HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 090 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, December 7, 2017

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, December 7, 2017

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I'd like to call to order the 90th meeting of the Standing Committee on Public Safety and National Security.

We have with us a familiar face, our Privacy Commissioner.

Welcome again to the committee, sir. I'll leave you to introduce your colleagues.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair.

[*English*]

Mr. Chair and members of the committee, I am here this morning with Patricia Kosseim, who is our general counsel, and Lara Ives, who is the director general of audit and review.

Thank you for the invitation to discuss Bill C-59.

As you know, Bill C-59 introduces a wide range of measures intended to strengthen Canada's national security framework in a manner that safeguards the rights and freedoms of Canadians. On the whole, I find it represents a step in the right direction, but as other commentators have noted, its weakest part is the Security of Canada Information Sharing Act, or SCISA, which contains provisions related to information sharing and privacy. Professor Forcese, for instance, gave these sections a failing grade. I was therefore glad to hear Minister Goodale last week say that SCISA was probably the part most deserving of scrutiny. I hope your study will result in much-needed improvements to these rules.

In previous parliamentary briefs, I highlighted the need for rigorous legal standards around the collection and sharing of personal information, effective oversight, and minimization of risks to the privacy of ordinary law-abiding Canadians, particularly through privacy-sensitive retention and destruction practices. Specifically, I indicated that the law should prescribe two things essentially, which are useful to bear in mind. First is clear and reasonable standards for the sharing, collection, use and retention of personal information", so substantive rules. Second is that compliance with these standards should be subject to independent and effective review mechanisms.

It is with this analysis in mind that I offer the following comments and recommendations. While I will focus in my remarks on SCISA, this analysis, looking at two types of issues, is also relevant for other parts of Bill C-59, including parts 3 and 4. The full list of our recommendations is attached to this statement.

Bill C-59 would create a new expert review body, the NSIRA, with broad jurisdiction to examine the activities of all departments and agencies involved in national security. Recently, Parliament also created, through Bill C-22, a new National Security and Intelligence Committee of Parliamentarians. Both of these bodies will be able to share confidential information and generally co-operate so as to produce well-informed and comprehensive reviews that reflect considerations both by experts and by elected officials.

These developments are most welcome, but they are, in my view, clearly insufficient. In my view, effective review of national security activities must include both parliamentary and expert review, and the latter must include both national security and privacy experts. Why privacy experts? Because the work of national security agencies depends in large part on personal information. It is what they call their "lifeblood". The OPC is the federal centre of expertise in privacy and personal data protection. Canadians are concerned that anti-terrorism efforts in government not unduly impede their privacy rights, and they expect my office to play a role in ensuring that balance.

Bill C-59 is oddly silent on the role of my office. It does not amend the Privacy Act, so my existing authorities appear to be untouched. The only body with explicit authority to play a role in relation to part 5, the renamed SCIDA, or security of canada information disclosure act, is the NSIRA, the national security and intelligence review agency.

The ethics committee, in its study of SCISA, has already noted the ambiguity in the interplay between that act and the Privacy Act. It has called for amendments to clarify that the Privacy Act continues to apply to all personal information disclosed pursuant to SCISA. I have provided to your committee amendments that would confirm the application of the Privacy Act and the OPC's role, which I am told the government wants to maintain.

However, there is no ambiguity on whether my office would be able, with Bill C-59, to share confidential information with the NSIRA and the new committee of parliamentarians. We would not have that authority, and actually we would be prohibited by existing provisions in the Privacy Act from sharing such information.

● (0850)

This means that the comprehensive review process offered in Bill C-59, as a fundamental element to bring balance between security and respect for rights, would stop short of the objective by leaving privacy experts out of integrated review. I am at a loss to understand why. If the fear is of duplication between our work and that of other review bodies, I would gladly explain through the question period how bringing the OPC firmly within the family of review bodies would not only bring required expertise but would actually enhance efficiency and reduce overlap.

[*Translation*]

When Bill C-51 enacted the Security of Canada Information Sharing Act, known as SCISA, I indicated that among my concerns was the fact that the relevance standard for sharing was set too low, and that there was an absence of clear data retention and recordkeeping requirements and a lack of information-sharing agreements and privacy impact assessments.

The relevance test is too permissive because it casts too wide a net and creates undue risks for ordinary citizens who pose no threat to national security. The government seems to recognize that a relevance standard does not sufficiently protect privacy because it is suggesting changes to section 5 of SCISA.

In its response to the Standing Committee on Access to Information, Privacy and Ethics, the government said the following:

> The key issue regarding the threshold is the need to establish specific decision making parameters for the discloser of information that will protect individual privacy but not cause undue delays in the information sharing process.

I agree with that assessment. The proposed new section 5, particularly paragraph 5(1)(b), incorporates some aspects of a necessity threshold but falls short of adopting what officials refer to as “strict necessity”.

In order to adequately protect privacy rights, under new section 5, this limited progress in increasing the threshold for disclosure would have to be accompanied by more complete changes to the standard applicable to receiving institutions, in other words, the security agencies receiving the information in question.

Information sharing involves two parties and, to protect rights, rules are also required for receiving institutions. If relevance is not adequate for disclosing institutions, it is also inadequate, even more so, for receiving agencies.

And the delay considerations that may apply to disclosure affect receiving departments very differently. These institutions are perfectly capable of applying the classic, internationally established necessity test, and should be required to do so.

We understand that the government intention is for receiving institutions to continue to be governed by the Privacy Act, or their specific enabling legislation where applicable. The current Privacy Act threshold is relevance.

As your committee recommended in its May 2017 report on Canada's national security framework, we also recommend that a dual threshold be adopted for information sharing—that set out in amended section 5 for disclosing institutions, and that of necessity and proportionality for receiving institutions.

Even if one accepts that government sharing of information related to law-abiding citizens may lead to the identification of new threats to national security, once that information is analyzed and leads to the conclusion that someone is not a threat, it should no longer be retained. Otherwise national security agencies will be able to keep a profile on all of us.

This is consistent with the conclusions of our review of the Canada Border Services Agency's scenario-based targeting initiative, summarized in my latest annual report to Parliament, and it is one of the principles upheld by the European Court of Justice in the passenger name and record case, decided in July 2017.

In addition, if the threshold for collecting or receiving information is higher than the standard for disclosure—which is currently the case at least for CSIS and would be the case if you adopt a dual threshold, that is, one for disclosing institutions and one for receiving institutions—then, rules are required to ensure that information is discarded without delay either when the collection test is not met or if the receiving institution is of the view that the disclosure standard was not satisfied.

● (0855)

In conclusion, my complete recommendations, annexed to this statement, include some that I have made in the past and do not have time to explain in the time allotted this morning. I also intend to write a fuller submission prior to the end of your study.

My team and I would be glad to answer any questions you may have.

[*English*]

The Chair: Thank you, Mr. Therrien.

Ms. Dabrusin, you have seven minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you for that. I appreciate that you have provided us with specific recommendations.

Last night I was reviewing the Air India inquiry recommendations and trying to get a sense, against that backdrop where 329 people were killed, of where their recommendations specifically pointed to problems with a lack of information sharing and yet understanding that there are many concerns in balancing privacy in that framework. With this set of questions I'm trying to figure out where we meet that balance.

You go quite a bit that way, talking about the required expertise you can bring to help us reach that balance. You touched on it and said you might be able to give us more information about that in the questions, so I am going to open that to you. Where do you see your expertise coming in to help us reach that balance? Where would you have us slot that in? Ultimately, we're going to have to be reviewing this legislation on a clause-by-clause basis. What would be the main recommendations you have listed that you think can bring that expertise?

Mr. Daniel Therrien: I start my analysis with the need to have good, clear, sufficiently high legal standards, including thresholds. That's where the issue of relevance for contributing to the mandate or being necessary comes in, so there are substantive legal safeguards.

The second element of well-balanced national security legislation requires strong, independent, effective review. On the substantive legal safeguards side, I accept that to apply the necessity test may pose problems for disclosing institutions, which is the main point the government made in responding to the ethics committee, and which may have been a contributing factor to your committee when you suggested a dual threshold.

I accept that a threshold lower than necessity helps disclosing institutions do a difficult task while having safeguards. However, receiving institutions—essentially national security agencies—know very well what their mandate is and what they need to do their job. There, the necessity threshold, which is the international norm, should apply fully.

That's the main substantive recommendation I'm making, which is again where this committee was at not long ago.

The second substantive rule is as follows. If there is a difference between the thresholds applicable to disclosing and receiving institutions which would be the result of a dual threshold, it's easier for disclosing institutions to disclose, but the threshold for receivers is higher. Point one is, what do we do about this gap, if the receiving institution has received something that is not necessary?

Point two is, if the receiving institution has received information about a law-abiding citizen—travellers are the best example—to identify in the mass of travellers the extremely few who may pose a threat to national security, there should be legal rules to require the receiving institution to get rid of the information, to destroy the information, to no longer retain the information if there's a gap between the two thresholds, or if, in relation to a given individual, the analysis leads to the conclusion that the person is not a threat and therefore that their information should not sit in the records of CSIS or the CSE or the intelligence apparatus. These are the substantive rules.

In terms of effective review, it is clear that the creation of the new NSIRA is an important improvement. The fact that it will be able to share information with the committee of parliamentarians creates a good step in the right direction, in that you have integrated review applicable to all departments—not only three as at the current time—and you have elected officials and experts who can talk to one another and reach a well-informed decision.

What we think we can bring to the picture—and we're not in the picture, at least not completely—with Bill C-59 is that the lifeblood, *la matière première*, the main tool that national security agencies have to do their job is information, and that includes personal information. We're the experts in how to deal with personal information in a way that respects privacy rights. We're not saying that NSIRA would be without any knowledge of the relevant issues, but there is an issue of core importance to the work of national security agencies, that of privacy, where we're the experts, and we think we can add value to the rest of the architecture.

