quicker response to that situation?

Prof. Craig Forcese: The honest answer to that is that we don't know. We have never had an accounting of the events of that day, other than some redacted reports from the police as to the security situation on the Hill. That can be juxtaposed with the Australian response to a similar incident in December 2014 and the British response to the murder of fusilier Lee Rigby in 2013, in which comprehensive reports were issued that looked at the landscape of security service actions and described where there were operational failures how they could improve.

In other words, we haven't done a “lessons learned”. That means it's next to impossible to look at the events of October 2014 and say definitively that if we had had this act at that time, things would have turned out differently.

My suspicion, based on what is on the public record, which is mostly journalistic accounts, is that the provisions of Bill C-51 were not responsive in any real way to the events of October 2014. I can't deny that in some of our work I've discussed how Bill C-51 not only overreacts in some of the ways we've discussed in terms of overbreadth, but also underreacts by not actually addressing the points that were raised in our last exchange about what caused the Air India disaster.

That is the awkward relationship between CSIS and the police, which means that we don't bring our A game to terrorism investigations. I like to call it “the tail wagging the national security dog in Canada”. The inability to reconcile those two agencies in terms of their information-sharing practices, I think, undergirds a lot of the workarounds that you see in various places in Canadian law, including Bill C-51.

The recommendation I would make to the current government is to fix that conundrum, much as the British have done between MI5 and the British police, which they did after the disasters of 7/7. Once we have fixed that, let's look and see whether there is a need for all these other measures that, on their face, seem so extreme.

● (1210)

Mr. Bob Bratina: We have a very high level of consultation right now on Bill C-51. What I am hearing is that there were already measures within the previous legislation that addressed issues of concern, so what should we do?

I'll ask you, if you were the king, how would you approach this? Can we set Bill C-51 aside and just work on filling the gaps, repairing the inappropriate definitions, and so on? What do you feel would be a good recommendation for us?

Prof. Craig Forcese: I'll take a stab at that, because I know that Ms. Pillay is going to have a view as well.

I think Prof. Roach and I would be in the camp of those saying that Bill C-51 was trying to address real problems but, as I've suggested, overreacted in some respects and underreacted in others.

In terms of what should be done, we have prepared a 37-page paper responsive to the government's consultation document and proposing some very concrete measures that have the effect of doing their best to renovate what's in Bill C-51 but also push the agenda on things like intelligence to evidence, which again we see as an undergirding conundrum for Canadian law.

We say fix the regime, because it was trying to address some real problems. That's not the universal view, though.

Mr. Bob Bratina: Ms. Pillay, go ahead.

Ms. Sukanya Pillay: Thank you.

CCLA has always taken the position that we didn't know why Bill C-51 was needed. We knew that we had had these tragic events. We all agreed that they were tragic, but we did not know what the gaps were in the October 2014 existing laws that Bill C-51 was remedying. What we do know is that Bill C-51 introduced a whole new set of problems, and very serious problems, and that's what we're concerned about.

I guess my summation would be that the open-wound problems we see in Bill C-51 need to be addressed. I would also completely agree with Professors Forcese and Roach, as they've said at other times, that the problems we have with respect to intelligence and evidence have to be addressed. It comes full circle, in a way, to the question you asked two questions ago and to what I referred to in my opening statement, which is that nothing in SCISA ensures that we have reliable information. If our goal is to keep Canadians safe and to protect against threats of terrorism and terrorist activity, we must have reliable information, and we don't have that.

We've referred in our submissions elsewhere to William Binney, who was a whistle-blower in the U.S. You've all heard this analogy before, but it's worth repeating today: if you're looking for a needle in a haystack, don't create more hay. I'm afraid that's what we've done, but it's not as benign as just more hay. There are also other problems.

Mr. Bob Bratina: Thank you.

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

[*Translation*]

Mr. Kelly, you have five minutes.

[*English*]

Mr. Pat Kelly: Thank you.

I'm going to continue in a similar vein and ask our witnesses to comment further on the various statutes and disclosures under certain circumstances.

I know that you both, Professor Roach and Professor Forcese, in your presentations mentioned that privacy law and information sharing is convoluted and patchy. Various statutes allow certain disclosures under certain circumstances, while others seem to limit them in similar cases.

