HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 096 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 8, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, February 8, 2018

● (1100)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I call to order the 96th meeting of the Standing Committee on Public Safety and National Security.

We're going to go a little bit out of order because Ms. Damoff, with the gracious consent of the opposition parties, has a motion that I hope we can dispose of without debate. If it goes to debate, we will put it to the end of the meeting because I don't want to take away from time with the witnesses.

Ms. Damoff.

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

Thanks to the opposition.

I'd like to bring forward a motion:

> That the motion adopted by the Committee on Tuesday February 6, 2018 regarding the submission of amendments to Bill C-59, An Act respecting national security matters, be rescinded and replaced with the following:
>
> That notwithstanding the motion adopted by the Committee on Tuesday, May 3, 2016, the date of March 8, 2018 be designated as the deadline for the submission of amendments to Bill C-59, An Act respecting national security matters, by Members of the Committee as well as by Members who are not part of a caucus represented on the Committee.

The Chair: Thank you, Ms. Damoff.

If there any debate?

(Motion agreed to)

The Chair: Thank you, all.

Witnesses, thank you for that indulgence.

We have, for the first hour this morning, Laura Tribe, executive director of OpenMedia; and from the International Civil Liberties Monitoring Group, Timothy McSorley.

You each have 10 minutes for your initial presentation.

Ms. Tribe.

Ms. Laura Tribe (Executive Director, OpenMedia): Good morning. My name is Laura Tribe, and I am the executive director of OpenMedia, a community-based organization committed to keeping the Internet open, affordable, and surveillance-free.

I'm here today with Tim McSorley of the International Civil Liberties Monitoring Group, who were unfortunately not invited by the committee to testify in these proceedings, but whose contributions OpenMedia believes to be critical for an informed discussion of Bill C-59.

OpenMedia's work on privacy and digital security dates back to Bills C-13 and C-30, but has focused more recently on the serious security violations introduced by the previous government's Bill C-51. The OpenMedia community's lengthy efforts on these issues include producing “Canada's Privacy Plan”, a positive vision for the future of privacy in Canada that was crowdsourced from over 125,000 contributors; over 300,000 people speaking up against Bill C-51; two national days of action against Bill C-51, organized in partnership with organizations across the country; over 15,000 citizen comments submitted to the government's national security consultation; and over 6,000 submissions to this committee's written consultation on Bill C-59.

Public Safety Canada's report summarizing the national security consultation results showed that Canadians are overwhelmingly in favour of increased protections for personal privacy. More than four in five responses indicated that their expectation of privacy in the digital world is the same as or higher than in the physical world.

As a result, when Bill C-59 was introduced, we were relieved; it was a sign that change was coming. However, the more we analyzed the bill, the more our worries returned. The changes are less substantive than we had hoped, and invasive new powers were even introduced.

Bill C-59 fails to adequately address the information disclosure provisions and terrorist speech offences brought in by Bill C-51, but also brings in new data collection, cybersecurity, and information-sharing powers that further threaten our privacy and security.

Today this committee has a chance to make this right. Over 6,000 Canadians submitted their concerns about Bill C-59 via OpenMedia's written submission to this consultation. Since then, in the past two weeks, we've had almost 10,000 more Canadians sign a new petition concerning the expanded cyber-operations powers proposed in the CSE act included within Bill C-59. It's addressed to the Standing Committee on Public Safety and National Security and reads:

“As a concerned Canadian, I am urging you to address the dangerous new powers being proposed for CSE in Bill C-59. Throughout the process of reforming Bill C-51, Canadians have been very clear on the need to scale back the drastic and invasive national security measures in the bill.

“Public Safety Canada's own 'What We Learned' report, which formed the basis of Bill C-59, confirmed that a majority of stakeholders and experts called for existing measures to be scaled back or repealed completely, and that most participants in the consultations 'opted to err on the side of protecting individual rights and freedoms rather than granting additional powers to national security agencies and law enforcement...'.

“The new active and defensive cyber-operations powers proposed in Bill C-59 for CSE are directly opposed to the wishes of the majority of Canadians. We asked for privacy, but instead we got an out-of-control spy agency with even more extreme powers than before.

“Security and privacy experts throughout Canada have expressed in great detail the issues with the proposed bill and the changes that need to be made to protect the privacy and security of Canadians. Experts have warned of the consequences of granting powers like these, powers that will be all the more dangerous given the lack of adequate oversight included in the bill.

“I would like to point you to the 'Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59' report, produced by the Citizen Lab and the Canadian Internet Policy and Public Interest Clinic, CIPPIC. The recommendations laid out in this report should be adopted by the SECU committee.

“In a world and time where digital technologies are being used by so many to threaten our digital safety, we need our government to be helping make the world better, not actively undermining our security.”

As of this morning, our petition has been signed by 9,633 Canadians. On behalf of these signatories, plus the over 300,000 against Conservative Bill C-51, and the other concerned civil society groups who have been unable to join these proceedings themselves, we respectfully ask that you make things right. We are asking you, our elected representatives, to stand up for our privacy and continue the work of repealing Bill C-51. Digital security is critical to Canada's infrastructure, economy, and future. Please do not compromise this in the name of fear or following other countries' bad practices to lead us in a race to the bottom. We need to be stronger than that.

Thank you.

● (1105)

The Chair: Thank you.

Mr. McSorley, for the balance of the 10 minutes.

Mr. Timothy McSorley (National Coordinator, International Civil Liberties Monitoring Group): Thank you. I'm very glad to be able to present today on behalf of the International Civil Liberties Monitoring Group and our 45 member organizations. I'd like to thank OpenMedia for inviting us to join them today.

I'd like to touch on three main points: first, review and oversight; second, some of the changes to the Canadian Security Intelligence Service Act; and third, the no-fly list.

Regarding oversight and review, the ICLMG greatly welcomes the creation of the national security and intelligence review agency, as well as the intelligence commissioner. However, we believe there are important ways in which both bodies could be strengthened. We hope the committee and government take this opportunity to ensure that both the NSIRA and the intelligence commissioner have the powers and resources they need to carry out their important work. Others have given feedback, which we largely support, regarding the intelligence commissioner, so I will focus on the NSIRA.

The ICLMG has long supported an overarching review mechanism as a way to ensure Canadians' rights are not violated, and to monitor the effectiveness of Canada's national security activities. Bill C-59 does away with the silos that have restricted the various review agencies' work, which alone is a major improvement.

I would highlight three issues, though, that we think the committee should examine regarding strengthening the NSIRA. First, to ensure independence we suggest that the NSIRA members be appointed via vote in Parliament and not through Governor in Council. Second, the complaints mechanism in the NSIRA act should apply not just to the RCMP, CSIS, the CSE, and security clearances, but be expanded to include, at a minimum, the national security activities of the CBSA as well as Global Affairs Canada, although ideally the complaints mechanism would actually include all federal national security related activities.

Third, SIRC has faced important criticism over the lack of transparency in its complaints system. There is, in fact, an ongoing lawsuit over this issue. We have also raised concerns about SIRC's inability to make binding recommendations. The NSIRA act would transpose these problems onto the new agency. We urge the committee to take this opportunity to improve on the SIRC model and ensure we have a strong, effective, overarching review body.

Next, regarding changes to the Canadian Security Intelligence Service Act, CSIS's threat-reduction powers were introduced with Bill C-51 and were heavily criticized at the time. Bill C-59 attempts to solve some of these issues by restricting the powers to a set list of activities. However, we must reiterate in the strongest possible terms our opposition to granting an intelligence agency, which operates in secret, powers akin to those of law enforcement.

My time does not allow me to go into all our specific concerns, but at the heart of this is that CSIS's creation was meant to separate intelligence activities from law enforcement, and today we continue to have the same concerns we had at that time. Even in cases that require a warrant, we believe that a non-adversarial system will not ensure the protection of a target's civil liberties. We do not believe that this is an issue of “if” the system will violate an individual's rights, but “when”.

We are also concerned about new powers granting CSIS agents immunity for acts or omissions that would otherwise constitute an offence. The Canadian Bar Association, among others, raised serious concerns when these powers were granted to law enforcement officers, calling it antithetical to the rule of law. We believe this even more so when such powers are granted to intelligence agents operating in secret, and we think this section should be removed from Bill C-59.

Finally, regarding the Secure Air Travel Act and the no-fly list, we support the tremendous efforts by the No Fly List Kids and other groups to bring about a redress system. However, we believe the government must go further and address the more fundamental problems with the no-fly list regime. Bill C-59 does not address the due process issues that have been raised since 2007. We cannot condone a system that is used to restrict individuals' travel and to place them on what amounts to a terrorist watch list but does not allow them full access to the information against them, in order to mount a full and adequate defence. We have also yet to be shown that it improves upon Criminal Code provisions already in place that can be used to restrict the activities of an individual suspected of planning a crime. While we appreciate potential solutions put forward by others, such as introducing a special advocate system into the appeals process, we do not believe it is sufficient to restore due process. We maintain our fundamental opposition and call for the repeal of the no-fly list regime.

For more on our positions, we sent a brief to the committee, which I believe was circulated yesterday. I'd also be happy to take any questions, or follow up with any members, following the meeting.

Thank you.

● (1110)

The Chair: Thank you, both of you, for your submissions.

Ms. Damoff, you have seven minutes, please.

Ms. Pam Damoff: Thank you, Chair.

Thank you to the witnesses for coming forward today. It's nice to see you again at the committee.

We've had a fair bit of testimony, and I've asked witnesses about the way CSE is using information gathered from the global information infrastructure, and the fact that right now, while they don't spy on Canadians, Canadians' information can get wrapped up in it, whether they're abroad or whether they've been transmitting through this global information infrastructure. Would you recommend that we amend Bill C-59 to clarify that a ministerial authorization should be required when CSE acquires information from or through this global information infrastructure, when a Canadian is implicated in it?

Ms. Laura Tribe: I would say as a starting point, yes. I think it's critical to have additional authorization required for that type of information collection. I think there are a lot of concerns about in particular about collection by the CSE, how that impacts Canadians, and how their information is collected.