● (0900)

Ms. Julie Dabrusin: Thank you. I only have 45 seconds.

I see you have provided some recommendations as to effective review and oversight. I was wondering if you might be able, when you're providing your written submissions later, to flesh out how you see your interconnection with the NSIRA. Where do you see us slotting that, in your preferred situation?

Mr. Daniel Therrien: In a few words, I would say that I have a broad mandate, which goes well beyond national security, and I have limited resources. If only for that reason, we cannot afford to be involved in national security activities as the NSIRA would be, whose only task would be that.

We need to be able to have discussions with NSIRA on where we fit best and in which cases our expertise would be of most value, on the basis that for the most part, they would do the review, but that there will be cases in which we can add value because privacy will be particularly important.

● (0905)

[*Translation*]

The Chair: Mr. Paul-Hus, you have seven minutes.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Good morning, Mr. Therrien.

We agree that, when it comes to the threat posed by terrorism, 9/11 was the tipping point for the public.

Last year, I visited NORAD headquarters. Although it concerned a military issue, you will see the connection. The people at NORAD, in Colorado Springs, told us that, prior to 9/11, they dealt with threats originating outside the U.S. and that the federal aviation agency was responsible for domestic threats. According to the commander in charge, after 9/11, the two organizations never hung up the phone. The communication and connection remained constant.

That leads me to the following question. In March 2015, you said that Bill C-51 would allow too many federal government agencies—up to 17—to share information. Do you still think the information sharing involving those organizations is too broad?

Mr. Daniel Therrien: I was a government lawyer at the time, and I was responsible for national security and public safety issues for nearly 10 years afterwards. I am very cognizant, then, of those considerations.

Coming back to what I said in 2015, I would agree that information sharing is necessary for national security agencies to be effective. In 2015, when I referred to the involvement of multiple agencies, I did not mean that a certain number of agencies should not be permitted to share information. Rather, I wanted to draw attention to the flaws in the review mechanism, which applied only to three of the 17 receiving agencies. I don't believe I said that information sharing should not be permitted or that 17 agencies was too many. The point I was trying to make was that, if 17 agencies were receiving information in order to do their jobs, they should all be subject to independent oversight.

Mr. Pierre Paul-Hus: In your brief, you say that "Canadians are concerned that anti-terrorism efforts in government not unduly impede their privacy rights". Why do you believe that Canadians are concerned? My impression is actually that Canadians are concerned about security. You, however, maintain that anti-terrorism measures cause privacy concerns among Canadians. Can you cite any sources to back up that statement?

Mr. Daniel Therrien: Yes, Canadians are concerned about both of those issues.

We regularly receive correspondence from people, and surveys done over the years show without a doubt that people are worried about their security. That is clear. A number of studies show that, despite that worry, which is normal, Canadians expect the government and Parliament to simultaneously protect their security and their rights, especially their privacy rights. A number of surveys demonstrate that to be true.

Mr. Pierre Paul-Hus: Would it be possible for you to provide copies of those surveys to the committee? It would be useful to take a close look at them.

Mr. Daniel Therrien: Yes.

Mr. Pierre Paul-Hus: Later on, in your remarks, you call the relevance test "too permissive", saying that it "creates undue risks for ordinary citizens who pose no threat". The problem with terrorism is that, technically speaking, everyone is a potential threat. How are we supposed to differentiate between an ordinary citizen who poses no threat to national security and someone who does?

Mr. Daniel Therrien: I am aware of the challenge. That is why I say that the sharing and fairly broad collection of information for the purpose of identifying threats is reasonable provided that, once the information is analyzed and leads to the conclusion that the vast majority of people do not pose a threat, it is destroyed. That way, security agencies will not have numerous profiles on people who are not threats.

It is fine to begin with a funnel-like approach and focus on a certain number of people, many of whom are not threats, and then come to an appropriate conclusion. Therefore, once it has been concluded that the vast majority of those people are not threats, their information should be destroyed.

[*English*]

The Chair: You have three minutes, closer to two.

[*Translation*]

Mr. Pierre Paul-Hus: You were actually very critical of Bill C-51 at the time. Now, you are not satisfied with Bill C-59. You consider the collection of information to be acceptable and see it as normal. However, you have concerns about Bill C-59's purpose. That's what you said this morning.

● (0910)

Mr. Daniel Therrien: Is the purpose of the bill reasonable? What do you mean by purpose?

What I mean is that the purpose of compiling information in order to analyze and identify threats is fine. I am saying, though, that, once an analysis of the information leads to the conclusion that the vast majority of people are not threats, there need to be consequences and agencies should not have the discretion to decide whether or not to retain the information. Clear legal rules governing the destruction of information are necessary to protect people's privacy.

Mr. Pierre Paul-Hus: I want to come back to the collection of information. When Bill C-51 was introduced, people were worried about intelligence agencies being able to spy on their computer activities. They wondered just how much agencies would be able to invade their privacy.

Do you currently see that as a problem? Do you think Canadians are subject to an excessive invasion of their privacy?

Do you think our intelligence agencies are likely to spy on our computer activities?

Mr. Daniel Therrien: We reviewed the operationalization of the Security of Canada Information Sharing Act, but, on the whole, we noted no such invasion.

My concern has more to do with the legal standards. We are not experts. The Security Intelligence Review Committee, or SIRC, actually assesses that on an ongoing basis. Other oversight agencies do as well.

Our review of the operationalization of the Security of Canada Information Sharing Act did not reveal any such invasions of privacy. The point I am trying to make actually pertains to the legal standards.

The Chair: Thank you.

Mr. Dubé, you have seven minutes. Please go ahead.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

Mr. Therrien, I want to thank you and your team for being with us today.

My question has to do with the Canada Border Services Agency, or CBSA for short.

On the one hand, should the agency have an oversight body? It isn't the only organization that Bill C-59 excludes.

On the other hand, should we broaden the scope of the bill to include those organizations in national security matters?

Mr. Daniel Therrien: As far as I know, from a national security standpoint, CBSA does fall under the jurisdiction of the newly created body, the National Security and Intelligence Review Agency.

Is there a need to subject CBSA to oversight in relation to other matters? The question bears asking, since it is something that would certainly be welcome. Nevertheless, CBSA's national security activities do fall under the jurisdiction of the National Security and Intelligence Review Agency.

Mr. Matthew Dubé: CBSA is unlike other agencies in that it deals with travellers crossing the border as part of its day-to-day operations.

Does it raise any concerns that only CBSA's operations involving national security are subject to oversight? It could become difficult to distinguish between an action taken in the name of national security and one taken in the exercise of its mandate?

Mr. Daniel Therrien: Yes, you're right.

We reviewed various elements under the Security of Canada Information Sharing Act, discussed in our most recent annual report. We, in fact, did a review of a CBSA program that uses scenario-based screening of travellers in order to identify threats.

The threat could involve national security, criminal activity or something else. Therefore, reviews of those types of programs—one of many at CBSA—should target not only national security initiatives, but also programs designed to identify criminal and other threats.

Mr. Matthew Dubé: Thank you.

In terms of the datasets that the Canadian Security Intelligence Service will be collecting, do you think the bill sets out an adequate definition?

I'll start with that question and follow up with my next question in a moment.

● (0915)

Mr. Daniel Therrien: There is no doubt that the concept of datasets is very broadly defined, something that could prove problematic without oversight mechanisms or legal standards. To my mind, the two safeguards are more or less adequate in relation to the various stages leading to the use and exploitation of the datasets.

The jumping off point is Judge Noël's Federal Court decision, indicating that CSIS had compiled and retained information on individuals who were not threats. Judge Noël also said that he had heard evidence to the effect that the information in question could be helpful to identify threats.

My view on the dataset provisions is that efforts should be made to use the value of that intelligence—which is very broadly defined, I agree—but with different filters to ensure the data are not retained for an excessive period of time. The Federal Court normally conducts a review within 90 days, which is a pretty good method. CSIS's exploitation of the data, relying on the necessity test, is the standard we think should be used for information-sharing purposes.

It would be tough to call the provisions inadequate. The ultimate use of the data depends on necessity. For two years now, I have advocated for the necessity test in information sharing.

I am asking parliamentarians to apply the same necessity standard in the Security of Canada Information Sharing Act to information sharing, in the case of receiving institutions.

Mr. Matthew Dubé: I am going to stay on the topic of datasets.

The definition is rather broad. On one hand, we heard from witnesses on Tuesday about the benefits of having a broader definition; they claimed that it would keep agencies from having to play a constant game of catch-up. The pace of technological change is something that comes to mind.

On the other hand, I wonder whether there isn't cause for concern, since we don't know what this type of data collection—which the various agencies need to carry out their mandate—will look like in five or 10 years.

Mr. Daniel Therrien: Yes, there is a risk, but I think it is being managed properly, more or less.

The definition could probably be narrower but then national security agencies, such as CSIS, would be deprived of the information they need for their work. However, there is a risk. How can the risk be reduced? The answer is through independent and effective review mechanisms.

The part of Bill C-59 that deals with CSIS has a number of filters exercised by independent members of the executive of the government and the Canadian Security Intelligence Service based on high standards, including necessity. Overall, I think it's a fair balance.

Mr. Matthew Dubé: Okay.

My last question is about the Communications Security Establishment (CSE) mentioned in part 3 of the bill.

Despite the fact that its mandate is to address foreign threats, do you think, in the operations that the CSE will now be able to conduct, there is a risk of casting a large net that could subject Canadians in the information infrastructure to phishing?

Mr. Daniel Therrien: Through collection, the CSE can gather a lot of information. It's sort of the same dynamic as CSIS and the concept of dataset.