What do you see as a way of reconciling disparate provisions in a comprehensive and reasonable regime? How would you launch a consolidation project to unite different provisions within one governing agency? Your analogy, Professor Forcese, is that it is wallpapering over cracks. You've made some comments already on this, but I'll allow you to continue on how you would rebuild rather than wallpaper or paint over.

● (1215)

Prof. Craig Forcese: That's a hard question, because it means going through a lot of statutes, and it's a lot of work. I would be hoping that the Department of Justice would help.

I'll give you an example within the context of the concept of terrorism, which obviously is a pertinent one for this conversation. There's a definition of something called “terrorist activity” in the Criminal Code. There's the concept of a “terrorism offence” in the Criminal Code. The Security of Canada Information Sharing Act talks about “terrorism”. The Immigration and Refugee protection Act talks about “terrorism”. Some of the provisions that relate to CBSA talk about terrorism-related activities. In other words, there's a proliferation of terms, and some of those terms, when they're applied in the context of actually ending up in front of a court, have been interpreted differently. The concept of terrorism in the immigration law has been construed differently by the Supreme Court from the definition of terrorist activity in the Criminal Code.

Imagine now that you have all these different terms, and you're the official who's trying to decide whether you should share information because of the invocation of terrorism in the Security of Canada Information Sharing Act. Which definition do you choose? My preference would be to have a consolidated definition of all the issues we think should fall within national security, one that is significantly less broad than what's presently in section 2, and to make sure that it becomes the hub in a bigger wheel. It would be the hub for the information-sharing provisions that exist in other statutes, so it would be a consolidated definition. That requires a lot of renovation, though, of the existing statutes, and that will be a lot of work, but it's probably a worthy endeavour, because I think it would simplify life.

I'll reiterate one of my core points at the outset, which is that even with the best legal language in the world, you're still dependent on people construing it, which means that you need independent review to ensure that those construals are reasonable.

Mr. Pat Kelly: Do you want to answer, Ms. Pillay?

Ms. Sukanya Pillay: I defer to Professor Forcese on this. I would say that I agree with him and just add that—this might be radical—I don't think we need to reinvent the wheel. We definitely need to have a consolidated definition.

When I say that we don't need to reinvent the wheel, this is something that has also been tackled elsewhere. We have had some thought given to it by the Supreme Court of Canada in Suresh, but we can also look to international laws in terms of how they have defined “terrorism” and “terrorist activities”.

Mr. Pat Kelly: Do we have time for Professor Roach to comment?

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

Prof. Kent Roach: In echoing that, I would add that no legal language is going to be perfect, but that's where the issue of integrated review comes in. I would hope that here a solution from the ground up would match information sharing with review, which I take to be the underlying principle that Justice O'Connor relied upon in the Arar commission.

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

We'll move to Mr. Long for five minutes.

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

Thank you to our guests for coming in today.

Obviously, as Canadians, I think we do want to find that balance between security and civil liberties. We are in a new era in which we have to wait longer at airports and so on and so forth, and I think we're all prepared to do that.

I've done a lot of reading on this over the last couple of days. A constitutional lawyer, Paul Cavalluzzo, said in an article that Bill C-51 is so flawed that it should just basically be blown up or should have many, many amendments. Do you agree with the statement that Bill C-51 should just be blown up and we should start from scratch?

Ms. Sukanya Pillay: I have an idealistic and a practical response to that. My idealistic response would be yes, that would have been great, and that's what we argued for when we had hearings on Bill C-51. My concern, though, is that we have an act in place now that's been operational for over a year, so how can we practically remove it?

I certainly do agree with the underpinning philosophy of Mr. Cavalluzzo, but I don't know where we are today. I think what we need to start with today are the serious problems that have been identified in our conversation this morning, including such things as a consolidated definition, such things as intelligence and evidence, and, very particularly, what I said in my opening statement with regard to the specific concerns in SCISA, where we have a definition that's overbroad, nothing in that act that ensures we have reliable information, no legally enforceable caveats, and two open potential charter land mines with respect to sections 7 and 8. If you're looking for practical fixes on this particular piece of legislation, I would say to please start there if you can't get rid of it altogether.

● (1220)

Mr. Wayne Long: Thank you.

Professor Forcese, would you comment?

Prof. Craig Forcese: I would be more surgical in terms of the analogy to blowing up Bill C-51.