You don't show a passport when you browse the Internet. It's really hard to justify who is or isn't a Canadian. I don't hold that against the intelligence agencies. It's difficult to know that information, but I think a lot of the provisions in the proposed CSE act are being hedged in, “But don't worry, this won't impact Canadians”. That's hard to guarantee.

I think that, even further, beyond just the information collection, a lot of the disruption powers can also impact Canadians. I think that's where having that additional authorization is important. I think using the idea they won't target Canadians is a little bit misleading. Even if they're not targeted, they will inevitably be affected by the way the Internet is set up and the way it works.

Ms. Pam Damoff: Sure. Just as a comment, I think we freely give information over the Internet, without giving thought to where it could end up, far more freely than we would if we were filling out a paper form or speaking to someone, right? We just enter that information, and then it's out there.

Mr. McSorley, what are you thoughts on that?

Mr. Timothy McSorley: We would largely agree with what Ms. Tribe just said. I think, as others have pointed out, there are also questions around the thresholds for those authorizations that we would want to keep in mind. In general, we have the same concerns that there's no distinguishing what information is travelling over the global information infrastructure, and there needs to be greater authorizations and oversight of any collection.

● (1115)

Ms. Pam Damoff: So you would support an amendment to the bill along those lines, then? Okay.

We've also heard from organizations about reporting. I'm just wondering if you think that public and civil society would benefit if the Information Commissioner were mandated to produce an annual public report about the activities of the bodies it oversees. Should CSIS produce an annual public report?

Mr. Timothy McSorley: We believe both would be helpful. We believe, as we submitted in our brief, that other steps need to be taken to ensure transparency and accountability. The fact that the proposed intelligence commissioner currently isn't required to submit an annual report is a large oversight. It should be included, especially because it is currently part of the CSEC commissioner's role. As well, having CSIS produce an annual report would also help the public to clarify.

We saw yesterday that CSIS issued a report on research it was doing. That gives us a chance to debate publicly what kind of research and work CSIS is carrying out.

Ms. Pam Damoff: Okay.

Ms. Laura Tribe: I would just add, one of the things that we've heard from our community is that the reports are really important and that that type of transparency is something critical to earn trust from those commissioners and those in positions of authority overseeing this, but that there's an added need to make sure the reports are telling the whole story. A report for the sake of a report doesn't instill confidence, so make sure that there are set criteria for what's being included in that and that there are checks and balances to make sure it's not just a report for the sake of it.

That's a concern we've heard from our community, and I don't have a specific recommendation for how to ensure that, but I feel it's important to pass along that the report itself won't necessarily gain trust if it doesn't come with ensured transparency around it as well.

Ms. Pam Damoff: We do have the new committee of parliamentarians. For security reasons, you can't put everything into a public report, but hopefully, if there was something in there that flagged an issue, that committee of parliamentarians could delve into it more fully because they do have the ability to do so.

I have two minutes left.

Right now there's no threshold on the retention of personal information with SCISA. I'm wondering if you think we should have two parts to this: an amendment to introduce a necessity threshold for the retention of personal information, as well as a destruction obligation for the personal information that does not meet the necessity threshold. Do you think that would increase transparency and privacy?

Ms. Laura Tribe: Yes, please.

Mr. Timothy McSorley: We also believe that would improve SCISA. In our brief, we give an outline for why we were opposed to SCISA and still have grave concerns about SCISA. We believe there needs to be more done, as the Privacy Commissioner brought up in his testimony, regarding threshold for disclosure and receipt of information.

Fundamentally, as others have pointed out, it's a complex law. Even some of the security officials have said they're worried it could bring in red tape. We believe the goal of the law, of the act, is to ensure that there's a legal framework for private information being shared and used for national security purposes.

We urge that the committee and the government reconsider having an act like SCISA that changes the definition of “threat to national security” and is very complex and, instead, bring in something much simpler that would simply set out the threshold for when information can be shared for national security purposes. That would answer a lot of the questions that have been raised. Changing SCISA to SCIDA, and how it's framed right now won't go far enough.

The Chair: Thank you.

Mr. Paul-Hus.

[*Translation*]

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

I'd like to welcome both of the witnesses.

Ms. Tribe, at one of the committee's last meetings, a leading national security expert said that approximately 200,000 people in China were actively engaged in computer network operations, the technical term for cyber operations. He said that China was a genuine threat to Canada.

Do you, knowing that genuine threats exist, maintain that the Communications Security Establishment should not have any defensive capability?

● (1120)

[*English*]

Ms. Laura Tribe: I believe there are a lot of very real threats to this country, and a lot of them are cyber-threats. I think the concern we are hearing from our community is that this really is a cyber arms race to try to figure out who can build the biggest and most destructive tools the fastest. What we are looking for is to increase our security, to build up our protections, to make sure that we are safe from those types of threats without building the vulnerabilities and the tools that can be actively captured and misused by other governments or other malicious actors who are trying to build those tools themselves.

As much as we would love to believe that if Canada builds these tools we can keep them safe, we have seen that this is not the case. I am sure the NSA felt the same way about a lot of the tools they built. We have seen those misused. We have seen them sit on exploitations that they have used, and vulnerabilities, that then ended up taking down the U.K.'s national health service. These are the kinds of exploitations we're looking to have Canada proactively prevent, to step in to actually increase our security, to build those protections and tools to keep us safe.

While in the short term it might seem easy.... Sorry, I shouldn't say that; I don't think any of this seems easy, because it might seem more simple to try to build the tools to take down the opposition before they get to us. I think in the end it creates additional tools that we don't actually want to be out there. It just perpetuates that environment with those malicious actors on the other side that we're fearing, and perpetuates a culture of fear. I think there are a lot of proactive digital security tools that we can build ourselves to keep us safe. I think CSE already has a lot of abilities, but I believe the active cyber-operations, particularly the ones geared at deploying tools abroad, pose a large security risk for Canada in the way that they could be exploited.

[*Translation*]

Mr. Pierre Paul-Hus: I'm having trouble understanding your reasoning. Fundamentally, Canada does not want to take an aggressive position against any international community, but we have to protect ourselves. According to what you've written and what you've provided to the committee, we are giving CSE too much power, but we have to be prepared to defend our institutions and systems.

You see the rise of certain practices in Canada as a potential gateway to intervention abroad. That's what I'm having trouble wrapping my head around. I appreciate that you don't want a cyber-arms race, but we have no choice. We want to protect ourselves, and we need the tools to do so.

Your group, OpenMedia, posted a video on YouTube. According to the video, Bill C-59 will give Canada's electronic spying agency near-limitless powers in the international realm, in terms of what you were saying, and make it possible to spread false information online for the purpose of influencing foreign elections, as the Russians are said to have done in the 2016 U.S. election.

Is it your position that CSE will proactively influence the democracies or elections of other countries?

[*English*]

Ms. Laura Tribe: I'm not certain what the powers are that CSE would use. I know that based on experts' reading of Bill C-59 and the proposed CSE act, those are the capabilities that are possible within the powers that are being given to CSE. I think that's the concern, that we might not be in a position right now where those are being used, but if we continue to grant those powers, we could be in a place where they are used. That's our concern.

[*Translation*]

Mr. Pierre Paul-Hus: Do you really believe CSE could and would do that? What makes you think Canada would want to interfere in that way?

[*English*]

Ms. Laura Tribe: I think that Canada could and might and would take those actions if the context arose where they felt it were appropriate. These are really complicated political issues and I'm not pretending otherwise. I think that once you have those powers in a very opaque system where it's difficult to build in the transparency mechanisms, it's hard to see how we can trust a system that we consistently see being misused around the world.

Our concern is not that we think that the current government is immediately about to deploy all of these weapons. It's that we're building the powers without any justification to prove that we need them. That's our concern.

[*Translation*]

Mr. Pierre Paul-Hus: I see.

You talk about the influence of the Government of Canada, but you issued a call to action on your website. The message reads as follows: “Not in the U.S.? You can still help save Net Neutrality. This is how.”

In Canada, you don't want to give CSE the power to intervene abroad, but your organization is intervening in the U.S. through a call to action. That's hypocritical; you are encouraging action abroad, and yet you are telling the Canadian government not to acquire certain tools because you fear they could be used for intervention abroad. Don't you think that's a bit hypocritical?

● (1125)

[*English*]

Ms. Laura Tribe: Just to make sure I'm clear, are you asking about our campaigns that we run in the United States?

[*Translation*]

Mr. Pierre Paul-Hus: Yes.

[*English*]

Ms. Laura Tribe: We have a community of supporters of almost 200,000 people within the United States who are active in their own government's activities. It is those supporters—

[*Translation*]

Mr. Pierre Paul-Hus: Your organization is based in Canada but is exerting influence in the U.S., meaning that it has influence abroad. You want the Canadian government to have fewer tools to achieve its objective of protecting Canadians. Don't you think that's contradictory?

[*English*]

Ms. Laura Tribe: I don't believe that OpenMedia has the same power and influence as the Canadian government.

[*Translation*]

Mr. Pierre Paul-Hus: It is nevertheless a position—

[*English*]

Ms. Laura Tribe: Although I appreciate that.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Thank you, Mr. Paul-Hus.

Possibly you'll want to respond after Mr. Dubé's questions.

For seven minutes, Mr. Dubé.

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

I think we've confused citizen activism with state surveillance, but that's a whole other discussion.

I want to ask about this notion in the bill of publicly available information. When the Canadian Bar Association was here, there was a discussion about how there isn't really any kind of jurisprudence or legal definition in Canadian law about what publicly available information is. I think a lot of people have assumed, perhaps wrongly, that this basically means that if I Google something right now, that's publicly available information. What some witnesses brought up was that it could mean information being sold for advertising purposes by social media or search engines like Google, and it could perhaps even go further than that. I know that at OpenMedia you've been very active on some of these "digital clauses", for lack of a better term, in trade agreements and things like that, which, arguably, from this very broad discussion that's happened over publicly available information, could potentially be what that means when companies start being able to freely exchange information across borders in that way.