The starting point allows for a fairly vast collection of information. However, not only does a provision, clause 25, require the CSE to enforce measures to protect privacy, but those measures are clearly defined elsewhere in the bill, in clauses 35 and 44 as well as other clauses.

Not only does the CSE have a general duty to protect privacy, but privacy is very clearly defined in some provisions. Once again, this ultimately leads us to the following conclusion: the information must be essential to the CSE's mandate before CSE analyzes, stores, uses and exploits the information.

Once again, we are working with the test of necessity. I would even say strict necessity, when we talk about what is essential to the CSE's mandate.

● (0920)

The Chair: Thank you, Mr. Dubé.

Mr. Picard, you have seven minutes.

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

Mr. Therrien, it's good to see you again. Your expertise is recognized, and we greatly appreciate the rigour of your comments.

I will use your big concern to try to move the debate forward, especially since we are at the most important stage where we can make significant changes. Let's try to see what we can do about this.

I would like to ask a quick question, to start.

Are your office's security clearances problematic or are they preventing you from being part of the bigger picture?

Mr. Daniel Therrien: A number of our employees have the required security clearance.

Mr. Michel Picard: Okay.

In the surveys you have carried out in the past, including the ones in which I participated for the department, it was clear that the concern is there. It's undeniable, which is normal, considering that the reality is what it is.

In 2017, we have started to feel that people are grasping the reality of the threat, but please correct me if you see things differently. They see what is happening abroad, and they are slowly starting to accept negotiations and compromises. It is always a matter of striking a balance between rights and freedoms and security. It's a never-ending juggling act and it's almost impossible to solve.

Do you feel that people are starting to rethink what they accept as an untouchable privacy threshold and what they would agree to compromise on and give up?

Mr. Daniel Therrien: People's opinions vary over time.

Let me use an example based on clear circumstances. As a result of Edward Snowden's revelations, there has, of course, been a spike in public concerns about respect for rights, including the right to privacy. After a terrorist event, the scales usually tip the other way.

I suggest that you assume that the public is concerned about both physical security and their rights. Depending on the events, those concerns may fluctuate.

In my opinion, your job, mine and that of the executive power is to put in place legal rules that respect the balance over a certain period of time, regardless of revelations and terrorist events. Legal rules must also take into account any realities in time. Then there should be a review.

The bill provides a number of good suggestions, but I think we have a role to play in ensuring that officers apply those rules correctly on a daily basis.

Mr. Michel Picard: The debate about privacy is undeniable and accepted, and it must be protected.

Let's try to be more practical and take a micromanagement approach. Since we are still in the theoretical realm, it may be appropriate to provide a tangible example.

Could you give me one or two specific examples of privacy information to put it in the context of information sharing or national security?

What sort of information are you referring to?

A person's name may not be enough. Is buying a plane ticket to go to Europe in two weeks an example of the type of personal information you are referring to or is it more specific information?

Could you give us one or two hypothetical examples—we will not use names—so that we can have a more concrete foundation for the debate?

Mr. Daniel Therrien: Take the case of travellers, since that is a good example. Many people travel. In fact, almost all of us travel.

It is normal for decisions on overseeing admission to different countries to include a national security component. Of the millions, if not tens of millions of travellers, only a tiny minority pose a problem for national security, but everyone needs to be analyzed. CSIS, in the case of Canada, must have access to the names of travellers, to ensure that they do not pose threats to national security.

There are no specific rules that require CSIS to dispose of the information when it concludes that 99.9% of people do not pose a threat.

● (0925)

Mr. Michel Picard: It's a different story in the case of metadata, correct?

Under the new bill, what is not relevant must be destroyed.

Mr. Daniel Therrien: Right, in part 4 of the bill, which deals with datasets, the conclusion is that the information must be destroyed. The Federal Court must analyze those datasets and authorize or not authorize their retention after 90 days. This is exactly the kind of measure I recommend in the case of information sharing. If it's good for datasets, it should be good for information sharing under part 5 as well.

Mr. Michel Picard: Information sharing is problematic. Objective information is may or may not be valuable if it is not contextualized. Information sharing depends precisely on this relationship between information and context. When there are two stakeholders, two or more organizations, we wonder whether the necessity threshold should be used.

When you talk about what is strictly necessary, are we referring to relevance? Here, I'm sort of calling on the lawyer in you. How will that be managed?

An organization may consider a piece of information important and necessary, but the recipient may disagree. The opposite can happen. An organization may consider a piece of information only somewhat useful, whereas the agency with which it interacts is waiting for that information because its context, which the other organization cannot access, justifies it. In this case, the two thresholds for assessing the information seem problematic to me.

[*English*]

The Chair: Be very brief, please.

[*Translation*]

Mr. Daniel Therrien: It's just that things are not always very clear, especially for the department that discloses the information and is not an expert on national security. I agree that, for the institution that discloses the information, the standard is a little more permissive. The new section 5 is not perfect, but it does the job. Its application ensures that the institution that discloses the information —the Department of Agriculture, for example, does not have many national security experts—feels empowered to do so. That's good.

When CSIS receives information, it must analyze it. It knows what it needs for its work and what is superfluous. After the analysis, CSIS should have not only the power but also the legal obligation to dispose of any information that it no longer needs for its work.

[*English*]

The Chair: Thank you, Mr. Picard.

Mr. Motz, you have five minutes, please.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Commissioner and your team, for being here.

You indicated in your recommendations—and thank you for providing some additions—specifically in recommendation A, in removing ambiguity, I suppose, with respect to the role of the Privacy Commissioner, that you should be among the review bodies having the legal authority and flexibility to share confidential information. I'm just curious, besides you and your background, does your office have the expertise to understand the ramifications and overall impacts of national security and the intel sharing?

Mr. Daniel Therrien: We have about 10 employees who have the security clearance and who review these issues from time to time and who, yes, have the expertise to know the context.

To give the other side of the coin, if we're not involved, it would mean that the expertise we have garnered through our work generally vis-à-vis all departments would not benefit national security agencies. That's something to bear in mind.

Mr. Glen Motz: Would you see a change in the mandate of your organization with the passage of Bill C-59? If so, would you require the allocation of more resources to manage those changes?

Mr. Daniel Therrien: If my recommendations are adopted, no. We don't need an army of people. We have a broad mandate. We supervise the private sector as well. I don't envisage that we would need more resources.

● (0930)

Mr. Glen Motz: Would you see the national security and intelligence review agency as a positive addition, through standardized practices, without allocating resources from protecting Canadians to the compliance and red tape practices?

Mr. Daniel Therrien: I think all review bodies should be sufficiently resourced, which does not mean necessarily a huge infusion of resources, but they should be able to do their job properly. Whether something is red tape or necessary review, I guess, is in the eye of the beholder. At this point, given the level of resources that SIRC, the CSE commissioner, and I have, with my limited resources, I would not talk about red tape. We're talking about 20 people, at the most. This is not red tape. This is necessary review. We need sufficient resources to do that job adequately.

Mr. Glen Motz: Okay, thank you.

Three inquiries—Air India, Arar, and the O'Connor decision—have identified sharing information and communicating threats as critical to having an effective national security team. You have indicated, certainly, that you agree with that.

With this new national security and intelligence review agency, can some of the overall issues you have found with procedure and reporting be fixed?

Mr. Daniel Therrien: With procedure reporting?

Mr. Glen Motz: Procedure and reporting: can those things be shored up with this new review agency?

Mr. Daniel Therrien: Absolutely. NSIRA is a very important step forward, in part because its jurisdiction encompasses all departments and agencies involved in national security, which is a flaw of the current system.

What I'm recommending is that our expertise be added to this mix so that the sum total of expert review and parliamentary review is able to give Canadians the assurance that both their security and their rights are protected.

Mr. Glen Motz: Would you characterize proactive collection or centralized intelligence as a threat to privacy?

Mr. Daniel Therrien: I'm not sure what you mean by proactive and centralized. I answered Mr. Paul-Hus to say I agree that the collection of information, including that of some who are not a threat, can be useful to actually identify threats.

If that's what you mean by proactive, yes, I agree with that, so long as there are safeguards to ensure that the privacy of those who are not threats is not at risk.

The Chair: Thank you, Mr. Motz.

Mr. Spengemann, you have five minutes.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Mr. Therrien, thank you for being here with your staff, and for your expertise and testimony.

I'd like to build briefly on the question my colleague, Mr. Picard, asked you in the form of an example to make it concrete for the committee, but also for Canadians who are listening now or are reviewing your testimony in the future.

Could you give us an example of a case from the area of security that would highlight how the application of relevance, necessity, and proportionality would unfold, perhaps an example that both meets and then, in an extrapolation, exceeds the threshold of each of these so there's a better understanding on the part of the Canadian public as to what analysis is actually taking place here?

Mr. Daniel Therrien: The best example would be, again, that of travellers. The information about travellers, many of whom are not a risk to national security, may be relevant and may contribute to the mandate of the receiving agency, to use the words of the new section 5, because in the mass of travellers there might be some who are a threat. To have information on a more permissive relevancy or contribution standard may be acceptable at the front end. However, when that information is then received and analyzed by the national security agency and the agency determines that the individual is not a threat, on what basis should the information be used and, moreover, retained by the agency? The retention of information about 99.9% of the travellers who are not a threat is not necessary to its work, to its mandate.

In looking at Bill C-59 as a whole with all of its parts, I'm struck by the fact that parts 3 and 4 have essentially the standards. I understand that relevance and necessity are somewhat esoteric notions, but in parts 3 and 4, the government and you as parliamentarians are seized with a bill that recognizes that there is a need for the higher necessity threshold in some circumstances.

CSIS and the CSE will not be able to use and exploit the personal information of individuals unless it meets a necessity test. If it's good for parts 3 and 4, I'm saying it should be good for part 5.