I think there are aspects of Bill C-51 that don't stand either a constitutional or a reasonableness test. The new speech crime of promotion and advocacy “of terrorism offences in general” is so sweeping that it encompasses speech that is potentially quite far removed from actual violence. There's no justification for it. Also, I think it underappreciates the extent to which speech that is closely affiliated with violence is already a terrorism crime under 15 or 14 existing terrorism crimes that existed before Bill C-51.

There are other aspects that are more complex, though. Take, for example, the CSIS threat reduction powers. You'll have different views on this. I am of the view that a case can be made that CSIS should have the capacity to act kinetically in limited circumstances —that is, to do more than be a watcher. How you craft that, though, is very different from the way it's been crafted in Bill C-51.

The other limit presently in Bill C-51 in terms of the circumstances in which CSIS can act is quite extreme. The prospect that CSIS, with a Federal Court warrant, could violate the charter is anathema to our constitutional tradition. More than that, it isn't actually responsive to the sorts of practices that one sees in other jurisdictions where they have deployed threat reduction successfully.

In the U.K. context, threat reduction by MI5 is generally spearheaded in a manner that facilitates criminal trials. Disruption in a U.K. context, based on what's in the public record, typically is that they make sure this person is arrested for not paying their local taxes. They may have a terrorism fear, but they can't act on it, so the police will bring a bona fide prosecution on some other grounds. Therefore, that's disruption. The criminal justice system is closely twinned there.

We haven't forced that twinning in the way that Bill C-51 has been crafted. The fear that Professor Roach and I have is that it could actually prove counterproductive. CSIS threat reduction could be counterproductive to a criminal law solution to terrorism.

Mr. Wayne Long: Thanks.

I want to briefly talk to Bill C-22 and the oversight to get your opinions. Do you feel that Bill C-22 is adequate? Do you think that with parliamentarians having oversight of something like that, there's the expertise, experience, and resources to provide adequate oversight?

Ms. Sukanya Pillay: I think having a parliamentary committee would be a welcome move in Canada, but it is not a substitute for an independent reviewer of national security issues, so the two have to work together. Second, I think that Bill C-22 has ineffectual review, because at the end of the day there's discretion in terms of what can be withheld from the committee. That effectively undermines the whole objective, so that's problematic.

If I may add one thing, when I responded to Bill C-51, I stuck to the CSIS Act, but there are many other things with respect to CSIS, such as the references to the IRPA and the no-fly list, that I think need to be done, and they would also be very quick fixes.

Mr. Wayne Long: Okay.

Prof. Craig Forcese: In the interest of full disclosure, Professor Roach and I are doing a doubleheader today. We're up in front of the standing committee on Bill C-22. Those thoughts are in the can, so to speak.

I would say that Bill C-22 provides a necessary remedy: that is, investing parliamentarians, for the first time in Canadian history, in a national security review function. That said, I would echo the concerns about the scope of information disclosure. It's not just that the government can, in certain circumstances, decline to provide information; there are actually mandatory exclusions, which are actually quite unusual as compared to our Five Eyes partners.

In the U.K. the exclusions of information are discretionary, and there's a protocol that the executive branch and the parliamentary committee have negotiated that says that those exclusions will only be used in the rarest of circumstances. In other words, they won't exercise their discretion to deny information.

In our system there's a whole cadre of information that will be ultimately excluded automatically. I would add that among the information that will automatically be denied the Bill C-22 committee are ongoing law enforcement investigations. It sounds sensible, except when you consider that the RCMP currently still has an ongoing investigation into Air India.

● (1225)

Mr. Wayne Long: Right. Thank you.

Thank you, Chair.

The Vice-Chair (Mr. Joël Lightbound): I will now move to our last questioner, Mr. Dusseault, for three minutes.

[*Translation*]

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

I am pleased to be able to go back to a few points.

My question will be about whether the Privacy Act takes precedence over other legislation. That was mentioned by Mr. Forcese.

If I understood correctly, when the Security of Canada Information Sharing Act was passed, it was considered to be on an equal footing with the Privacy Act. But finally, the Minister of Public Safety and Emergency Preparedness stated in his National Security Green Paper that the Privacy Act takes precedence. Unless it was the opposite.

Can you correct me if I am mistaken?

[*English*]

Prof. Craig Forcese: I think the situation right now is quite confused. Section 5 of the new act says that it's subject to other existing acts that constrain or control the disclosure of information, which would suggest the Privacy Act. The Privacy Act itself has an exception saying that where some other active statute authorizes disclosure, then the Privacy Act rules don't apply, so you get into a bit of a circle. The new act says subject to other laws, the Privacy Act says subject to permission in new laws, so which prevails?