First of all, I'm just wondering what you think publicly available information means. Secondly, why would that be a cause for concern in the context of what's being presented here, both with the datasets for CSIS but also with the capabilities of CSE?

Ms. Laura Tribe: I think one of our concerns is that it's unclear what publicly available means. We would love to have that addressed through the amendments to Bill C-59, so that it is really clear on exactly what these things do or don't mean so they aren't left to law enforcement to interpret themselves. With publicly available information, unless it explicitly says that people are not allowed to purchase commercially available information, to purchase huge datasets, then, as far as we're concerned, that's still a possibility and a real concern for us.

We would put forward the idea that the ability to Google everything and start recording all of those datasets is problematic. Collecting that mass amount of information, in general, is of concern. Additionally, proactively purchasing and growing those datasets without any direct targets, without any clear suspicion or motivation is really concerning as citizens who are trying to live our lives, who are feeling like we are victims or targets or suspicious actors in our own state. The ability to engage as a citizen is really hard to do without putting a lot of information on the Internet right now. Feeling like anything you put out there is now also being proactively collected and stored by your own government is quite terrifying.

Mr. Timothy McSorley: We would share those concerns. I would also like to highlight that publicly available information is with regard to both CSE and CSIS, as well as the collection of new datasets. Any concern regarding the CSE's collection of publicly available information, we believe, is reflected also in the new powers that will be granted to CSIS. We share OpenMedia's concerns that it needs to be further defined. It needs to follow the same authorization process as other information that will be collected, either through datasets for CSIS or through authorizations for the CSE.

Mr. Matthew Dubé: The natural follow-up to that is what's collected incidentally, which is also brought up in the legislation. The counter-argument could be made that when they do collect incidental information, keeping it requires authorization, but it feels as though the way the thresholds are defined is not sufficient and that it would be relatively easy to justify the collection of incidental information while going after someone else. What are the concerns about incidental information being collected?

I think to some people in the digital world incidental information means something very different from what it would have meant for a more old-fashioned police or national security investigation from 25 or 30 years ago, for example.

● (1130)

Ms. Laura Tribe: I think the concern with incidental information is that the non-incidental, the critical information, in a lot of cases already feels too broad. The ability to keep that incidental information—to first define it, and then also retain it—is quite challenging for us as citizens, for our community to really understand what that means to them. How do they know it's incidental? How do we as regular people understand what information is being collected about us, in addition to how hard it is to keep that incidental information? I think we're hearing a lot of arguments from law enforcement about how incidental information is not actually incidental, which is our first concern, and that, even when it is, it could be useful in the future. I think if you're looking at 25 or 30 years ago, that might be a notepad that's stored somewhere in a filling cabinet. I think right now it's these datasets from which that information is being cross-referenced against multiple other datasets that can potentially provide a lot of either false positives or misleading information, which actually take away from the very purpose of trying to collect this information in the first place.

Mr. Timothy McSorley: Our concern would be that the inclusion of incidental information will in fact lead to what others have described as "mass surveillance" and collection of too much information. Concerns have also been raised about metadata not being properly defined and included. By combining that with incidental information...which often could be very important information. Incidental doesn't mean it's just minor information about somebody, but that something is collected outside of the scope of what the targeted investigation is. In that respect, we don't have a clear idea of what that incidental information would be. If it is to be retained, it would have to meet the same authorizations and thresholds for collection and retention and querying. As Ms. Tribe mentioned, we already have concerns about whether those thresholds are at the appropriate level to ensure adequate oversight and adequate sorting of that information.

Mr. Matthew Dubé: As my time wraps up here I'll try to make this as much of a yes-or-no question as possible, which is always precarious in this line of work.

There has been the notion that things have changed at the border when it comes to cellphones. There is the suitcase rule, or however it's referred to, where you have this expectation of sacrificing some privacy when you cross the border, whereas now, with the increasing ability to look at cellphones, that's different. Do you feel with legislation like this that the same kind of principle applies, that in a traditional investigation there would have been an expectation of people to hand things over, whereas now, given how much information is on cellphones, the expectation has shifted about what people are giving up to investigators?

Ms. Laura Tribe: Yes. We're actively campaigning on both sides of the border to increase privacy at the border for cellphones, because so much information is available on them.

[*Translation*]

The Chair: Mr. Picard, you may go ahead for seven minutes.

[*English*]

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

You mentioned that we have laws and regulations indicating that we don't spy on Canadians. The CSE commissioner came before us and confirmed that there's no spying on Canadians. Even so, you mentioned at the beginning of your speech that there's no guarantee that Canadians will not be spied upon and that we cannot trust the simple fact that it is written somewhere, that we are not sure whether the CSE will or will not spy on Canadians. What does it take then to make sure that we can be assure of that?

Ms. Laura Tribe: I think that one of the things that are important to address is that they cannot be sure and that there will be some spying on Canadians. When that information is identified as being Canadians' data or information being collected, it's immediately treated otherwise, but those protections must also be actively put in to ensure that Canadians are not included. I think that in some cases, some of the provisions that are being put forward in the proposed CSE act will inevitably target Canadians. That's one of the things that we are raising concerns about. I think there are a number of recommendations in the Citizen Lab CIPPIC report that would also help address that. I think the biggest thing is to recognize that it just doesn't work that way. We have to put provisions in place to try to proactively identify Canadian information, and then also make sure that it's treated as such once it's identified and recognize that it might also just be that Canadians are going to be caught up in this, so let's not build systems that we don't want Canadians to be a part of.

● (1135)

Mr. Michel Picard: When you talk to a stranger, do you ask whether the stranger can be under surveillance by another country, so you don't get caught in what may be a monitored call?

Mr. Timothy McSorley: Do I personally ask people?

Mr. Michel Picard: If you talk to a stranger, how do you make sure you will not be caught in a monitored call, because that person might be a target?

Mr. Timothy McSorley: It's true, we don't know if in our communications, they could be targeted or surveilled. That's why we believe we need the strongest possible authorizations and restrictions on how the surveillance tools are used, both in Canada and....

Part of what we do at the ICLMG is argue that Canada also has an obligation to set a standard and to work internationally, to ensure there is a standard for what other countries do as well, on an international level. We know that's difficult to achieve. We're not dreaming that every country is going to be friendly and not spy. Canada states it plays a proactive role in protecting civil liberties and human rights on the international level, and we believe we need to set those policies domestically in order to set an example internationally.

Mr. Michel Picard: The work that both of your organizations are doing, making sure that our private lives are well protected and our rights are well protected, is needed. We salute that.

I had the privilege of leading more than a dozen consultations on Bill C-59 in the first year I was here. People were very loud, on both sides of the fence. There were those who wanted to have a bit of protection, and those who accepted the fact that we need to maybe compromise—if the word works—part of our privacy in order to make sure we are safe.

I'm sure you did a lot of research here and there to make sure you got the most precise and value-added comments supporting both sides of the fence. What is the nature of the comments you received from those who accept reducing their privacy in order to be more secure?

Ms. Laura Tribe: The majority of comments that were received —in fact, almost the entirety of the comments that the OpenMedia community submitted—were not asking for us to compromise our privacy. I think that we say in the consultation results that over 80% of submissions asked to increase our individual privacy, feeling that we've already overstepped those boundaries of individual privacy in the name of protecting national security and that it isn't actually a balance.

I think that's the biggest problem we keep running into, which is acting as though we have to sacrifice all of our personal information in order to be safe. In effect, we haven't seen any evidence that the mass surveillance and mass collection of data has helped prevent any national security incidents. We also haven't seen any evidence that the information will be lacking in future; we haven't seen that it's providing the insights we need.

All we've seen is that Canadians are scared. They're scared of the information their government is collecting about them. They're scared about how it could be misused in future, maybe not by this government, but the government after that, or the one after that.

We've seen a lot of fear after the change in government in the United States about the way the information is being misused, about what happens when that information gets into different hands—and that's only when it stays within the government. If that information gets into the hands of someone outside of government, which we hope never happens, our intelligence agencies will themselves be compromised. We have and will be collecting the information on our own citizens that hand it over to any other government. That's terrifying.

I think what we're hearing from our community is prove to us that you need it, prove to us that it helps.

Mr. Michel Picard: You mentioned—and I'm following the question of Mr. Paul-Hus—that the technology in other countries may increase that threat in Canada, and therefore you are looking for, and I'll quote you, "tools to take down". Therefore, you are open to the possibility of taking measures to make sure that we reduce the aggression or the attack before it happens, and then we have to act after the fact.

What is the justification behind your position to increase those offensive measures, which seems to be the same as the justification not to allow CSIS or CSE to act?

Ms. Laura Tribe: I'm not clear on exactly which contribution of ours you're quoting, but our concern is that we don't have strong enough protections internally to prevent ourselves from cyber-attack, making Canadians and Canada's databases vulnerable. In addition, we do not believe that we should be proactively creating devices, tools, and technologies to go on the cyber offensive, particularly without the checks and balances that we're asking to be put in place.

● (1140)

The Chair: Thank you.

It appears that we've had a massive case of inter-party co-operation break out here.

Mr. Dubé, you have five minutes.

Mr. Matthew Dubé: Thank you.

We don't want to start trends here or rumours of any kind.

I just want to go back to the issue of datasets. Even for parliamentarians there is some confusion as to what that means.

The Privacy Commissioner made an important and interesting point when he mentioned that you always have to consider the future definition of datasets as technology evolves, but also how it's being defined currently. I'm just wondering what you think of the definition and whether or not that's appropriate for now, but also for how things will change in the future.

Mr. Timothy McSorley: Sorry, just to clarify that question, do you mean a specific kind of dataset for CSIS, or just the idea of datasets in general?

Mr. Matthew Dubé: I mean in general and also how it's defined in the bill.

Mr. Timothy McSorley: Right. Our concern is that without allowing for the definition of what datasets are on a yearly basis.... It is concerning. We believe there should be more clarity on what those datasets could and should be.