● (0935)

Mr. Sven Spengemann: Okay.

In your view, is there a risk of collecting irrelevant information at the outset? You're advocating for a broad funnel, the way I understand it, at the beginning. What kind of information might be irrelevant, and is there a risk of collecting irrelevant information?

Mr. Daniel Therrien: If the necessity threshold for the receiving institution is higher, yes, it will receive irrelevant information, but only for a fleeting period. That may be a price to pay for the fact that in that large basket of information, some information may be relevant.

Mr. Sven Spengemann: So we shouldn't really be concerned with the quality of the irrelevant information. There's no categorical concern—

Mr. Daniel Therrien: I wouldn't say we should not be concerned at all, but I see safeguards, including reliability of the information in the bill which are useful. I'm less concerned at the front end, the disclosing end, than I am at the receiving end.

Mr. Sven Spengemann: Thank you very much for that.

My second question goes into the area of youth and the criminal justice system. As you know, in counterterrorism work or terrorism generally, youth are often the target for radicalization efforts by such entities as al-Shabab, or Abu Sayyaf for ISIS, and youth are vulnerable in many ways with respect to data as well. Clause 159 of the bill brings the Youth Criminal Justice Act into play on the criminal justice side of things.

What concerns, if any, do you have from the privacy side that are specific to Canadian youth?

Mr. Daniel Therrien: I confess that we haven't paid much attention to this, but we will, and we will address that question in our ultimate submission.

Mr. Sven Spengemann: I'd be grateful. Thanks very much.

Mr. Sven Spengemann: Are you in a position to comment on whether there will be judicial review of decisions made by the intelligence commissioner? Judicial review is an important component of accountability and ultimately privacy as well. Would he or she be subject to judicial review, in your assessment?

Mr. Daniel Therrien: I haven't thought this through in detail, but the intelligence commissioner is an interesting, new creation. It is more of an oversight body. It reviews matters before the fact, as opposed to after the fact. It's a bit novel and it's a different position from, say, the current SIRC, which is clearly subject to judicial review.

I would say probably, yes.

Mr. Sven Spengemann: If you could add your thoughts into your written submissions, I think that would be helpful to the committee as well.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Spengemann.

Mr. MacKenzie, you have five minutes, please.

Mr. Dave MacKenzie (Oxford, CPC): Thank you, Commissioner, and your panel for being here today.

I'm intrigued by your comments about 90 days for the destruction. How broad is that across agencies when they look at their information and within 90 days they don't see any value? Is that when you would suggest the destruction period would occur?

Mr. Daniel Therrien: The 90-day period in Bill C-59 applies to the specific situation of the collection of datasets by CSIS. In a model where it's conceivable that more information may be required at the front end, but an exercise is required to funnel this to less information at some point, it's important that this period of analysis not be too long so as to give time to security agencies to do the analysis they need to do.

Ninety days strikes me as a very reasonable period. Should it be 90 days throughout regardless of whether it's CSIS, CSC, or others? We would have to look at it, but 90 days is a good rule of thumb.

Mr. Dave MacKenzie: From a practical, operative view, that may be a short period of time. I only have to look back to the more recent situation in New York City with the motor vehicle running down people on the street, and the British went back and looked at their records and determined that they had missed something in a telephone call that would have been helpful. I don't know whether it was 90 days or more, but it just seems that frequently it's the necessity to go back maybe a bit longer, and then make the connections not only directly to that, but to other events.

● (0940)

Mr. Daniel Therrien: Absolutely. There's no magical solution here. It's a question of balancing the value of the information and how long agencies should have to analyze it. Obviously the delay cannot be so long as to result in the creation of profiles or dossiers on all of us forever.

I'll note that for the CSIS provision in part 4, after 90 days the court doesn't base its determination on necessity, but rather on whether the information can be useful. It's a threshold, but we're not yet at the necessity stage. It's when this bank of information is then queried by officers that the necessity threshold applies.

I think there's room for CSIS in the regime for information that may not be clearly necessary at that point to be kept. It can be useful, but it will only be queried by CSIS officers at the back end, on a necessity threshold.

Mr. Dave MacKenzie: Okay. I appreciate that.

In looking at this legislation, as you have, how do you compare it, if you have done so, with that of our allies in the same businesses we are dealing with here, counter-intelligence and terrorism, particularly, I guess, that of the Five Eyes?

Mr. Daniel Therrien: I think that on the whole this legislation would allow Canada to catch up to the Five Eyes. Particularly this, plus Bill C-22, with the committee of parliamentarians, would allow some catching up, perhaps getting us near the front of the pack.

Mr. Dave MacKenzie: Okay.

I'd like to go back very briefly to the destruction at 90 days. I think you would appreciate, as most would, that once the destruction has occurred, it's very difficult to reassemble the information.

How do we balance that for our security agencies?

Mr. Daniel Therrien: Absolutely I appreciate that. That's why I say that the standard applied by the Federal Court at that 90-day stage is not a necessity. Perhaps somebody can help me with the standard, but it's essentially whether information would be useful for a national security investigation. That's a way to ensure that potentially useful information is not destroyed too early.

Mr. Dave MacKenzie: Thank you.

The Chair: The last five minutes go to Mr. Fragiskatos, please.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you very much, Mr. Chair, and thank you for being here today, Mr. Therrien.

I have a question about the connection between speech and privacy. I think you would agree that free speech and the right to it and to privacy enjoy a very intimate and indeed interdependent connection. Bill C-59 would replace one of the most controversial features of Bill C-51, the advocating of terrorism offences in general, with a more traditional offence, that of counselling specific terrorism offences.

We heard just the other day from Professor Stephanie Carvin, who in a piece for *The Globe and Mail*, wrote:

> This better respects freedom of expression while still recognizing that much speech — including terrorist recruitment and instruction — is a reasonable target for criminalization.

Can you comment on this change in Bill C-59 and what you make of it from a privacy perspective?

Mr. Daniel Therrien: I would agree; I don't have much to add to the analysis of Professor Carvin. To be frank, I focused more on SCISA, because it's the weakest part. I have noted, of course, the provision you are referring to, and I think it is an improvement inf terms of striking the right balance between freedom of speech, privacy, and ensuring the security of Canadians.

● (0945)

Mr. Peter Fragiskatos: In your comments—and you followed up on that matter—you made the point about privacy experts being involved with the NSIRA. Can you go into that a little further? Are we talking about an oversight role to ensure that the Privacy Act's provisions are being followed? You talked about examples specifically relating to travellers, but are there other examples you could mention to give us an idea of how officials focusing on privacy could have a role in such a body?

Mr. Daniel Therrien: Sure.

Yes, the application of the Privacy Act would be part of this, as would the lessons learned in the application of the Privacy Act otherwise in government to national security agencies. I think it's important that national security agencies be covered by specific rules, as in Bill C-59, but also by the legal regime of the Privacy Act, because these are emanations of the state, and as with all emanations of the state, they should be covered to the general rules applicable through the Privacy Act.

As an example of how we might add value, about two years ago we reviewed an incident involving the unfortunate but unlawful disclosure of metadata by the CSE to the Five Eyes. We played a very specific role. We did not look at all of the situation, but we looked at sufficient parts of it to examine the importance of metadata to privacy. We were able to look at the deficiencies, make recommendations on how to improve things, and play a public education role to make sure that the public was informed of the importance of metadata for privacy protection. That's something we added.

Mr. Peter Fragiskatos: Thank you very much.

I have one final question. You wrote an overview of C-51 in *The Globe and Mail* shortly after the bill was released. You said, "In a country governed by the rule of law, it should not be left for national security and other government agencies to determine the limits of their own powers."

On balance, are you satisfied that Bill C-59 has addressed this concern?

Mr. Daniel Therrien: On balance, Bill C-59 makes important improvements, but the recommendations I am making, particularly on the necessity threshold and legal safeguards for retention or destruction, are necessary to achieve the right balance.

Mr. Peter Fragiskatos: Thank you very much.

The Chair: Thank you, Mr. Fragiskatos.

On behalf of the committee, Mr. Therrien, I want to thank you and your colleagues for your very thorough presentation and just remind you that there was some undertaking to Mr. Paul-Hus concerning the survey, which I will look forward to receiving.

With that, we'll suspend.

● (0945)

(Pause)

● (0950)

The Chair: I call the meeting back to order.

We have in our next set of witnesses the Canadian Civil Liberties Association, and as individuals Christian Leuprecht and Hayley McNorton.

Unless you have any other way of ordering this, I am simply going to go in the order of the Canadian Civil Liberties Association first, Christian Leuprecht second, and Hayley McNorton third.

Is the Civil Liberties Association ready to go?

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association): I'm sorry, Mr. Chair. Cara Zwibel has just stepped out. She'll be here in just a moment. We would ask that someone else go first.

Thank you.

The Chair: Okay.

Christian Leuprecht, go ahead, please.

Dr. Christian Leuprecht (Professor, Department of Political Science, Royal Military College of Canada, As an Individual): We'll do it in two parts here. I'll set the scene, and then Ms. McNorton is going to explain the specific recommendations we have. I have copies of these. I have submitted them to the committee for translation, but I'm happy to circulate the documents.

The Chair: We should have you go first and Ms. McNorton second, and then we'll go back to the Civil Liberties Association.

Thank you.

Dr. Christian Leuprecht: Mr. Chair, I think we need to ask ourselves why we are here. I think one of the challenges we've had is that we hear a lot of tactics, but we don't hear a lot about what the strategy is and what the ultimate rationale is behind this. The rationale is that, as Canadians, we've long lived in an environment where we believed we have been safe by virtue of where we are in the world, which is very far away from all the troubles in the world. I would submit that this is no longer the case. The fundamental conditions have changed. The security threats and vectors are much broader and much deeper than they have ever been.