The green paper implies that the government views the Security of Canada Information Sharing Act as a lawful authority constituting an exception to the Privacy Act, and so they've opted for an exit off the merry-go-round, but it's not an exit that you can predict from the wording of the statutes. Again, I think the best we can say about the drafting is it's very confusing, and that's just one illustration of how confusing drafting could be construed inside government. We wouldn't necessarily know how it's being construed, and so we're left with the prospect that an ambiguous law is given definitional rigour by secret legal opinions that we can never see.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you for that clarification. It was very instructive, once again.

I would like to go back to a point which was mentioned by several experts, as well as by the Privacy Commissioner, which is that expansive information sharing opens the door to federal government surveillance.

Does the Security of Canada Information Sharing Act contain new means the government could use to collect information, or does it simply provide a framework for information sharing?

According to certain experts, this could increase the surveillance of citizens by the government.

Can you confirm that the Security of Canada Information Sharing Act contains new powers allowing the government to collect more information than what was already permitted by law?

Perhaps Ms. Pillay could answer that question.

[*English*]

Ms. Sukanya Pillay: Thank you so much for the question.

I suppose I would go back to section 2 of the act. The definition of any activity that undermines the security of Canada is so overbroad that now we have a legislatively prescribed definition that's just opened it so wide that any information could, in the view of CCLA, fall under that definition.

I believe that SCISA now allows for more information to be gathered as well as more information to be shared, and all of it without any appropriate and necessary safeguards or review.

[*Translation*]

Mr. Pierre-Luc Dusseault: Do you share that opinion, Mr. Forcese?

[*English*]

Prof. Craig Forcese: I understand the government's view, which was taken during the Bill C-51 debates, that the new act doesn't authorize new collection, but it depends how you measure collection. Sufficiently broad information sharing allows for the pooling of information within the hands of one agency. The information that would not legally have been able to accrue in one agency is now available to it. Technically that's not collection in the sense that it's not been extracted from outside of government from an individual, but rather it's the amalgamation of information in a database in the hands of an agency.

Then the question becomes what the agency can do with that new amalgamated database. Are there controls on the searches it can run through that mother of all databases? Are there provisions that guard how it can then be combined with public-source information to paint an intimate portrait of an individual?

In the world of big data, the boundaries between collection and use are beginning to blur because of the amount of information that is currently in circulation and easily extractable from the public domain. In the absence of safeguards on how information is amalgamated by an agency and then what it can do with that information, I think that we run the risk that the net result is that the government knows more about people than it would otherwise know.

● (1230)

[*Translation*]

Mr. Pierre-Luc Dusseault: Fine.

Thank you, Mr. Chair.

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

Since we still have about 30 minutes left, I am going to allow some supplementary questions from the members.

I see that Mr. Massé and Mr. Erskine-Smith want to speak.

Mr. Massé, you may begin.

[*English*]

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): First of all, thank you for being here as a witness to participate in the work of our committee. I know that there is a lot of work needed to prepare for being here as a witness.

I'm not a lawyer; I'm just a new MP who used to run different organizations in the past. I'm not a specialist on the question either, but you used strong words throughout your presentation about Bill C-51. You said it was carelessly drafted, poorly drafted. You used an expression like trying to use wallpaper to cover a wall that is cracked.

It raises the question of why this happened. Was it a reaction to something that happened? Did we try to react quickly? Was it drafted quickly? Did the previous government provide poor direction?

The second question would be about what lessons we learned. If you tried to identify two or three lessons learned, could you say what those would be, so that we could avoid such situations?

Prof. Craig Forcese: I'm going to duck the first question, about why it happened, because that would require me to make a political judgment, and I'm no more qualified than anyone on the street to make that political judgment. The honest answer is that I don't know why it happened. There are probably a number of reasons.

Your second question is an important one. These are real issues. National security is an acute issue. How we grapple with it is an acute issue, both legally and operationally. One of the difficulties we have in Canada is that we're not sufficiently discursive on it; that is, the expertise in the area tends to be monopolized within government. Government tends to be close-lipped on national security issues. There is no diffusion of expertise, because we don't have a conversation, or at least up until this point we haven't had a conversation.

One of the things both Professor Roach and I said in the aftermath of Bill C-51 was that aside from whatever you think about the merits of Bill C-51, we can't have a process like this again. We need to have a more premeditated policy discussion. I think the idea of a consultation process in national security, which we've never had before, is a very valuable one.