As well, we're worried, just as others have pointed out, that throughout the process of collecting those datasets has a changing threshold for what can be collected, what can be retained, and then what can be queried. Instead of allowing for so much information to be collected at the beginning and then narrowing it as we go, there should be strong requirements from the very beginning on of what information can go into those datasets.

Of course, as we've already mentioned, the fact that publicly available information could form a kind of dataset is a concern.

There is also concern that, at the very tail end of CSIS datasets, information collected in Canadian datasets can be accessed at a lower threshold for foreign surveillance purposes and that information collected by CSIS for foreign purposes can be collected, albeit at a higher threshold, from those datasets for domestic intelligence purposes. We believe that to fix that problem we need stronger authorization and stronger thresholds from the beginning. As we've mentioned, we also need an increase in the transparency and powers of the intelligence commissioner to verify those datasets and authorizations.

Ms. Laura Tribe: I would just add that the shifting definition of datasets, the different interpretations of datasets, comes back to the bigger question that we keep revisiting: if it's difficult for the government to understand, it's really difficult for citizens to understand what it means. Ultimately, to give this much power to governments to collect this information, and to our law enforcement agencies to gather and use this information, requires a large level of public trust. When the definitions keep changing and when it seems very vague or hard for parliamentary committees to understand and nail down, it's really hard for our community to understand what it means and what's included in it. Any clarity that can be provided on that would be much appreciated.

Mr. Matthew Dubé: Great. Thank you.

I just want to shift gears a bit and go to the position of the intelligence commissioner. It perhaps seems like a nitpicking thing, but it is important, this notion that it's a part-time position. I'm just wondering what your thoughts are on that, and if you think it should be full time, especially considering that, should this bill be adopted, it's essentially the only form of real-time oversight, versus everything else in this country that's based on review after the fact.

Mr. Timothy McSorley: We believe that it should be a full-time position and that, as others have suggested, perhaps a pool could be expanded from being a retired judge to looking at the current judicial pool. Definitely, because of the amount of work that's expected from the intelligence commissioner, we believe that it needs to be a full-time position.

Ms. Laura Tribe: We would agree.

Mr. Matthew Dubé: Thank you very much.

When it comes to information sharing, how concerned should be about what are essentially cosmetic changes in this bill from what was brought in by the former Bill C-51? You mentioned it in your comments, and I don't really have time to get into some of the details I was going to ask about, but perhaps you could reiterate those concerns in the 30 seconds that are probably left.

Ms. Laura Tribe: We definitely have big concerns about the Security of Canada Information Sharing Act that was enabled by Bill C-51 not really being revised or overhauled in the way we had hoped. One of the big changes that we would look for is limiting the information requested to those who request it, and not allowing it to continue being shared between departments after the fact. Another change we would look for is limiting who can access information within other government agencies.

● (1145)

The Chair: Thank you.

Ms. Dabrusin, you have five minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

I want to pick up where you left off on where information sharing is going. In your opening statement, Mr. McSorley, you talked about how you would like to see a simplified version. When I'm looking at this, I'm mindful also of the Air India recommendations, which pointed out that there were very strong problems with the system not sharing information and that that had led to 280 Canadians losing their lives.

Mindful of that as a background, and of some of the concerns you raise as well, what would you see as a simplified version? If you had us doing the rewrite, what would you want to see?

Mr. Timothy McSorley: It's difficult to say precisely legally what it should say, but what I would say is that—

Ms. Julie Dabrusin: Unfortunately, that's where we're at now.

Mr. Timothy McSorley: I realize that, yes. We believe that it should be based on the principles of information, on what's defined under the Privacy Act as information that's private for Canadians; that if it is to be shared for national security purposes that it meet the threshold of necessity; and that, as is laid out already in SCIDA, there's clear record-keeping as to what information is being shared, but that there needs to be a necessity threshold—

Ms. Julie Dabrusin: I just want to stop you there. You said that it is in the SCIDA, though, the record—

Mr. Timothy McSorley: There is record-keeping, and we believe it should be continued because it's obviously important to have records, but it should be at a necessity level.

We're baffled that the expanded definition of a threat to national security is continued with SCIDA. We believe that it should be removed and that we should follow what's in the CSIS Act of the definition of a threat to Canada's national security.

Off the top of my head, I think those would answer a lot of our concerns, but in general what we see right now with the question of the different levels of threshold, that expanded definition of what constitutes a threat that undermines Canada's national security, raises serious concerns for us. I don't believe that rolling that back would undermine what came out of the Air India inquiry, because clearly we need to be sharing the information between government agencies.

Ms. Julie Dabrusin: I'm just looking at the sections, because we are at this point looking at the legal wording in this bill. You're talking about "activity that undermines the security of Canada". One section that has received some comment, I believe from Professor Wark, is this one: "conduct that takes place in Canada and that undermines the security of another state". Is that where your concern is?

Mr. Timothy McSorley: That's one of the concerns. We're also concerned regarding the inclusion of "critical infrastructure" as a threat to Canada's national security. We're also concerned—and the CCLA has raised this—about the changed wording around trying to carve out political expression and activism. Adding to the clause that "unless [it's] carried on in conjunction" with one of those issues actually causes a larger problem than what we see in SCISA—

Ms. Julie Dabrusin: I'm sorry, but I want to stop you there and ask about the critical infrastructure in the minute and 20 seconds that I have left. You're talking about how it's at the request of...there has to be a consent on the critical infrastructure piece in this legislation, for example, with regard to hospitals. I believe we had some evidence that this is in fact one big area to be worried or concerned about. What's your concern about that on the critical infrastructure?

Mr. Timothy McSorley: Our concern isn't regarding CSE's powers to be able to help support and improve critical infrastructure. It's regarding the information sharing that could be triggered by a threat to critical infrastructure in combination.... For example, we see opposition right now to pipelines being built across Canada. In the past, we've seen indigenous action to block a train line or protests that cause disruptions. We're concerned that the way SCISA is currently worded, and how SCIDA eventually will be worded, will continue to pose a threat to legitimate dissent and protestors' actions in Canada by including critical infrastructure as it's currently defined.

● (1150)

Ms. Julie Dabrusin: Thank you.

I think I'm out of time.

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

Mr. Dubé, please, for five minutes.

Mr. Matthew Dubé: I want to go back to the information-sharing issue again, because there was a report in LaPresse a few weeks on an RCMP operation that essentially collects information from the DEA on Canadians, which circumvents the warrant system and all the other legal and accountability measures that would normally be in place for that type of thing.

I'm wondering about it in this context, where departments are exchanging information. If you're working with Five Eyes Allies, let's say, and the RCMP is taking that kind of action, and that information can then be shared between departments, I just want to elaborate—beyond even the legislation—on this notion of this ecosystem, almost, that exists and that I think people are underestimating. It seems on the surface to make sense that Canadian department A should share information with Canadian department B, but insofar as it goes beyond that, I'd like to hear some of your thoughts on that.

Ms. Laura Tribe: One of our concerns, beyond just intergovernmental, inter-Canadian departmental information-sharing, is how that feeds into the Five Eyes network and all the different agencies within it. I think the DEA providing information to the RCMP is a great example of that.

I think one of the big concerns we have is that we don't know, or have any information about, how many information-sharing agreements Canada has. We don't know whom they're with. We don't know what all of them are about. When we give our information to the Canadian government or it's being collected, we don't know where it could end up. Conversely, when we take part in agreements with other countries, we don't know how that information could end up back in Canada.

One of the concerns we have, and one that our community continues to express, is feeling that no matter what the information it is, eventually anyone can get it within the Five Eyes agencies or within any of the related countries' departments. Once it's in one dataset, it's in everyone's. There are a lot of concerns around that when it comes to accurate record-keeping and how that data can be misused. I think Maher Arar is a great example of how that data can be misused to demonstrate some of its more extreme consequences.

It also comes to simple things like no-fly lists. It comes to all kinds of things where simple mistaken identities from a different agency outside the Canadian government can give us a total spiral of how our information is handled domestically, and vice versa. I think that's where outlining who can share what information and with whom, and what those information-sharing agreements are, would go a long way.

Mr. Timothy McSorley: Ms. Tribe has summarized our concerns really well.

I'd just add that one of the recommendations we're making is that, especially for the proposed CSE act and CSIS, proactive roles should be put in place around the disclosure of foreign intelligence-sharing, as well as around SCISA and SCIDA, and that we have clear definitions on what foreign information-sharing is taking place and how it can take place. We should keep in mind, as Ms. Tribe said, that we don't know where that information could eventually end up.

Mr. Matthew Dubé: Something that has come up a few times—and the minister has evoked interest in this, but nothing has really come of it yet. Do you both believe that there should be an oversight and complaints mechanism specifically for CBSA, which is currently the only body dealing with national security that doesn't have that kind of thing in place?

Ms. Laura Tribe: Yes, but I think Tim may have more to say on that.

Mr. Timothy McSorley: We believe there needs to be an independent review body for CBSA. As I mentioned, we believe that CBSA should be added to the complaints mechanism for the NSIRA for its national security activities. That fact that so much of what CBSA does isn't specific to national security, and the fact that it is an evolving and changing definition, means there needs to be a review agency for CBSA on its own.

Mr. Matthew Dubé: There's a sense that everything the CBSA does could be considered national security because it involves the flow at the border. Is there any concern that this definition is not tight enough even for the work that existing bodies such as SIRC currently do when they have to follow the breadcrumbs leading to CBSA?

Mr. Timothy McSorley: I think because national security can be viewed broadly.... In fact, by including CBSA in the complaints mechanism, it would open up NSIRA to be able to dig into what's happening at the CBSA. In this case they will be able to go further.

However, at the same time, we need clarity on what constitutes national security so that on the other side it can't be shrunk in private to say that national security only means situations where somebody gets flagged on a no-fly list, or something like that, and that everything else, for example, refugees and similar issues, aren't considered.

● (1155)

Mr. Matthew Dubé: Thank you.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Dubé.

Mr. Fragiskatos, you have the floor for five minutes.

[*English*]

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you very much, Chair.

Thank you to both of you for being here today.