If you think about hypersonic manoeuvrable cruise missiles, intercontinental ballistic missiles, cyberspace, violent extremism, terrorism ideology, and also matters such as the globalization of organized crime, these are all things that we can't just keep away from our borders. They affect us here now, and they affect us every day. The security environment has fundamentally changed. The premise that we're somehow safe because we're far away from the troubles in the world simply no longer applies.

We've also, of course, seen these threats specifically associated with certain entities. This is often what's referred to as the four-plus-one issue: the four countries—China, Russia, North Korea, and Iran—and the plus one is transnational terrorism. In Canada we don't have a systematic human foreign intelligence service, so we rely disproportionately on our signals intelligence service to provide us the foreign intelligence we need to get domain awareness.

We also have the benefit of being part of the Five Eyes community. This membership should not be taken lightly. There is an international security hierarchy in the world. If you think about this as a pyramid, the United States is at the top and the Five Eyes community is below that. That means we need to be able to continue to be effective contributors to that community if we want to benefit from that community. The benefit from that community has precisely been that we have been able effectively to underinvest relative to most of our allies in defence, in security, and in intelligence because we have this force multiplier capability of domain awareness and overcoming the fallacy of composition that we wouldn't otherwise have. We need to balance here our obligations and the benefits to the community with the constraints that we impose on our own community.

We've also seen a fundamental change in the intelligence business as a result of two events, if you will. One is the advent of the Internet and of large data. The bad guys have been exploiting those systematically, and I would submit that in Canada we have been a little bit too easy on the bad guys who exploit the Internet and data, and too hard and making life a little bit too difficult for the people who are actually trying to disrupt, rein in, detect, and defend us against these nefarious entities. We need to strike a balance between the good guys and the bad guys. Of course, the advent of 9/11 has fundamentally changed the intelligence community and also the expectations the public has of the state in terms of keeping them safe and secure.

More than ever before, in light of the threats I've outlined, we are relying on intelligence to help us anticipate the security and safety challenges for Canada and to be able to mitigate those challenges effectively.

My fourth and final submission on this point is that, as a result of the Snowden revelations, much of the public has some skepticism about how the community operates. We are not here because there's in any way some large-scale violation of the professionalism or the capabilities in which the community does its job. We have the odd issue that comes up. Usually those issues are first identified by the community itself and then brought to the appropriate offices. We have a professional community, but we have the public that is skeptical, so I think the primary purpose of review here is to reassure the public that in a rule-of-law society and in a constitutional society everything is indeed on the up and up.

The other problem is that we have a massive public misunderstanding of what the community does, why it does it, and how it operates. That's as a result of the media, because where we see the community operate is largely on television where there are shows about law enforcement, intelligence, terrorism, and whatnot. If you watch those shows about the systematic violations of the rule of law and of constitutionalism, it makes for great television, but it is simply not how the community operates. However, this is what most Canadians and much of the public think is happening, reinforced by some of the ways the revelations by Edward Snowden have been interpreted and misinterpreted in much of the public discourse.

● (0955)

I would also say we need to be careful, then, in Canada with the security culture that we've created. In the Five Eyes community, we have, by far, the most restrictive privacy regime. This is a choice that we have made as Canadians, that what we are doing here is.... Other countries that have more rigorous parliamentary and other review mechanisms than Canada have also given their community more latitude in terms of how it can act, what it can do, and how it can do it.

In Canada, I'm a little concerned that, on the one hand, we're imposing considerable constraints on the ability of the community to be agile and flexible to continue to reassure the safety and security of Canadians, while at the same time, imposing this very strict review regime which, yes, is necessary to reassure the public, but we need to make sure we strike an effective balance here.

I hear lots of people constantly talk about privacy as if review were only about privacy, which, of course, is nonsense. There is review; there is oversight, yes, and there is compliance review, but review is also about efficacy. Are Canadians getting what they pay for from the community? Currently, nobody is really able to ask that question. We will now, as a result of these mechanisms, have the ability to ask those questions, and effectively, these committees will also be peer review for the community. Are they doing the best job they possibly can with the best methods and the best approaches that are available to them?

This discussion that it is simply about privacy, to me, misconstrues the broader benefits and payoffs of a more robust review regime by parliamentarians and by the now-revised community of review bodies that will have a broader remit overall.

I'll close on six questions that we need to ask ourselves when we try to introduce this type of legislation. What are the methods that should be used to hold the intelligence and security agencies to account? What ISAs, intelligence security agencies, should fall in the remit of those accountability bodies? Who is staffing those accountability bodies? What relationship does the accountability body have with the political executive? To what information does the accountability body have access? If there is more than one accountability body, how do they coordinate, and how do they prevent duplication?

This dovetails now with Ms. McNorton's recommendations that follow directly from some of these issues that we have laid out here that people need to think about when we implement such legislation.

The Chair: You have about two minutes left.

Ms. Hayley McNorton (Research Assistant, Department of Political Science, Royal Military College of Canada, As an Individual):

Mr. Chair, to enhance intelligence accountability, we have suggested five recommendations.

The first is that Bill C-59 does not describe if and how NSIRA, which is the national security and intelligence review agency, will support the National Security and Intelligence Committee of Parliamentarians. In the existing system, the committee of parliamentarians could apply to OCSE, the office of the CSE commissioner, the Security Intelligence Review Committee, or the Civilian Review and Complaints Commission, if they needed additional assistance. However, if Bill C-59 is passed, it will only apply to NSIRA or the CRCC. In regard to this recommendation, we consider how much support NSIRA will give the committee of parliamentarians and what kind of support they will give the committee of parliamentarians.

The second suggestion is that the Civilian Review and Complaints Commission should retain its ability to review issues and investigate complaints related to national security. The existing legislation giving NSIRA the ability to review matters related to national security issues goes against the recommendations from the O'Connor commission. Also, in the end, it would give the CRCC undue influence over what NSIRA reviews in regard to national security, because NSIRA will remain the principal point of contact for the complaints and reviews, which it would then refer to NSIRA.

The third recommendation is that NSIRA should have the ability to conduct joint investigations with provincial police and complaint bodies. The CRCC has this power as well. Basically, a lot of the federal intelligence and security agencies work with provincial police bodies, so that is also a consideration.

NSIRA should develop and establish standards for intelligence accountability.

Last, NSIRA should take reasonable steps to co-operate with the committee of parliamentarians to avoid unnecessary duplication of work in relation to the fulfillment of their respective mandates.

● (1000)

The Chair: Thank you very much.

I see the Civil Liberties Association. I assume you're ready.

Ms. Cara Zwibel (Acting General Counsel, Canadian Civil Liberties Association): Yes, my apologies to the committee for coming in late.

Thank you, Mr. Chair, and members of the committee. The Canadian Civil Liberties Association appreciates the opportunity to make submissions with respect to Bill C-59.

CCLA was a vocal critic of the Anti-terrorism Act passed in the last Parliament and initiated a constitutional challenge to a number of aspects of that law, which remains in abeyance pending consideration of Bill C-59. While this new bill has partially addressed some of Bill C-51's constitutional deficits, it has certainly not resolved all of them. The bill also grants our national security agencies a number of extraordinary new powers that have not been adequately justified and that do give rise to very real civil liberties concerns. The government has framed this bill as being about protecting both national security and rights, and CCLA supports both of these goals, and our comments and recommendations are made in that spirit.

We will begin by identifying the positive changes Bill C-59 makes to former Bill C-51, outline the issues that remain unaddressed, and finally, set out the new problems created by Bill C-59.

Since we certainly can't cover everything in 10 minutes, we'll also be filing a more detailed written submission. Beginning with the items that Bill C-59 has improved, we are reassured by the government's amendments to the terrorist speech offences. Without these amendments, the provisions violate sections 2 and 7 of the charter and may also undermine community-based deradicalization efforts. While the amended offence is arguably unnecessary, given the large number of pre-existing terrorism offences in the Criminal Code, counselling offences are a known quantity in the criminal law and follow a clear legal framework. However, the language of "terrorism offence" in the amendment would be better changed to "terrorist activity", which is a defined term in the code.

On information sharing, Bill C-59 adds new proportionality and reporting requirements, which is a distinct improvement over the largely unaccountable system introduced in Bill C-51. However, the definition of "threats to the security of Canada" that triggers information disclosure remains unduly broad and circular. It is not clear why this definition is so much broader than the one included in the CSIS Act, and we remain concerned that constitutionally protected acts of advocacy, protest, dissent, or artistic expression, particularly by environmental and indigenous activists, will continue to be swept up in the process.

One of the most controversial aspects of Bill C-51 was the threat reduction powers granted to CSIS and the accompanying warrant provisions that appeared to allow for judicially sanctioned charter breaches. We do not doubt that there are times when CSIS may see an opportunity to take action to reduce the threat to the security of Canada. What is unclear is why this goal cannot be achieved through better communication and co-operation between CSIS, the RCMP, and other law enforcement bodies. This is a very significant shift in mandate that appears to ignore the historical reasons for separating law enforcement and intelligence in the first place, and there has been no convincing case made for why this shift is necessary.

Moreover, the legal framework for the exercise of these powers established in Bill C-51 was deeply problematic and clearly unconstitutional in our view. The scheme as modified by Bill C-59 is an improvement. It establishes clearer contours around what actions are permitted and what is prohibited, and the warrant scheme appears to be intended to ensure that the charter rights of individuals are respected. If CSIS is to continue to have these powers there are a number of ways in which we believe the scheme should be improved.

First, the requirement for CSIS to consult with other federal departments or agencies to see if they can reduce the threat should be amended to clarify that if a law enforcement body is better placed to do so, CSIS should not pursue threat reduction. Second, the list of measures set out in proposed section 21.1(1.1) only require a warrant where CSIS determines that they may violate the law or limit a charter right. A warrant should be required in any case where these measures will be pursued by CSIS. It is vital that the determination of whether a law is being violated or a charter right limited not be left solely to CSIS.