Professor Roach and I have said that we have concerns about aspects of the green paper, and we do. We do not, however, have concerns about the existence of the green paper. We welcome the consultations that are under way across the country, which you mentioned. As private individuals trying to keep up, we welcome them, but we're finding them somewhat exhausting. That will help then encourage insight and expertise in this area and cultivate expertise outside of government.

Mr. Rémi Massé: Thank you, Mr. Forcese.

I have the same question for Madam Pillay, and then I'll ask the same question to Mr. Roach.

Ms. Sukanya Pillay: I suppose that I would have to provide the same answer that I gave a bit earlier, which is that we asked the question when Bill C-51 came out: why was this necessary? We had existing laws in place already. We have never received an appropriate answer, and I don't know why.

I do know that it is not a mere aspiration to say that we have to ensure that we have our constitutional safeguards in place and in mind. I would urge this committee to remember that it is not a choice necessarily between security and civil liberties; to the contrary, I think that we can only have effective security when we ensure that our civil liberties are there.

Civil liberties do not prevent, in the context of SCISA, for example, relevant, necessary, and proportional information from being shared; rather, they ensure that only relevant, necessary, and proportional information is being shared.

We have a wealth of information provided from three federal commissions of inquiry that speak directly to these issues of information. I would very much urge this honourable committee to consider that and to implement it in any recommendations that you make.

● (1235)

[*Translation*]

Mr. Rémi Massé: Thank you.

[*English*]

Mr. Roach, do you have anything to add?

Prof. Kent Roach: I agree with what both of my colleagues have said, but I would point out that even with the green paper, one of the things that we have to guard against is siloing these different areas. We have a whole-of-government approach to security, which I think is understandable, given the threats, but we still tend to think about this in a siloed way.

Our discussion today about this piece of legislation should lead you to thinking about the adequacy of review. That has been a scene that has come up again and again. Also, any new powers that may be given in the future to any department or agency of the federal government will be subject to this information sharing act, if it is not changed. I think the green paper is a good first start, but we need to encourage thinking about this in a holisitic way.

On the Bill C-22 question, I do regret the fact that, although it's a good idea to move ahead with a parliamentary committee, it's only part of the picture. We need to look at an executive watchdog review. We don't need to be looking for perfect legal language, because all legal language is going to be subject to interpretation, and as Professor Forcese has said, it's often interpretation that the public will not have access to. We need to think of a process solution to this issue. I think part of the process solution is to have a review structure that commands the confidence of Canadians.

[*Translation*]

Mr. Rémi Massé: Thank you.

I have finished.

The Vice-Chair (Mr. Joël Lightbound): Mr. Erskine-Smith now has the floor.

[*English*]

Mr. Nathaniel Erskine-Smith: I want to go to the issue of safeguards.

Professors, you mentioned that one of your recommendations is to update the CSIS Act, section 19, and the National Defence Act provisions related to CSE so that they comply with the Wakeling decision of the Supreme Court.

We haven't really discussed that today, and I wonder if you could speak to that and what it means for us.

Prof. Craig Forcese: I'll start, and then Kent can jump in.

The Wakeling case involved information shared by the RCMP to American authorities under what's known as part VI of the Criminal Code, which is the wiretapping provision. It was a lawfully gathered wiretap that complied with the charter, and that information was then transmitted to the United States. The Supreme Court concluded that even though the information was lawfully collected, it was still subject to charter privacy protections that had to govern the manner of information sharing.

In that case the RCMP, under part VI of the Criminal Code, was successful in defending the constitutionality of that information sharing, because there was enough architecture in part VI that defined who was going to receive the information and it imposed safeguards on how that information would be transmitted. The court along the way, incidentally, made a point of noting the Arar case as an example of where things can go awry in information sharing.

Now transpose the holding in that case to the context for CSIS under the CSIS Act and for the Communications Security Establishment under the National Defence Act. There is none of the architecture that rendered the Criminal Code constitutional. None of that architecture is found in the CSIS Act or the National Defence Act, and yet those two agencies, CSIS and CSE, are elemental bodies in information sharing for the purposes of supporting Five Eyes activities and others.

I think Professor Roach and I were surprised that the government didn't take the opportunity in either Bill C-51, or before that in Bill C-44, to introduce that architecture to put this vital information sharing on sounder constitutional footing.