For the sake of full disclosure, almost 20 years ago, Steve Anderson, the founder of OpenMedia, was my roommate at Western University, so please say hello.

In any case, I want to begin with Ms. Tribe, if I could, and follow up on some of the questioning we've heard with respect to CSE.

This committee has heard a great deal of testimony on the threats to Canada's critical infrastructure: hydroelectric systems, nuclear energy, the banking system, and in particular health information. I take what you say about CSE seriously, although I disagree because I think we have to have an offensive capability that can protect that critical infrastructure.

From your perspective I'd like to understand how you would advise this or any Canadian government to guard itself from the very real threats that exist in the cyber network or cyber sphere? It's not a loaded question; I'm sincere in asking it.

Ms. Laura Tribe: The biggest concerns we have are that there aren't checks and balances in place in the way that the proposed CSE act is currently worded. There's 90 pages' worth of report and recommendations put forward on it specifically by Citizen Lab and CIPPIC, which gets at a lot of the details.

Fundamentally, though, we are concerned that the scope is too broad, that it lets CSE do too much without the accountability and checks and balances needed to make sure it's used only if someone is targeting something like our energy infrastructure.

Mr. Peter Fragiskatos: I want to read a quotation for you. It comes from James Lewis, currently senior vice-president at the Center for Strategic and International Studies, who says that the most effective way to provide sustainable and long-term protection against cyber-attacks is through offensive capabilities and the destruction of opponent networks and systems. If we continue with an orientation that is strictly defensive, in his words, it's “the equivalent of a static defence, defending fixed positions rather than manoeuvring, and conceding initiative to opponents...”.

The nature of national security is changing constantly. Our Five Eyes allies have the ability to carry out an offensive cyber approach. I'm not simply speaking about the United States—middle powers like New Zealand, Australia, and Canada have this ability already. In fact, we've heard at this committee that we are behind those countries.

What would you say to someone like Professor Lewis, who states that if countries like Canada choose not to act, we're always going to be on the defensive and we can't pre-empt attacks on our critical infrastructure. This pre-emptive capacity is important for the safety and security of this country and its citizens.

Ms. Laura Tribe: There are two responses to that. In the first place, that is a very proactive military solution or militaristic-style solution, which is fundamentally not what we're hearing from our community as the approach they're looking at. It might look and feel different because it's being done online, but its the exact same approach—we need to get them before they get us. This is just a difference of opinion, and we might have to agree to disagree.

Mr. Peter Fragiskatos: I think we will, yes.

Ms. Laura Tribe: I think the idea that we need to keep up with everyone else is what has gotten us here in the first place. That's the challenge we're facing. Just because other countries are doing it doesn't mean we have to. I think CSE already has immense powers around hacking and disruption, and we are looking to ensure that there is transparency and oversight in the system.

Mr. Peter Fragiskatos: If your banking data were to suddenly be hacked and disappear, if the vital health information that doctors need to access were to disappear, if our electrical system were to suddenly collapse, what would you say then? If we're simply on the defensive and not acting against threats in an offensive way, I think the security of the country would be compromised. Do you see that point?

Ms. Laura Tribe: Absolutely, I see that point. I think that we are focusing so much on trying to get them before they get us that we're failing to recognize where we're weak, where we're vulnerable. We are also ignoring some of the powers we already have. Of course, I agree that if our health information were to suddenly disappear, that would be a concern.

There are a number of abilities CSE might like—abilities that we might like them to have—that might even be proposed within the CSE act. But this doesn't come with the limitations we need to ensure that it's only being used for things like our health information. I think the scope is too broad. The clarifications are not there to provide the trust that Canadians need. We weren't consulted on it. We were never asked in the consultation what we thought about giving CSE new powers. I think that's where our community's concern comes from.

● (1200)

Mr. Peter Fragiskatos: Final question where does terrorism—?

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Fragiskatos.

I'd like to thank the witnesses for being with us today.

We will now take a quick break, to bring in our next panel of witnesses.

Thank you.

● (1200)

(Pause)

● (1205)

The Vice-Chair (Mr. Pierre Paul-Hus): Good afternoon, Mr. Nesbitt. Can you hear us?

[*English*]

Professor Michael Nesbitt (Professor of Law, University of Calgary, As an Individual): Indeed, I can. Thank you.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Good afternoon gentlemen.

I'd like to welcome Michael Mostyn and David Matas, from B'nai Brith Canada, and joining us by video conference, is Michael Nesbitt, law professor at the University of Calgary.

We will begin with your presentation, Mr. Nesbitt.

[*English*]

Prof. Michael Nesbitt: Thank you so much.

Let me start by thanking you all for this wonderful opportunity and for undertaking the crucial task of reviewing Bill C-59. It is truly indeed an honour and a privilege to be here today and to sit with you.

I have been asked to focus my attention today on part 3 of Bill C-59, the proposed CSE act, and that is what I intend to do. In general, there is no question to me that updating the antiquated authorities governing the CSE and putting the establishment on solid statutory footing is vitally important. As a result, I am strongly in favour of the initiative to craft a CSE act. Indeed, it is obvious to me that the result of this endeavour is a carefully crafted piece of legislation that tries hard to balance the operational needs of CSE to protect Canada's national security interests with Canada's commitment to democracy and the rule of law.

Obviously, given its size and complexity, there will also be much work to do. That simply goes with the territory. In this regard, I have had the distinct benefit of reading the briefs and testimonies of the witnesses that have already presented to this committee. While each guest has offered thoughtful commentary that I encourage you to strongly consider, my overarching sense is that none of us will foresee all the legal or operational challenges to come.

This is the reality of dealing with such a large, important, complex, and highly technical bill. Therefore, more than anything else, it will be vitally important that the current review of the CSE act is thorough and rigorous and that such rigorous review and oversight continues, particularly in the early days and years. This is not an act that should look precisely as it does now, by this summer, or when it is first reviewed, years after coming into force. It will have to be updated to keep pace with technological, operational, and legal developments.

In my mind, the best bet is to focus on robust review and oversight, such that, the issues that do arise in the coming days and years come to the attention of Parliament, to the public, and to the CSE itself, and that there is an opportunity to make the necessary corrections when the time comes.

Neither the law nor Canada's security is well served, if the CSE's legal and/or operational fault lines are kept in the shadows, and it is my sense that the CSE would agree with that sentiment. For this reason, I would start by encouraging you to adopt Professor Kent Roach's recommendation that the review contemplated in part 9 of the act take place sooner, rather than later.

The same goes for the CSE Commissioner's recommendation with regard to the need for the proposed intelligence commissioner to produce an annual report on his or her authorizations, to be tabled in both Houses yearly. Also, there is the need to ensure that any activities that implicate a reasonable expectation of privacy, and thus implicate section 8 of the charter, by necessity, are properly overseen by the intelligence commissioner.

Here, I have three things in mind. First, the CSE Commissioner has recommended that proposed section 37(3) of the CSE act be amended to require the IC approval of ministerial authorizations to extend foreign intelligence operations. Indeed, if the original operation requires IC approval, so too should any follow-up. Arguably, the IC will have more information on which to base a decision at this re-authorization stage. More to the point, it is at this later stage that we will really see whether, and how much, incidental collection of Canadian content is forming a part of the foreign intelligence collection.

This brings me to my second point fairly neatly. I encourage you to focus your legal review of the proposed CSE act on those sections that implicate the collection of incidental information not, as we commonly say, directed at Canadians. In the past, including recently in both the U.S. and Canada, we have seen that lack of oversight over just this sort of incidentally collected information can cause great legal and political controversy that I don't believe anyone is looking for.

In the context of the proposed CSE act, I would then encourage you to adopt Professor Craig Forcese's call to amend subsections 23 (3) dealing with the collection of foreign intelligence, and 23(4) dealing with cybersecurity. CSE is made to seek ministerial authorization, and thus IC oversight, where its activities will contravene an act of Parliament, as it currently states, or involve the acquisition of information in which a Canadian or person in Canada has a reasonable expectation of privacy.

Our charter demands oversight where there is a reasonable expectation of privacy. Therefore, it is very hard to see how, without ministerial authorization and IC oversight, the bulk collection of information that implicates the reasonable expectation of privacy, which under the current wording could be permitted, would hold up in any court of law in Canada.

● (1210)

Third and finally, I believe that you have heard testimony that has expressed concern about the collection of publicly available data, without the oversight of the IC. I'd be happy to provide more detail here during the question period. For now, I will simply say that one can certainly be sympathetic to the carve-out for publicly available data. If the public can access it, surely there is no need for the CSE to get approval to do the same, or so the theory might go.

But not all publicly available information is the same, and bulk publicly accessible information in the hands of the state is a very different thing indeed from that information in the hands of an individual like you or me. For example, unlawfully obtained information, hacked passwords for example, can become public but nevertheless will also be thought of as private information—at least in the eyes of those who hold those passwords. Moreover, discrete pieces of public information may seem harmless on their own, but when harnessed together by the state to produce big data analytics that can also be publicly purchased and then collected as one piece of information, the amalgam of public information can offer very private insights into the lives of individuals. Of course, all of this adds to the thinking, which is already present with respect to some publicly available information, that in the right context public information can itself implicate a reasonable expectation of privacy and thus implicate section 7 of the charter once again.

Put another way, just because it was accessed publicly, does not mean it doesn't implicate the privacy protections of our charter. This will, of course, have ripple effects for how that information can be used and shared. With IC oversight, for example, such private “public” information might be shared with the RCMP for prosecutorial purposes. Without IC oversight, information collected in violation of the charter will not likely be able to be used in support of such prosecutions.

In short, unless CSE's collection of public information is brought under the purview of the IC, there is real reason to fear that we have both a security and a liberty concern here.

Thank you very much for your time.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Nesbitt.

Mr. Mostyn, you have 10 minutes. Please go ahead.

[*English*]

Mr. Michael Mostyn (Chief Executive Officer, National Office, B'nai Brith Canada): Thank you. I will be sharing my time with Mr. Matas.

We thank the committee for inviting us to appear. I will provide some introductory remarks. My colleague David Matas, our senior legal counsel, will elaborate on some of our key points on the proposed legislation.