Finally, the new national security and intelligence review agency should be required to report on the number of warrants issued under proposed section 21.1, and the number of requests that were refused. SIRC does so now, and reducing reporting requirements is not consistent with Bill C-59's stated goal of enhancing accountability.

Some of the most problematic aspects of Bill C-51 received only cosmetic improvement or none at all. As this committee is aware, the passenger protect program continues to raise serious constitutional problems. The process by which individuals are placed on the list remains opaque, and proposed redress mechanisms are inadequate. Bill C-59 also fails to correct the flawed appeals procedure, which parallels the system in place for security certificates prior to the Supreme Court's Charkaoui decision in 2007.

● (1005)

While the no-fly list is undoubtedly different from being named in a security certificate, both have the ability to substantially interfere with the constitutionally protected rights and liberties of an individual and to seriously impact their lives and families. The current process allows the use of hearsay and secret evidence, without access to a special advocate able to test that evidence or to represent the interests of the listed person.

This committee recognized these profound issues in May when it recommended the use of special advocates in no-fly list proceedings, among other safeguards, and yet Bill C-59 does not address these concerns. It should do so by adopting this committee's initial recommendation. We would note that the terrorist entities list raised similar issues.

Ms. Lex Gill (Advocate, National Security Program, Canadian Civil Liberties Association): Mr. Chair, another deeply problematic aspect of Bill C-51 that has not been touched are changes to the Immigration and Refugee Protection Act that undid important protections for named persons in security certificate proceedings. Bill C-51 limited the requirement for disclosure of relevant information to special advocates and introduced a series of procedural barriers which further disadvantaged the rights of the named person.

In our legal challenge, CCLA has argued that these amendments are an unconstitutional violation of the section 7 guarantee to a hearing before an independent and impartial tribunal. Our Supreme Court has affirmed that the individual named in the security certificate "must be given an opportunity to know the case to meet, and an opportunity to meet the case", an impossible exercise in the absence of a coherent legal framework for full disclosure.

This committee recognized as much in May 2017 when it recommended amending IRPA in order to give special advocates full access to complete security certificate files. We urge that Bill C-59 be amended to correct this issue.

We move now to the new elements of the new national security landscape that Bill C-59 has introduced. Our written submission will address a much wider range of issues in relation to the CSE Act, but we would like to highlight two parts today.

First, the proposed active and defensive cyber-operations aspects of the CSE's mandate essentially allow the establishment to engage in secret and largely unconstrained state-sponsored hacking and disruption. The limitation of not directing these activities at Canadian infrastructure is clearly inadequate given the inherently interconnected nature of the digital ecosystem. Such activities are also bound to impact the privacy expression and security interests of Canadians and persons in Canada, and may threaten the integrity of communications tools such as encryption and anonymity software that are vital for the protection of human rights in the digital age.

In the case of CSIS's disruption powers, which are in some ways analogous to these new aspects of CSE's mandate, the government has set out a complex framework for prior judicial authorization and a longer list of prohibited activities. While we do not concede the adequacy of that framework, it is notable that, in contrast, CSE's cyber-operations activities involve no meaningful privacy protections, require only secret ministerial authorization, and involve only after-the-fact review.

Second, while the majority of CSE's activities cannot be directed at Canadians or persons in Canada, this is an inadequate safeguard against CSE's overreach in the face of unselected bulk collection. Bill C-59 exacerbates this privacy risk by creating a series of exceptions for the collection of Canadian data, including one which allows its acquisition, use, analysis, retention, and disclosure, so long as it is publicly available.

This definition is so broad that it plausibly includes information in which individuals have a strong privacy interest, and potentially allows for the collection of private data obtained by hacks, leaks, or other illicit means. Furthermore, it may encourage the creation of grey markets for data that would otherwise never have been available to government—a client with deep pockets.

The government has failed to demonstrate why this exception, as worded, is necessary or proportionate, or what risk it is meant to mitigate in the first place.

● (1010)

The Chair: I appreciate that time is the enemy here, but you're speaking so quickly that the interpreters are having difficulty keeping up.

Ms. Lex Gill: My apologies.

The Chair: Could you slow it down a bit, please.

Ms. Lex Gill: Absolutely.

The government has failed to demonstrate why this publicly available information exception as worded is necessary or proportionate, or what risks it's meant to mitigate in the first place. The CSE has identified a need to access reports on the global infrastructure as a justification for this provision, yet a more narrowly defined list of information types would easily respond to such a need.

While section 7 specifies that privacy must be considered, the nature of the protection is vague; the regulations setting out the scope of protection are likely to be secret, and the potential for invasive information collection and abuse is high.

The parallel term "publicly available dataset" in the CSIS Act remains undefined but appears to replicate the same types of problems.

Finally, we welcome the new accountability mechanisms in Bill C-59 and strongly support the creation of the new, integrated review body, and the introduction of an intelligence commissioner with the ability to exercise quasi-judicial oversight. However, we are concerned that significant gaps remain. The commissioner only issues reasons when rejecting an authorization. The reasons are kept secret from the public. There is no adversarial input. The authorizations will continue to be issued on a class basis, and there is no framework for appeal or review of decisions except by the minister and the intelligence agencies themselves.

Without amendments that strengthen the role of the commissioner, his or her ability to exercise meaningful oversight and control will be limited in practice.

We welcome questions from the committee about these issues and other aspects of Bill C-59.

The Chair: Thank you very much.

The first questioner is Mr. Fragiskatos.

I think the issue is kind of joined here with this panel, so if there is a will on the part of one of the other persons wishing to respond, you might get the attention of the questioner or me so that you can engage.

Mr. Peter Fragiskatos: Thank you, Chair.

Thank you to all of you for being here today.

My first question goes to Mr. Leuprecht and Ms. McNorton.

In a recent *Toronto Star* piece, you noted that the National Security and Intelligence Committee of Parliamentarians lacked a security background among the members that had been appointed. There are some members who have some experience in the realm of security, but by and large, you said there was a lack of experience and expertise.

I think you would agree that there is something to be said about an outsider's perspective, on the condition that there is advisory opportunity in the form of a secretariat to assist in the work and provide information, and that kind of expertise and background. You would agree that's a necessary thing.

Dr. Christian Leuprecht: I think one of the strengths of parliamentarians is that they are generalists and that they have to deal with wide ranges of legislation. My concern is that there is a lot disinformation and misinformation in this particular realm and it can be very difficult to understand, because most people have not worked in the actual community and don't understand.

Mr. Peter Fragiskatos: Point taken. I just wanted to offer that idea—we're on the same page—because there is something to be said about an outsider's perspective.

Staying with the committee of parliamentarians, you have argued, and others have argued, for example, Professor Wesley Wark, whom we heard from just the other day, that this committee will need research and advisory support in the form of an independent secretariat. The question is, where should the experts be drawn from? Wesley Wark said, "Are they too close to the security and intelligence community? Are they going to be too pal-sy? Too much a defender of the security and intelligence community?"

Is that a concern that you have? Go into that, if you could, because I think it's an interesting point.

Dr. Christian Leuprecht: There are always trade-offs, but I think the expertise is critical for the committee to ask the right questions and to know what information to ask for from the community.

I would also submit that we propose people, for instance, who are done with their careers, who have retired, so they have nothing at stake, per se, in the overall undertaking. These are folks who have decades of careers as professionals. If there is a community in the country that takes both their job and the need to absolutely respect the law 100% every time absolutely seriously, it is the security and intelligence community federally, provincially, and locally in this country.

● (1015)

Mr. Peter Fragiskatos: You don't see a danger in the same way that Professor Wark does, that perhaps there would be too much of a close relationship. As he said, are they too close to the security and intelligence community to offer the kind of independent advice and analysis that would be necessary for the parliamentarians to carry out their work?

Ms. Hayley McNorton: There has been a precedent set with some of the existing intelligence accountability bodies that hire employees who have experience with the intelligence and security agencies in Canada. As far as I know, they have not had a problem with it. Additionally, there are also tests that can be employed to test the loyalty of employees.

Mr. Peter Fragiskatos: Would the Civil Liberties Association have a view on that?

Ms. Cara Zwibel: I don't think we have a comment.

Mr. Peter Fragiskatos: Okay.

Again, Professor Leuprecht and Ms. McNorton, you point out that you have a fear of overlap of work between the committee of parliamentarians and the NSIRA. Could you go into that in greater detail?

Ms. Hayley McNorton: Considering the broad mandates of both NSIRA and NSICOP, there is a potential for overlap, especially in what they review for. They both could technically review issues related to efficacy, compliance, innovation of agencies.

They're geared toward different things. For example, the parliamentarians have a diversity of expertise, so they would be very useful in reviewing legislation. According to Bill C-59, NSIRA is made up of former SIRC members. They have the experience and intelligence accountability to look at things that are more geared to compliance. However, there probably will need to be some kind of delineating of responsibilities to prevent overlap and the minimization of duplication of work.

Dr. Christian Leuprecht: We also want to consider that every time one of these committees makes a request to the agencies, given there's no new money to the agencies to support all these new requests, this is effectively a cut in the budgets to the agencies themselves. We want to make sure that committees coordinate so that we also afford the agencies as efficient an opportunity to respond, rather than having to provide very similar things to multiple committees.

I think that the greatest payoff for the taxpayer and for parliamentarians and Canadians will be a clear division of labour among these entities based on the particular areas of expertise that they bring to bear. For NSICOP, one clear advantage is that now we finally have somebody who can advocate for changes in legislation. We know there are many pieces of flawed legislation. This government is addressing several of them in this parliamentary period, but when cabinet meets, they are never high enough to actually make it on the cabinet agenda. For years, we have had MCs, memoranda to cabinet, to make changes that don't actually ever make it through cabinet. Now, we actually have advocates. We have legislators and parliamentarians who can make sure the legislation is as effective as possible, both on the constitutionality and legality side and relative to a changing security environment.