● (1240)

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

I have a couple of follow-up questions on the review, because we're discussing it quite a lot. The first question is on powers, the power to compel the deletion of unreliable information. I know that it was one of your recommendations, and this power would be exercised by a super-SIRC type of body. Is that the idea?

Prof. Kent Roach: Generally, SIRC has not had powers to implement its recommendations. It makes recommendations, and the minister responsible responds to them. This is part of the sometimes confused distinction between review and oversight.

Mr. Nathaniel Erskine-Smith: Then does the power to compel information then lie with the minister, perhaps acting on the recommendation of a super-SIRC type body? I'm trying to understand who should hold that power.

Prof. Kent Roach: I think that unless an exception is made because of privacy interests, probably the power probably ultimately has to reside with the minister.

Mr. Nathaniel Erskine-Smith: Okay.

My last question is a resource issue. As lawyers, we deal with data dumps, and you mentioned about finding that needle in a haystack, and we've just started on information sharing. I don't think the Privacy Commissioner has been able to keep up with all the information that's already been shared. If a super-SIRC type body has the ability to review information sharing, there's a great mismatch in resources between security agencies and review agencies. If you tally up SIRC's resources and the CSE commissioner's resources and the oversight body of the RCMP, is that sufficient to really do the job?

Prof. Craig Forcese: Well, I think it depends on who you ask. SIRC of course has grown in terms of its budget and staffing in response to the new CSIS powers to do threat reduction and now CSIS's operations overseas. At the end of the day, any kind of review body is going to be a partial audit. You're not going to be able, in any given year, to audit all of the activities of a service, and that's by necessity. You are not going to be able to match the scale and scope of agency activities.

On the other hand, if you put in place a triage system within the review body to decide what you're going to audit this year and decided to take into account the legal issues and the constitutional issues that might be raised by this practice, its notoriety, and how new and novel it is, then I think that a reasonably well-resourced SIRC or super-SIRC would probably put a priority on information sharing when it came up in the cycle of auditing, because of the sensitivities around it.

The consequence, of course, is that they're not necessarily reviewing other things, so at the end of the day, any review body is going to engage in triage. When you ask about resourcing, it's how much triage you are willing to pay for. Historically I think that SIRC has been underfunded relative to the growth in CSIS since 9/11. It's starting to catch up now.

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

Mr. Dusseault is next.

[*Translation*]

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

To respond to Mr. Massé, I would say that this was done during the previous Parliament, in Bill C-51.

The mistake too many governments make is to respond to unique, one-time situations by passing laws. Sometimes those laws are too radical and have unexpected consequences. Moreover, they are not necessarily adopted in the public interest, but rather in the political interest of a government. Unfortunately, many members in the previous Parliament fell into the C-51 trap.

That said, I would like to go back to the issue of the oversight of national security organizations and by the organization that will be created if Bill C-22 is adopted.

What do you think of the idea that existing oversight bodies, and the one that will be made up of parliamentarians, examine information in real time rather than information on past situations? Would it be appropriate that all of the oversight organizations, including the one made up of parliamentarians, have the information immediately, and not after the fact?

My question is addressed to you, Mr. Forcese.

● (1245)

[*English*]

Prof. Craig Forcese: There is a discussion quite often about review versus oversight. There is some confusion about the terms, but in Canadian practice, oversight means command, control, and coordination. The oversight entity authorizes or has a role in authorizing activities.

Review is looking at the performance of the agency against standards. Typically it examines whether the conduct of the agency was legal and was in accordance with ministerial directives.

Review is after the fact, in the sense that you need agency action before you can review it, but review can be close to actual in the sense that the review doesn't necessarily have to be 20 years after the fact or a year after the fact or a month after the fact. My understanding from SIRC is that increasingly their review is more approximate in time to the actual operation, so it's still after the fact, but it's not that much after the fact.

The same thing should probably be true for the parliamentary committee under Bill C-22; that is, it is competent to do review. It does not do command and control oversight, and I think it would not be proper for that body to do command and control oversight. It does review, but I don't think it should fear doing review that's approximate in time to the actual operations, as long as it doesn't impede those operations.

Where this might become controversial is the extent to which the executive branch can deny the committee the information it requires to do this more timely review.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you.

That's all for me.

[*English*]

The Vice-Chair (Mr. Joël Lightbound): Members, I wasn't expecting to chair. If you would allow me, I have a few questions.