B'nai Brith Canada is this country's oldest national Jewish organization, founded in 1875, with a long history of defending the human rights of Canadian Jewry and others across the country. We advocate for the interests of the grassroots Jewish community in Canada and for their rights such as freedom of conscience and religion.

B'nai Brith Canada testified before this committee in 2015 and, most recently, in February 2017, on what was then Bill C-51. Our testimony today will develop the same points we had previously expressed, and we will focus on specific areas that touch on our work, particularly part 7.

Our latest audit of anti-Semitic incidents in Canada contains a key truth: Jews are consistently targeted by hate and bias-related crimes in Canada at a rate higher than that of any other identifiable group. Statistics Canada recently released its report on 2016 police-reported hate crimes, and once again Jews were targeted more than any other group in the country. But police-reported hate crimes are only the tip of the iceberg. We require better tools—data and analysis—to gain greater insights into all hate crimes and to do a better job of countering them.

Bill C-59 includes proposals to change the Criminal Code aimed at improving the efficiency and effectiveness of the terrorist entity listing regime. We endorse those proposals providing for a staggered ministerial review of listed entities and granting the minister the authority to amend the names, including aliases, of listed entities.

In the past, B'nai Brith has been supportive of measures to empower security officials to criminalize advocacy and promotion of terrorism, and seize terrorist propaganda. We supported these measures to deny those intent on inspiring, radicalizing, or recruiting Canadians to commit acts of terror and who exploit the legal leeway to be clever but dangerous with their words. Bill C-59 seeks to change the law's articulation of this offence from “advocates or promotes” to “counselling” the commission of a terrorism offence. This is a weakening of the law that we believe is unhelpful. We have noted the assurances provided by the Minister of Public Safety and Emergency Preparedness, but we are still uncertain that such a change, which in our view weakens the law, is needed.

The change of advocacy and promotion to “counselling” also impacts on the definition of “terrorism propaganda”. Bill C-59 would remove the advocacy and promotion of terrorism offences in general from the definition. This is also a weakening of the law.

We accept that the right to freedom of expression is an important consideration, but the right of potential victims to be free from terrorism and the threat of terrorism must be a greater priority.

The importance of a clear articulation of the penalties for advocacy and promotion of terrorism should include the glorification of terrorism, something that should be of concern to all of us.

These are specific points I wanted to raise. There are others that, while not specifically part of the proposed amendments to Bill C-59, are intimately associated and are of interest and concern to B'nai Brith Canada. There are further points here. I'd like to highlight some.

The continuing manifestation of anti-Semitism, hate crimes, and hate speech in Canada affects not only the Jewish community. B'nai Brith Canada sees these worrying trends as national security issues. Organizations such as ours working with law enforcement agencies at the federal, provincial, and municipal levels must address these issues collaboratively.

The government's framework to counter youth radicalization is also extremely important. We endorse the work of the Canada Centre for Community Engagement and Prevention of Violence. We look forward to a stronger dialogue with them.

How can we collaborate in the more effective monitoring of groups engaged in hate speech or incitement directed at children, including those using coded messages that are nonetheless threatening, even where these might fall short of actual crimes? This is very much the focus in countering radicalization at an early stage, where civil society can have better dialogue with law enforcement.

How can we ensure that government agencies shun questionable organizations and groups, particularly those that receive government grants and nonetheless are operating in ways inimical to the fundamental rights and freedoms of Canadian society? We would welcome a channel of dialogue for this purpose.

Lastly, how can we better engage in dialogue with the Canada Revenue Agency to ensure diligent follow-up to complaints regarding organizations engaged in or supporting those expressing hate speech at odds with their charitable status?

There are other points, as I mentioned, in our paper. I'm sure we can answer those in questions.

I'd like to cede the floor to my colleague David Matas.

● (1215)

Mr. David Matas (Senior Legal Counsel, B'nai Brith Canada): Thank you very much, and thanks for allowing us to be here.

I want to restrict my remarks to one particular component of the bill, the proposal to remove from the Criminal Code the offence of advocating or promoting a terrorist offence, and to replace it with the offence of counselling a terrorist offence. We are sympathetic to the expressed government motivation that led to the introduction of this change. Nonetheless, we believe the proposal is problematic.

Public Safety Minister Ralph Goodale expressed concern that there were no prosecutions under the existing law. He introduced the change, so he said, in order to introduce a more familiar offence for which prosecution would be easier. We, too, of course, are concerned by the absence of prosecutions under the existing law. However, it is far from obvious that changing the offences of advocacy and promotion to the offence of counselling will resolve this problem.

For one, we note, as you've already seen in the submission of the International Civil Liberty Monitoring Group, that there is the view that the offence of counselling is superfluous now because that offence already exists in the Criminal Code. If that submission is right, and the offence is already there, then shifting the offence of advocacy and promotion of terrorism to counselling of terrorism will do nothing to solve the problem of inactive prosecution. Saying the same thing twice does nothing to spur prosecutions. If incitement to commit a terrorist offence was not prosecuted under the present counselling law, there's no reason why it would be prosecuted under a repetition of that law.

The alternative, of course, is that the proposed counselling offence does add something new, that it is not just a re-enactment of the already-existing offence. However, if that is the case, then the advantage of familiarity with an existing standard that the minister touted does not exist. If this counselling offence is different from already-existing counselling offences, then the new law will suffer from the same teething problems that the existing advocacy and promotion law have arguably suffered.

The rationale of the minister for the need to enact a familiar offence to make the law work is further undermined by the fact that advocacy and promotion are not new and different offences. The offence of advocacy exists for both genocide and sexual activity with a person under the age of 18. The offence of promotion exists both for genocide and hatred. In my written materials, I go through a number of cases in the Supreme Court of Canada that look at, define, and circumscribe these offences of advocacy and promotion. Therefore, we already have plenty of legal guidance about the meaning of the concepts of advocacy and promotion.

The notion that prosecutors have stayed their hands because they're uncertain about the meaning of the current law or worried about its overbreadth is not supported by an examination of the Criminal Code and the jurisprudence.

The minister has identified a real problem: a failure of prosecutions under the existing law despite the multiplicity of apparent violations. The solution he proposes, we suggest, does not directly address the problem. The solution, we suggest, lies elsewhere. The prosecution of incitement to terrorism within crown investigation and prosecution offices needs to be given a higher priority. There need to be more resources, more expertise, more training. There needs to be more international co-operation, more experience-sharing, more learning from others, including Israel, who have had to grapple with this problem.

We would encourage Canada to sign and ratify the Council of Europe Convention on the Prevention of Terrorism, which incorporates the specific obligation to prohibit public provocation of terrorism. Ratifying the treaty would not only allow for closer collaboration between Canada and other terror-combatting states, it would also make directly relevant to Canada the jurisprudence in other countries and the European Court of Human Rights, which interpret the relevant treaty provisions.

The government could publish advisory guidelines on its understanding of the meaning of the advocacy or promotion of terrorism. The guidelines would not bind prosecutors but could help dispel uncertainty. One suggestion already indicated by my colleague, Michael Mostyn, is that the guidelines should state that glorification of terrorism should be included in advocacy or promotion of terrorism.

We welcome the fact that the government and the committee are giving the combat against incitement to terrorism the attention it deserves. It remains, nonetheless, for us all to choose the best course to follow in combatting this scourge.

Thank you.

● (1220)

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you gentlemen.

We now move into questions and comments. Starting us off is Mr. Fragiskatos for seven minutes.

Mr. Peter Fragiskatos: Thank you.

[*English*]

Thank you very much to all witnesses for being here today.

I want to begin with B'nai Brith if I could.

You mentioned in your comments the recent StatsCan report that has been compiled on hate crimes. We've heard a number of witnesses speak about specifically national security, conceptions of national security, and how they define threats to this country. The conclusion that I've come to is that this is a matter of perspective. Daesh is certainly a clear threat to Canada and other democracies, but it is not the only threat.

From your perspective, Mr. Mostyn, could you speak to the threat of far-right groups who take an anti-Semitic view, and what that means for the Jewish community in Canada? I think that matter of perspective can get us a long way to understanding exactly what is the nature of the threats confronting Canada. I don't think we can pick one or two or even three.

Mr. Michael Mostyn: Thank you very much for the question. I think it's a very important question. It points to how interrelated some of these hatreds are, and that are actually a pathway towards radicalization, and terrorism in certain cases. As you mentioned, there is something of a resurgence within the extreme right, the neo-Nazi movement. A Canadian, Monika Schaefer, is sitting in jail in Germany for the promotion of Holocaust denial. She's a dual citizen and a former candidate for a political party here in Canada.

The one thing that seems to connect the extreme right anti-Semitism and the extreme left anti-Semitism unfortunately seems to be the hatred of Jews. They're very explicit about that hatred. It's interesting, because when you're talking about the pathway an individual might go down, whether it's for a Criminal Code offence of hate speech or further down towards actually engaging in an act of terrorism, promotion and incitement to terror begin with the vilification of a target group. It starts in broad and general terms, and then incessantly dehumanizes that target group until eventually that pathway has gone so that an individual has accepted the ideology and is willing to act out on that ideology. That, we know, is the pathway down to radicalization. That's why B'nai Brith has been speaking out so strongly about hate speech. We don't want it to get to that pathway where individuals—particularly those, like the youth, who are most vulnerable—get those messages, dehumanize certain groups, and then act upon that.

Again, that's why we're focusing on the promotion of terrorism here. This is something we don't want to see in our country. It is a real threat. Unfortunately, in the world today it's a growing threat.

● (1225)

Mr. David Matas: One further comment I would make is that the Jewish community, unfortunately, of course has been the target of terrorist offences from a variety of different groups, but it also historically has been a victim of violation of the right to freedom of expression through religious intolerance. As a result, we have a lived experience of the violation of both of these rights, the loss of which we feel keenly. In our own minds and through our own experience, we've had to grapple with the need to balance these rights off against each other, which leads us to come to the conclusions we do.