Mr. Peter Fragiskatos: It's certainly a welcome development and an important one.

Professor Leuprecht, you have argued in the past that to meet the security challenges that Canada faces, we would need to "improve professional development mechanisms to build the skill sets and recruit the skill sets into our national security organizations". There's a lot about skill sets there. In your view, are we doing that well enough, currently?

Dr. Christian Leuprecht: There are agencies that do it better and agencies that could benefit from some improvement. I think we have a very careful selection process and professional development process, for instance, among the Canadian Armed Forces, and within the Communications Security Establishment to a large degree, also within CSIS. However, on the law enforcement side, we also know that there is considerable opportunity for improvement on capabilities, capacities, and skill sets. For instance, while I respect the suggestions that CSIS should stick to it's knitting and, as far as possible, basically have other agencies deal with particular issues, I would submit to you that, yes, in the best of all worlds, we would want to have the RCMP do things, like disruption and whatnot. However, my submission to you is that the RCMP is struggling on so many fronts already that I think we also need to figure out where the relative advantage of different organizations lies and allow them to bring it up to speed.

● (1020)

The Chair: Thank you.

Mr. Motz, please, you have seven minutes.

Mr. Glen Motz: Thank you, Mr. Chair, and thank you to both groups for being here today.

Mr. Leuprecht, you had said in previous testimony on Bill C-51, "CSIS is the most reviewed intelligence security service in the western world and therefore, I think we can safely say in the world as it is." In your reading of Bill C-59, are there any new layers of review placed upon CSIS, and do you think those are helpful in helping CSIS fulfill it's mandate?

Ms. Hayley McNorton: Under the new legislation, the NSIRA has a wider remit when it comes to reviewing Canadian intelligence and security agencies in general, and they do have the potential under a different mandate to not only review more but also help CSIS innovate in different ways. Therefore, yes, they are reviewed to a more...sorry, I didn't catch the latter part of your question.

Mr. Glen Motz: Do you think those are helpful in CSIS fulfilling its mandate?

Ms. Hayley McNorton: Yes. I definitely think that NSIRA has a greater potential to enhance the compliance, the efficacy, and the innovation within CSIS.

Mr. Glen Motz: Thank you.

Dr. Leuprecht, the powers in Bill C-51 are not uncommon. You had said in your testimony, again on Bill C-51, "Canadians have a profound misconception of what disruption constitutes. CSIS being able to talk to parents to tell them that their child is up to no good is a disruption power." I can go on with that, but with the changes proposed in Bill C-59, particularly in securing a warrant to conduct certain disruption activities, do you believe we are heading in the right direction with this legislation on that particular front?

Dr. Christian Leuprecht: The challenge is always, as my colleagues also pointed out, in reassuring Canadians that the activity in which the service engages is compliant with the Constitution and the rule of law. While I am personally satisfied that the service engages with the utmost professionalism when it comes to the use of its disruption powers, such a measure may be justified in some cases as a way to reassure Canadians about the expanded powers that CSIS has been given. Also, where there is controversy over whether these powers should reside with CSIS or with law enforcement—and I explained why I think, for better or for worse, for the time being they need to reside with CSIS—the warrant measures may be necessary to ensure the legitimacy and credibility of the activities in which CSIS engages.

Mr. Glen Motz: All right.

Ms. Cara Zwibel: May I have an opportunity to answer that question?

Mr. Glen Motz: Please do.

Ms. Cara Zwibel: We feel that the scheme laid out in Bill C-59, as we said, is an improvement in terms of clarifying what the contours of threat disruption look like and making clearer to both the public and to the service itself what the acceptable and prohibited bounds are. In particular, the addition of prohibited activities, including detention, was in our view quite an important one.

I want to reference that when we expressed concerns about disruption and why this is not being done by law enforcement, some of that has to do with making sure we can effectively prosecute people once we determine they've done something contrary to the law. The other thing is that we've never been particularly concerned about the kind of disruption you mentioned, such as talking to a parent and saying, "Your child's been getting into some trouble." We're more concerned with some of the items that are now specifically enumerated in the legislation—things like fabricating or disseminating any information, record, or document; altering or removing websites and communications, and things like that. It's helpful, in our view, to have those in the legislation.

We have suggestions for how the warrant scheme might be improved, and we can elaborate on those in our written submissions.

● (1025)

Mr. Glen Motz: Thank you.

Mr. Leuprecht, from your background and history of working in cybersecurity, are there steps we need to be taking to protect our critical infrastructure? Does restricting CSE to reacting to significant and widespread threats help Canada or delay our ability to respond?

Dr. Christian Leuprecht: The government's proposed establishment of an act for CSE itself is a huge improvement and innovation over the current situation, where it is embedded in the National Defence Act.

I would say that on cybersecurity in this country, by and large not only do we have our head in the sand, but we need to do much better, especially at the intelligence sharing. The CCTX, the new mechanism to exchange cyber-intelligence, is a good improvement here. One challenge we have had is that CSE is, by law, extremely restricted as to what it can share with the private sector, and under what conditions. In this area, you ultimately need to prevent, anticipate, and have effective and timely intelligence sharing, given how quickly cyber-challenges and threats move. It is integral.

Other countries are much further ahead, if you look at Australia, the Netherlands, Israel, or the United Kingdom. This is what's sometimes known as phase two. If we cannot effectively protect our cyber-infrastructure, that is going to have a deleterious consequence for our economy, because people will only invest in innovation, in R and D, in the Canadian economy if those elements are then also protected. Why would you invest, if that's going to be immediately stolen? We know this country has done particularly poorly on the innovation agenda, and luckily, this government is trying to improve Canada's innovation capacity. That will not be effective if we can't then also ensure that the cyber-domain is effectively protected.

Ms. Lex Gill: Sorry, Mr. Chair, may I have an opportunity to respond to that question as well?

Mr. Glen Motz: I have 30 seconds. I have one more question I want a response to. Sorry.

Bill C-59, as we've heard from the Department of Justice, will make it more difficult for law enforcement to secure preventative arrests. Now, because the threshold to secure such an order is being raised, do you, Mr. Leuprecht, consider this to be problematic?

The Chair: We're going to have to hold the answer to that question, because we've just run out of time.

Mr. Glen Motz: Could you provide the answer to the question to the committee in writing?

Dr. Christian Leuprecht: Yes.

The Chair: Mr. Dubé, you have seven minutes. Go ahead, please.

Mr. Matthew Dubé: Thank you, Mr. Chair.

I don't know if you want to answer that question, because I'm coming to the cybersecurity stuff as well.

Ms. Lex Gill: I would love to. Thank you for the opportunity.

The question was about how Canada's cybersecurity can be improved. I would like to draw the committee's attention to the active and defensive cyber-operations aspects of CSE's mandate, that have been added in proposed sections 20 and 19 respectively. It's our position that the inclusion of these two aspects and the activities that come along with them may actually run counter to Canada's broader security interest.

I would draw the committee's attention in particular to the short list of prohibited conduct in proposed section 33. I think there are at least three fundamental problems with that proposed section. The first issue is that, for reasons that are not clear to us, the explicit limitations for prohibited conduct apply only to authorizations issued under the defensive and active cyber-operations component of the mandate and not to the rest of CSE's activities.

The second issue is that neither “justice” nor “democracy” is defined in the act, leaving the limitation about interfering with the course of justice and democracy vague and open to perhaps creative interpretation.

The third problem is that this short list of prohibited conduct, from our perspective, is radically under-inclusive, and at minimum the committee should compare the list with that in proposed subsection 21.1(1.1) of the CSIS Act with that in proposed subsection 33(1). We are concerned about the broad scope of potential activities that CSE would be able to conduct under these aspects of the mandate. We're not convinced that they've been appropriately justified.

Mr. Matthew Dubé: Thank you for that.

I want to stay in part 3 of the bill as well and look specifically at proposed section 24. I'm hoping to hear from everyone but in particular from you, Ms. Gill.

You mentioned encryption software and some of the applications that are used and not used just by so-called bad guys but also by law-abiding Canadians seeking to protect their privacy. In the course of, in particular, proposed paragraphs 24(1)(b) and 24(1)(c), where we're talking about essentially testing and studying information infrastructure and evaluating software and testing them for vulnerabilities, does that potentially create a situation in which we can go down that rabbit hole to find ways to counter some encryption that can be used for the lawful purposes of simply having the peace of mind of protecting your privacy?

● (1030)

Ms. Lex Gill: Certainly, we know that allied intelligence agencies have engaged in the past in activities meant to interfere with or undermine encryption on anonymity tools. I think we should be concerned about those types of operations, not just in the course of the testing and infrastructure information aspects under proposed section 24, but more generally in the pursuit of the foreign intelligence mandate. Encryption and anonymity tools are vital to protecting the safety of Canadians and persons in Canada as well as Canadian infrastructure. We should be concerned if CSE ends up inadvertently working at cross-purposes by interfering with the very tools designed to protect us.

I would also raise something that's been raised in the past, which is that there's no public framework for disclosing vulnerabilities. While CCLA doesn't have a concrete position on that yet, it is an open issue, from our perspective.

Mr. Matthew Dubé: When you say “disclosing vulnerabilities”, do you mean CSE disclosing those to, say, the private sector, so, for example, a telecom company?

Ms. Lex Gill: Right. It's responsible disclosure to ensure that where CSE finds vulnerabilities and where it's appropriate in the public interest to do so, that they are disclosed responsibly in order to protect privacy interests as well as expression interests. This is not just about privacy rights. Of course, these types of technologies, our digital ecosystem is an important guarantor of the right to freedom of expression protected under paragraph 2(b) of the charter as well as broader interests of security and liberty that all Canadians and this committee are very concerned about.