We've learned over recent years, mainly through the CBC, of various programs by CSE, such as EONBLUE, whereby captures were put at the Internet backbone and the impact and inspection was used to scan vast amounts of data that go through the Internet.

There are other programs like Levitation, if I'm not mistaken, which screened 10 to 15 million downloads for suspicious events and then transmitted the results to our security agencies.

Another one was Wi-Fi at a Canadian airport, where metadata of Canadians was stored and analyzed as part of a pilot project.

CSE gathers a lot of information. It's not supposed to spy on Canadians, but can inadvertently do so. When it has that information, based on SCISA as it's written, if a law enforcement agency wants that data about a Canadian, technically it would need a warrant, in the wake of Spencer and Wakeling.

Prof. Craig Forcese: This is an area of some confusion.

I mentioned briefly a few moments ago that there is a lot of uncertainty in this area as to how various statutory rules are being construed by the government. One area of uncertainty is over the practice of what's known as deminimization. CSE, as part of its foreign intelligence conduct and its activities, may acquire metadata and that metadata may include metadata from a Canadian source because of the nature of the Internet. It's not directing its activities at Canadians, but it's sweeping up some of this Canadian data in its operations.

Thereafter, when it shares its analytical work products dealing with that metadata, it is supposed to minimize Canadian identifying information. In other words, it redacts the Canadian identifying information. Those redactions can be lifted in relation to CSIS and the RCMP on request.

The question that remains unanswered in my mind is, what is the legal basis for that request? From what I've seen, it's clear that it has to comply with the Privacy Act in that all parties agree that it has to comply with the Privacy Act. There is an investigation, and CSIS is entitled to ask for the redactions to be lifted as part of its investigation.

What is unclear to me is whether they also come with a warrant, because if they don't come with a warrant, then information that CSIS could not lawfully collect itself is nevertheless put in play within CSIS by virtue of the inadvertent collection by CSE, and that CSE collection has never been supervised by an independent judge. Therefore, it's an open question in my mind as to whether, when CSIS or the RCMP comes looking for those redactions to be lifted, they comes supplied with a warrant. In other words, I don't know.

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

If you look at section 5 of SCISA, CSE could also volunteer information so long as it's relevant to the definition in section 2, so it's supposed to redact when it volunteers also.

I'm trying to understand. I'm confused as much as....

● (1250)

Prof. Craig Forcese: Does Kent want to respond?

Prof. Kent Roach: The volunteering under section 5 takes us back to “subject to any provision of any other Act of Parliament, or of any other regulation made under such an Act, that prohibits or restricts the disclosure of information”, so I guess it would depend upon that, although certainly if you're talking about Spencer and Wakeling, you're talking about the charter. Although section 5 makes no reference to the charter being an exception, I would think if we're going to respect acts of Parliament, then CSE should be respecting the charter, but that then brings you back to the question of how CSE's lawyers interpret the charter and how they interpret, say, the Spencer decision. One of the disturbing factors in the green paper is that the green paper seems to be asking Canadians what they think about Spencer, whereas most lawyers would consider Spencer to be settled law in saying that metadata, because of our interests in anonymity, is actually protected privacy.

We don't mean to be obtuse in answering these questions, but I think they are genuinely difficult questions that are made significantly more difficult by the rather convoluted drafting of, say, section 5.

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

Go ahead, Madam Pillay.

Ms. Sukanya Pillay: I would agree with what my two colleagues said, and I wish to underscore the serious civil liberties concerns here. Not only are we concerned about how the lawyers of various agencies might be interpreting things or what charter rights are engaged, including sections 11 and 13, but also we're concerned even about the initial question, which is that we have collection by CSE of information and that very collection is what we question and what we're very concerned about.

As I mentioned, I had this discussion a few years ago with Bill Binney, and I don't think anything has changed. You have agencies like the CSE in Canada and comparable ones in the United States, which presumably have all this information at their fingertips on Canadians, and that is a serious concern to the CCLA.

The Vice-Chair (Mr. Joël Lightbound): Thank you, and that's a concern not just to the CCLA.

I have another short question. On section 2, you've mentioned that terrorism is not defined anywhere, or is defined differently in various acts, such as the Criminal Code. Are there definitions of interference? For instance, if I look at paragraph 2(a), to your mind, that's a clear definition of what interference is. Interference comes back in paragraph 2(f). Mr. Forcese, are there working definitions of that?