Mr. Peter Fragiskatos: Thank you very much to both of you for that.

I want to pick up on something that was mentioned toward the end of your comments. That's the critique of the change in Bill C-51, the speech crime provision, and the change to a counselling offence. It's interesting, because one of the criticisms of Bill C-51 was that under the speech crime provision as written, it was conceivable, for example, for a Canadian journalist to be convicted under that bill for writing in favour of some of the actions taken by anti-apartheid activists against the infrastructure of the racist South African state in the 1980s. That's if Bill C-51 had been in place, obviously, during that time.

With the counselling offence, this is much more common in existing criminal law. It still would allow for individuals who are involved in encouraging terrorism to face legal consequences. I wonder if you could comment from this perspective. I mean, do you see that point about the dangers of Bill C-51 and how that might impact upon freedom of expression?

Mr. David Matas: I would say that any law has to be interpreted purposively and with the limitations imposed by the Charter of Rights and Freedoms. As I said, advocacy and promotion have both been canvassed extensively by all courts, including at the Supreme Court of Canada in a variety of cases. The Keegstra, Mugesera, and Sharpe cases have dealt with these concepts at the Supreme Court of Canada. B'nai Brith intervened in a couple of them. I myself intervened in the Sharpe case through another NGO at the time.

It's possible to think about any law that can be abused or misinterpreted or misapplied, but what we're looking at is what the law is intended to get at. There are some real problems there. One of the examples that the court gave, in one of these cases, is that in one of Shakespeare's plays, there's the statement, “Let's kill all the lawyers”.

Mr. Peter Fragiskatos: Let's not.

Mr. David Matas: I mean, we're both lawyers. Obviously, we don't like that.

Voices: Oh, oh!

Mr. Peter Fragiskatos: I'm not even a lawyer, but I know some of my colleagues are. Julie is.

Mr. David Matas: We concede that it doesn't fall within these laws.

In looking at the law, we shouldn't look at it in such a way that it makes the law look absurd because that can undercut almost any law.

● (1230)

Mr. Peter Fragiskatos: Thank you, Mr. Matas.

I will go to Professor Nesbitt. I know you have been critical of CSIS having disruption powers. You've expressed concern on that front.

Should CSIS have any disruptive powers? Should its officials not have an opportunity to get in the way of potential attacks before they strike Canada and compromise our security? I'm trying to understand where you see an intelligence service such as CSIS fitting in and what powers it ought to have under its mandate to protect Canadian security.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): I have to cut you off there, unfortunately. You're out of time, Mr. Fragiskatos.

Mr. Motz, it is now your turn, and you have 14 minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Mr. Chair.

[*English*]

I will ask my first set of questions to our guests who are here in the committee room with us today.

We heard from the Centre for Israel and Jewish Affairs that the proposed change with respect to the promotion and advocacy of terrorism effectively makes the change to the Criminal Code somewhat redundant. Yet, we need to ensure that those promoting lone wolf attacks are stopped from promoting violence and hate.

Are the changes that are proposed from advocating or promoting terrorism to “counselling” it a fundamental shift from that? You spoke about it earlier, sir. Is there anything more you want to add on that?

Mr. David Matas: Right now I think the government has identified a real problem; there are no prosecutions. I don't think the problem is the wording in the law. In fact, the wording in the law we have now I think is preferable to the wording the government proposes. I think there's a different way of dealing with this problem. I don't see the problem being solved by changing the law to more restrictive wording, because I don't see the problem existing in the wording in the law. In fact, it sends a counterintuitive message that we're stepping back from directly addressing this problem. We have to think of ways of moving forward rather than stepping back.

Mr. Glen Motz: For the sake of time I'm not going to pursue it, but I'm really interested to know what you think those solutions might be, for another day.

Mr. David Matas: I did try to indicate at least some of them in my brief: education, training, signing the convention guidelines, and working with other countries. I would say we are dealing with terrorism—not just incitement, but terrorism generally—as a relatively new phenomenon. As a result, it requires a form of expertise that the police authorities' prosecution and investigation haven't traditionally had. I don't see the development of that experience and the ability to use the law being affected by changing the law. I think it has to lie elsewhere.

Mr. Glen Motz: Okay.

Mr. Michael Mostyn: If I could just add to that, we need to ensure that conceptually there is no narrowing, so that our security agencies can properly deal with the threats of terrorism today and the threats of terrorism that exist tomorrow.

On the Justice Canada website right now, in a description of Bill C-51 discussing the criminalization of the advocacy or promotion of terrorism offences in general, it states that:

> It is directed at prohibiting the active encouragement of the commission of terrorism offences and not mere expressions of opinion about the acceptability of terrorism.

A sentence later states:

> It extended the concept of counselling to cases where no specific terrorism offence is being counselled, but it is evident nonetheless that terrorism offences are being counselled.

I think we need to be careful about narrowing it as if that were handcuffing our security apparatus from dealing with the threats of terrorism into the future.

Mr. Glen Motz: For me to properly understand, you're suggesting that the language in the former Bill C-51 might actually serve national security interests better than the proposed language in Bill C-59. Is that correct?

Mr. Michael Mostyn: That's correct.

Mr. Glen Motz: Mr. Mostyn, in testimony on Canada's national security framework you said:

> ...the Jewish community is particularly vulnerable to hate propaganda throughout the world, and many of the most powerful terrorist organizations in existence today, such as Hamas, Hezbollah, and Daesh, rely upon the promotion of hatred with a particular focus on anti-Semitism to inspire acts of terror.

As we know, we don't have to look very far in time to see a place where this very much is the case, and still is the case, from the attacks on supermarkets in Paris to the endless calls for the death of Jews and the democratic state of Israel by regimes like Iran.

When we think of those real-life examples, does this bill go far enough? Does it do enough to protect Canadians in its minority communities against radical Islam terrorism?

● (1235)

Mr. Michael Mostyn: As Mr. Matas stated earlier, I don't think any law, no matter how it's worded, is going to protect Canadians.

It's how it's interpreted. At the end of the day, it's about the training and education of our law enforcement agencies. It's how they work together and how they work with their international partners. It's understanding the threats. It's understanding the new coded language of those threats, which it doesn't appear that all law enforcement agencies in Canada are familiar with. It changes. Sometimes there are religious nuances, and this needs to be understood because....

For example, many police forces across the country have guns and gangs divisions. They speak in coded languages. They don't speak in ordinary English. We need to understand that language. That is an educational exercise. That's a training exercise. It's not necessarily something that might be covered in legislation, per se.

Mr. Glen Motz: I appreciate your comment that the law itself doesn't necessarily make this, but that it's the application of it that will add to national security. I appreciate those comments.

You spoke earlier, in your follow-up to my colleague's questions, of the link between hate and terrorism. If I understood you, you're suggesting that all terrorism, or terrorism generally, is rooted in hate.

Mr. Michael Mostyn: Terrorism has to come from a place of hate for any individual to go out and perform such heinous, murderous violence. There has to be seething hatred inside of them, and that's a pathway.

Sometimes it can happen very quickly. Sometimes it can get extended out. However, there are going to be various moments in time—trigger points, and influencers of individuals. Individuals who are more vulnerable tend to be targeted by this radicalization, but at the end of the day, yes, it's based in hatred. It's based in dehumanization of identifiable groups, absolutely.

Mr. Glen Motz: This is for both of you, and for you, Professor Nesbitt, as well.

I'd like your view on the following. In part 5 of this bill, in subclause 115(4), it says:

> ...[any form of] advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada...

Now, is there a risk that including this language may potentially present loopholes that the authors of the bill may not have considered at the time and that may, indeed, present a risk to the security of Canada and Canadians?

Mr. David Matas: That provision's already in the law, if I remember correctly.

Are you asking if it should continue to be there?

Mr. Glen Motz: Yes. It's in a different form in Bill C-59 than it was in C-51, if I am correct.

Mr. David Matas: Yes. Right now, that's a theoretical concern. If we had an actual prosecution that was stopped by that language and we felt shouldn't have been stopped, then we would say yes. But right now, we're at a state where.... Or if the government said that it felt that this language was what was inhibiting it, then we would say yes also.

However, that's not what the government is saying. It's saying that it's concerned about the punitive sections, not the defence sections.

I should say that this is a problem that we have seen with the police and the administration of justice with regard to hate offences. Now police have a lot of hate crime units. We've seen it with sexual assault offences, and now police are becoming more sensitized to this.

I really think that what we need to do is make this work. If it's not working with the language that we have, then we can change it. However, to try to change the language before we even start making it work, in my view, sends the wrong signal.

Mr. Glen Motz: Mr. Nesbitt.

Prof. Michael Nesbitt: I'd have to look at the precise language and compare it to the Supreme Court, but my sense is that it is just implementing Supreme Court requirements with respect to this sort of crime in particular, namely hate speech. This is making it charter compliant, and it's not doing a whole lot more than that. In fact, without this, I think there were concerns that we would not have charter compliant law.

● (1240)

Mr. Glen Motz: Thank you.

Professor Nesbitt, in your testimony on the national security review, you suggested that there needed to be better coordination of agencies and organizations.

Is this achieved here in Bill C-59? Do you see the new NSIRA as an ideal group to conduct this centralized information collection and analysis and then to put it together in a bigger picture?

Prof. Michael Nesbitt: Yes, I'm quite supportive of both the new review bodies and the intelligence commissioner oversight. As I said during my testimony as well, I think this is not just my speaking as a lawyer about the promotion of liberties and rights and laws in Canada, by my speaking as someone who has worked in government and seen the benefit of having outside review to the efficacy of internal operations.

My biggest concern will not be legal but will be with respect to resourcing. If the resources are there—to get into the weeds—specifically to consider the operations of those agencies when certain matters are considered, then I think this could be very beneficial. Again, that will probably come down to—at least as far as I can tell so far—resourcing.

Mr. Glen Motz: To follow up, in 2015, in an article you authored for the *National Post*, you wrote that "Canada cannot claim to have taken the threat of ISIL funding seriously in the way the U.S. has. Canada's sanctions, legislation and enforcement are outdated, under-funded and limited in scope."