Mr. Matthew Dubé: I also wanted to look at proposed subsection 24(4), Information acquired incidentally. I don't know if you had any thoughts on that, where it says:

> The Establishment may acquire information relating to a Canadian or a person in Canada incidentally in the course of carrying out activities under an authorization issued under

and then it lists the appropriate subsections.

Especially in the context of information sharing, is there any concern with that type of provision?

Ms. Lex Gill: That's something we hope to detail more explicitly in our written submission.

We are concerned about that. The word “incidentally” is defined but the limitation of not directing is not defined anywhere in the act, and that's a concern that experts, including Bill Robinson, have raised in the past. This would help better define the contours of what we mean. Certainly, to the extent that CSE engages in unselected bulk collection, there will be incidental collection of Canadian data. We do have to make sure that explicit, clear, and detailed measures are taken to ensure that this information is handled responsibly where collected.

Mr. Matthew Dubé: Okay.

My last question on part 3 concerns the many sections dealing with ministerial authorizations. I don't know whether you have any thoughts on that. In particular, one aspect is the extension of the period of validity without its being subject to review by the commissioner created by this very same bill.

Ms. Lex Gill: We are concerned about the ability to extend by the one-year period, but we think it's important that where there's a significant change in the scope of the authorization, it be brought to the commissioner's attention. We think that's important.

We want to also raise that the authorization framework for active and defensive cyber-operations is extremely problematic from our point of view, insofar as those operations have the capacity to significantly interfere with express privacy or security interests of Canadians and persons in Canada and persons elsewhere. We don't believe that ministerial authorization through the minister and the Minister of Foreign Affairs is sufficient. We would prefer to analogize these types of powers to the disruption or reduction powers in the CSIS Act. We note that there is a much more rigorous system for oversight and prior authorization in that context.

I would also note that if the committee decided not to adopt these aspects of the CSE Act that allow CSE to engage in active defensive cyber-operations unbound from other aspects of its mandate, CSE could continue to assist CSIS through its assistance mandate in the course of threat reduction activities.

Thank you.

● (1035)

Mr. Matthew Dubé: It's judicial oversight, essentially.

Ms. Lex Gill: That will be detailed in our written submissions. For now, what I feel comfortable putting on the record is that we're not comfortable with ministerial authorization alone.

Mr. Matthew Dubé: Thank you.

The Chair: Ms. Damoff, you have seven minutes.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Chair.

Before I start, I have a student shadowing me today. I want to recognize Ian Lewis, who is here. He's a student here in Ottawa. I think it's wonderful that he's taken an interest in what the national security framework in this legislation is looking at.

During our previous study on the national security framework, there was a lot of desire on the part of Canadians for greater transparency from the intelligence and security agencies. We also heard that when we were looking at Bill C-22. A witness we heard at the last meeting, Dr. Stephanie Carvin, was quite passionate about calling for better transparency. She cited a couple of models to look at. One was the U.S. Office of the Director of National Intelligence's worldwide threat assessment report as well as the recent report on cyber-threats to Canada's election system and democratic institutions by the Communications Security Establishment.

I wonder whether both of you might comment on that and say whether you see it as something that should be included in the legislation we're looking at or whether it's something that would be looked at more through regulation or ministerial directive.

Ms. Hayley McNorton: I think the NSIRA provides a greater transparency, because they have several different types of reports, including annual reports and agency-specific reports, that they must submit to Parliament. They have a number of reports going to Parliament that parliamentarians as public representatives of people can read and analyze and speak about.

I think that will speak a lot to enhancing transparency. The agencies themselves, specifically CSE and the existing account-ability bodies, have made a publicity push to get people to know what they do and how they do it and give them more information regarding it.

Ms. Pam Damoff: Just before we move on, when she was here she was talking specifically about the U.S. report dealing with specific threats. It outlines the number of threats. It was very specific on threats within the United States. In this it differs, I think, from the reports that we'll be getting to Parliament right now.

Dr. Christian Leuprecht: I think there is a need for demystification, because of course our adversaries play actively in this environment on a permanent basis. The cyber-threat is the single greatest threat to our national security, to our democracy, our social harmony, and our prosperity today. I think there is opportunity here to be more systematic in the way we communicate that fact to Canadians.

Also, however, we currently don't do particularly well in the area of small and medium-sized enterprise. Large enterprise has the capacity; small and medium-sized enterprise—the people who generate much of our prosperity, our innovation, and much of the employment in this country—currently do not have access to those tools. Any mechanism the government can agree upon to inform people better and give, for instance, organizations such as CSE more capacity to support small and medium-sized enterprise would be critical. I think a report is one effort to that effect.

Ms. Pam Damoff: Okay, thank you.

Did you have any comment on that?

Ms. Brenda McPhail: Yes. Thank you.

I think that, in general, the CCLA would share Professor Carvin's passion for the concept of transparency. In relation to the U.S. report on specific threats, one thing we often hear, as a civil liberties organization, when we make comments that are perceived to be idealistic about national security and accountability, is that we don't understand what's really going on. A report such as you're referring to, which actually shares with all Canadians the nature of real and existing threats, would provide, I think, an important framework for every Canadian and every civil society group to be able to make more rational assessments in relation to these kinds of analyses and processes that we're going through today. It would enhance public trust that things are happening as they should, that risks are real, and that we therefore have the clear and specific procedures enacted in legislation to deal with the kinds of threats that we're legitimately facing.

● (1040)

Ms. Pam Damoff: Thank you very much.

My next question has to do with the minister's testimony when he was before this committee on Bill C-59. He was talking about the changes from Bill C-51, amending, advocating, and promoting the commission of terrorism offences in general, and replacing the offence to apply only when a person specifically counsels another person to commit a terrorism offence. It provides a clear and more appropriate legal structure surrounding them. When he was questioned, he was asked if this would actually provide law enforcement with better tools to be able to enforce.... Now, you had mentioned that you thought the definition was still too broad. I don't know if you had an opportunity to see what the minister was saying in terms of it actually narrowing the definition to allow law enforcement to enforce....

I'd also welcome comments from both of you on that.

Ms. Cara Zwibel: I didn't have the opportunity to see all of the minister's testimony, but I do know, and we do agree, that this is an improvement in terms of narrowing the offence considerably. In our view, it's still arguably unnecessary, since counselling any offence that's already an offence under the Criminal Code is already an offence. So it's not exactly clear what this offence is doing. The fact that it references terrorism offences, which is not actually a defined term in the code, makes me think that there may be some interest in being able to prosecute someone for counselling without having to specify which terrorism offence in particular they were counselling, which is potentially problematic from a rule of law perspective, in terms of someone understanding what it is they're charged with and where the bounds of the law are. The list of terrorist activity in the code—and that's the language we think should be inserted into that provision—is quite long, and it does include a number of things that fall well beyond any acts of violence, that is, things that are participating in or that may be facilitating terrorist activity. So we think it could be sharpened and clarified by making that amendment.

The Chair: We'll have to leave it there. Thank you very much.

Ms. Leitch, we're down to about three minutes.

Hon. K. Kellie Leitch (Simcoe—Grey, CPC): Thank you very much, Mr. Chairman.

Thank you, all, for taking the time to come today.

Mr. Leuprecht, I'd like to ask you one particular question. I guess it's in follow-up to your comment about how Canada no longer lives in an isolated part of the world with respect to these issues around security.

Bill C-59, we've heard from the Department of Justice, will make it more difficult for law enforcement to secure preventative arrests because the threshold is being raised to secure such an order. I was wondering if you could make some comments with respect to that and your perspective on it.

Dr. Christian Leuprecht: The challenge in that space is that you ultimately have to be preventative, and different countries have different mechanisms. The Australian Criminal Intelligence Commission has fantastic mechanisms that work very well in this particular sphere. I'm concerned about the reduction of the ability to work in a preventative space.

I'm also—and this ties in with the previous question—deeply concerned that we have upwards of 120 Canadians who have returned to this country, some of whom have pillaged, raped, killed, and are able to return to this country and live here with impunity because we do not have the legislative instruments to bring them to justice.

To that effect, it's helpful to have some changes with the Criminal Code, but we need other offences, including offences, for instance, that make it illegal to travel to certain parts of the world, which has proven a very effective measure in Australia to prosecute people who engage in this type of activity. I think we're tinkering at the edges here when it comes to preventative arrest and when it comes to how exactly we define it, to hopefully make it more effective for law enforcement to use the tools that we have. I think there's a lot more that needs to be done.

Hon. K. Kellie Leitch: I've been meaning to ask all of you another question.

In your reading of Bill C-59, each of you have made some comments on the number of layers and whether or not new reviews would be placed on CSIS and their capacity to be able to do things. Do you think it's helpful in allowing CSIS to meet its mandate by having these additional layers? Mr. Leuprecht, you had commented with regard to the issues around methodology and how that would be implemented. Could you comment and then we'll come back to the others?

● (1045)

Ms. Hayley McNorton: I think that in order to allow CSIS to complete their mandate in time while making the most of their resources, that the committee of parliamentarians and the review agencies should coordinate on how they get information from CSIS, whether it's through their parliamentary liaison to save time and not be such a burden on the agency.

Dr. Christian Leuprecht: There is a cost to every layer of review and oversight that we impose on agencies. Without additional funding, in a democracy we need to weigh the trade-offs we engage in, but as we mentioned, there are potentially quite positive outcomes, especially in efficacy and innovation for the community itself, as a result of the work that will be done.

The Chair: Thank you, Ms. Leitch.

On behalf of the committee, I want to thank all of you for your contributions. We look forward to receipt of your further submissions as may be required.

Thank you very much.

The meeting is adjourned.