Prof. Craig Forcese: No, they're not definitions. The definitions that apply to section 2...well, they have a definition of the people of Canada, which, if you read it, is itself extremely broad and somewhat uncertain, so “people of Canada” means the people in Canada. Could that be one person, or does it have to be more than one person?

On the definitions, some of these concepts are known to law. Espionage, sabotage, and covert and foreign-influenced activities are concepts that are found in the CSIS Act. Espionage and sabotage are Criminal Code concepts, so presumably you want to define them consistently subject to whatever rules of statutory interpretation you're applying. Terrorism, as I mentioned, has multiple definitions, so which one do you prefer? Then the other concepts, with the exception of the ones that are cross-referenced expressly to existing statutory provisions, are all novel concepts that would require some sort of understanding.

The Vice-Chair (Mr. Joël Lightbound): As a quick recap, I know that Mr. Erskine-Smith has tried to do that, but if we look at the changes.... If we take SCISA and we want to offer recommendations that are useful, the first thing, as you've mentioned—and correct me if I'm wrong—would be to change the definition under section 2 to limit it probably to terrorism as defined in the Criminal Code. What would be the ideal amendment?

Prof. Craig Forcese: Perhaps Kent should speak to this, but for section 2 we essentially said to get rid of this novel concept of “activity that undermines the security of Canada”. Use the better-understood concept of “threats to the security of Canada” from the CSIS Act, as adjusted to accommodate, say, bona fide concerns about weapons proliferation that might not be captured by that CSIS concept.

● (1255)

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

Then for section 5, you would be adding necessity and proportionality for disclosure.

Prof. Kent Roach: Yes, and we also recommend that it be amended to make it crystal clear that recipients must operate within their existing mandates and legal authorities, because although we thought that was reasonably clear, the green paper actually makes it more ambiguous.

The Vice-Chair (Mr. Joël Lightbound): As well, with regard to section 9 on immunity in civil proceedings, we would get rid of that altogether and leave that up to the court, correct?

Prof. Kent Roach: Yes.

The Vice-Chair (Mr. Joël Lightbound): Is there something that I'm missing?

Prof. Kent Roach: Well, there's the issue of review. I think a unifying theme in all three of our testimonies is that you really need to look at information sharing in light of the adequacy of review. There are no perfect legal fixes here, but as I said, I think there may be a process fix that all Canadians can agree will govern us as these things continue to evolve over time.

The Vice-Chair (Mr. Joël Lightbound): All right. I've given myself a liberal nine minutes.

I thank you all. That's...Bob, do you have a quick question?

Mr. Bob Bratina: To Ms. Pillay, you've defended lots of controversial positions, and I wonder if you have a sense of the public perception of these issues.

I've been in a Communist country where the film was taken from my camera because I took a picture of a train and somebody spotted that and told somebody. This is the kind of life that we don't want to approach, and I think that's why we're concerned about this, but what would you say? Is the public as engrossed in this question that we're bringing forward today?

Ms. Sukanya Pillay: I admit that I may talk to people who tend to already be interested in this issue, but certainly I've talked to people who aren't.

However, I saw a coming together of Canadians on Bill C-51 and a concern about the scope of information sharing that I hadn't seen before in recent years. Based on that and based on the response that CCLA had to the application that we brought and the very specific grounds in our application that referred to SCISA in particular and also broadly to Bill C-51, my answer is that we had a swell of support among Canadians.

I would also point out that other colleagues among civil liberties organizations had petitions that were signed by hundreds of thousands of Canadians, so I think that Canadians are very concerned. We don't want an all-government all-knowing all-the-time society. We don't want an all-surveillance society.

We also recognize in this country that legitimate dissent and protest and disagreement and counter-speech are constitutionally protected rights in Canada, regardless of whether those opinions are directed at the Canadian government or a government anywhere else in the world. Provided that they don't engage in violence, these are activities that are protected. My view, based on the evidence of who signed up and who donated to the campaigns that we launched in this regard, is that Canadians are very much on board with protecting our privacy and making sure that any information shared is necessary and proportional.

Mr. Bob Bratina: Thank you.

The Vice-Chair (Mr. Joël Lightbound): That's all the time we have.

I want to thank all members and thank our witnesses for being with us today, and also for the work that you do. I think that holding the government to account and safeguarding charter rights is eminently patriotic. I thank you for it.

The meeting is adjourned.