Does Bill C-59 address this issue of terrorist group funding in a meaningful way?

Prof. Michael Nesbitt: No, actually that's one of the concerns I continue to have with respect to our national security laws. That is, when we prosecuted terrorist group funding, there's been only one example under our Special Economic Measures Act, or our sanctions, and one or two examples under our Criminal Code. So we have very few examples of Canada taking this particularly seriously, and that's despite the fact that we have ample evidence from foreign organizations, including the CIA for example, saying that Canada is at risk of being a home to terrorist financing and other sanctions-busting activities.

One of the things at some point we'll have to look at is more than just the Magnitsky act as it went through, but the Special Economic Measures Act, in particular, and how we're dealing with terrorist funding through, frankly, Foreign Affairs, under our suppression of terrorist regulations, which are crimes under their purview, and our economic sanctions against Russia, North Korea, Syria, Iraq, and others.

Mr. Glen Motz: Would you suggest, then, that there might be an opportunity to strengthen Bill C-59 by adding some provisions that have to do with this specifically?

Prof. Michael Nesbitt: I don't know whether.... I wouldn't want to tell you folks how to do your job—

Mr. Glen Motz: But that's why you're here. Sir, you're here to give us advice based on your experience on how to properly, in your opinion, address this issue of national security and public safety. We have a unique opportunity with this bill being before committee before second reading—

Prof. Michael Nesbitt: Sure.

Mr. Glen Motz: —so it's quite by purpose to ask experts to tell us what we're missing.

Prof. Michael Nesbitt: I'll tell you my only concern with that. It's not at all with the question you're asking, which is do we need to do something more? Absolutely. Does it need to be legislated? Absolutely. Do we need significant oversight by the NSIRA over Foreign Affairs operations and CBSA operations here? Absolutely. Whether that should be in what is already a very long omnibus bill, that's where I'm more tentative, on whether you want to add language to this bill or a different bill. In general, I would be very supportive of seeing increased oversight of and attention to this issue.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Motz.

Ms. Damoff, it is now over to you for seven minutes.

Ms. Pam Damoff: Thank you, Mr. Chair.

[*English*]

Thank you to all three of our witnesses for being here today. I believe you were here when we were studying the national security framework the last time. I seem to recall being on a panel with both of you when we were looking at that, so I appreciate your coming back.

It always concerns me when our discussions on terrorist attacks focus solely on ISIS and not on the attacks on our Muslim community and by right-wing groups. That has come up. I think I mentioned the last time you were here that when there is an attack on the Muslim community, I am always struck by the fact that the first people to step up are from the Jewish community. I think it's because of that long history of hatred towards the Jewish community that you recognize the impact. Certainly in my own community, I know there's Halton Interfaith Council and tremendous co-operation, and that it is the Jewish community that is always the first to step up when there is an attack on the Muslim community.

I just want to thank you for that and make sure that our conversation is on the broader terrorism threat, not just on ISIL.

We had the Minister here—and this is directed to B'nai Brith, because you were talking about advocacy versus counselling—and law enforcement here, and I believe there were other witnesses as well, although I don't recall for sure. They agreed with what the minister said about the ability to prosecute, that advocacy did not give them the tools they needed and that counselling actually would give them the tools to go out to get those prosecutions.

I'm wondering if you saw that testimony and if you would agree with what they were saying. I will put that to both of you, just quickly.

● (1245)

Mr. David Matas: No, I do not agree, because, as I pointed out previously, the offence of counselling for a terrorist activity is already there in the Criminal Code. It's a different section. It's not section 83.221. I think it's subparagraph 83.01(1)(b)(ii), but it's there, and if all they needed was the offence of counselling to go ahead, they could have used that provision. They didn't have to get a change in the law.

The fact that they didn't do it, even though it's already there, doesn't give me much confidence, as I said, that just saying it twice, in two different parts of the Criminal Code, is going to do much. I think the problem lies elsewhere. It's basically that they're just not used to dealing with terrorism. It's not traditional expertise within the police force. They really have to develop a specialized expertise that can address it.

Ms. Pam Damoff: Thank you.

Professor Nesbitt, do you have anything to add to that?

Prof. Michael Nesbitt: No. Just in general I would say that for a very long time, in section 22 of the Criminal Code, we have had a counselling offence, which is to say it's an offence to counsel another offence within the Criminal Code, and, in fact, we've had at least two terrorist prosecutions that I can think of that have actually included counselling offences, though not counselling in the sense we are thinking of here, but counselling the participation in a terrorist group or counselling the facilitation of a terrorist activity.

As far as I can tell, this is redundant to section 22 of the Criminal Code.

Ms. Pam Damoff: In terms of potential amendments to the bill, during testimony on the national security framework, we heard about the difficulties that law and enforcement agencies have when crucial information isn't shared in a timely and efficient manner.

Do you think the creation of the new national security and intelligence review agency will help to ensure that we're effectively sharing that information with other departments and countries in order to address terrorist threats more quickly and efficiently? Do you have any additional suggestions on how we might improve the efficiency between our intelligence and law enforcement agencies?

Maybe, Professor Nesbitt, you can start this time and then we'll turn it over.

Prof. Michael Nesbitt: Sure. You're asking about the new review agency and whether that will—

Ms. Pam Damoff: Right. Will that assist with the information sharing? We have heard that the information isn't shared between agencies in a timely manner and so it ties their hands in terms of not getting the information quickly enough.

Do you think this will assist with that? Also do you have any additional suggestions to help with that process?

Prof. Michael Nesbitt: Sure. Let me start by saying that, at least in my experience—and this is now drawing a little bit more on my experience than on my studies—one of the big problems with information sharing in government was always cultural. Certainly there was a need to open up more information sharing. The avenues of information sharing can sometimes be overly bureaucratic, but often it was cultural.

This harkens back to the previous answer I gave, which is that one of the benefits of this review agency is that it can look at the totality of the approach within government to something like sanctions. Those sanctions are done at Foreign Affairs, but CBSA is obviously involved if we're talking about goods going out of or coming into Canada. FINTRAC could be involved. CSIS could be involved, etc.

How would a review agency help with the sharing of information? Well, if they're looking across departments at those various organizations in a way that the organizations themselves are not as they've remained siloed, it will force those organizations to then do the same. It can bring together some of those activities.

I'm actually very supportive and very encouraged by that opportunity. I hope it is taken up in practice.

● (1250)

Ms. Pam Damoff: I have less than a minute left. Do you gentlemen have anything to add to that, or is that good?

Thank you.

Actually I have only 30 seconds left. I don't think there is time to ask and answer, so I'll end there.

Thank you.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Ms. Damoff.

Mr. Motz, you have five minutes. Go ahead.

[*English*]

Mr. Glen Motz: Thank you, Mr. Chair.

Thank you again for being here.

I want to take off just a little bit from what my colleague Ms. Damoff was talking about. You mentioned in your previous testimony, Mr. Nesbitt, I believe it was, that the culture of security agencies to protect information is a barrier to centralizing information and that ensuring that the right information gets to the right people in a timely manner is problematic.

Would you say that Bill C-59 is well placed to deal with this issue; that is, this mandatory reporting agency that compels information rather than sitting back and waiting? Are we dealing with this right with respect to Bill C-59 being the mechanism and the way it's going to play out?

Prof. Michael Nesbitt: It's a good question, frankly.

I would start by saying that I do have some concerns about the changes, or lack thereof, to the part of the act that deals with information sharing itself, which is—and I won't get into the details, as you've heard this from others—that the definition of "threat to security of Canada" is not the definition that exists in the CSIS act but a new and very broad definition. So, to answer your question, I don't think that is the right approach.

More broadly, I think the benefit to what is happening now is that we're looking at information sharing more holistically. We're not just talking about opening up the avenues to information sharing within government. We're also looking at how it can be encouraged culturally, and how review across agencies can break down the silos of review, and then, hopefully, break down these silos of information sharing. It can force people, if the job is done correctly, to get in the same room, which is often a problem within any large organizations, really.

I'd have to think more closely about whether there is anything else we could do. I hadn't, frankly, prepared for that. I'd be happy to get back to you on that if that's of interest.

Mr. Glen Motz: Yes.

Prof. Michael Nesbitt: But I think, for now, this is a very good start. I'm heartened to see a lot of the details in the bill.

Mr. Glen Motz: If you have more suggestions, I would think the committee would be open to receiving those. That would be great. Thank you.

To the guests who are here, the committee has heard that terrorist groups will continue to operate and coordinate and recruit online. We do also know that there is a rise in online hate. You had said previously that terrorism is rooted in hatred. Does this bill go far enough to deal with the online hate, and to limit that in some...?

Mr. Nesbitt, please feel free to join us in your comments.

Mr. David Matas: I am not aware of anything in terms of the bill that deals specifically with the Internet in relation to advocacy, promotion, and counselling. I know there used to be something in the Canadian Human Rights Act at section 13.1 that dealt specifically with the Internet, which was repealed. We realized it was problematic. What we were proposing was a repeal and re-enactment with the problems removed, but it just disappeared.

I think that the Internet is pervasive enough, problematic enough, and presents its own very specific problems, that it would be worthwhile developing some specific legislation that deals with it.

One facet of the Internet is that it's a commercial network of contracts that often have good standards, but which aren't being enforced. There is a question of the extent to which mechanisms should be developed for enforcing those standards. It may be too much to do all of that in the context of amendments of this bill, but I really think it's something this committee and this government should be looking at very specifically.

● (1255)

Mr. Glen Motz: Professor Nesbitt.

Prof. Michael Nesbitt: To my mind, the biggest barrier to enforcement and prosecution of the terrorist activity that speak of, or any terrorist act, is the so-called problem with intelligence to evidence. I understand that the bureaucracy, or the government, may be thinking about dealing with that in the future. I would say that if this is what we are concerned about, then in the near future we will have to tackle this intelligence to evidence problem—which involves the collection of information by security agencies—and how it can be properly, legally, and safely shared with the RCMP for the purpose of actually enforcing the laws that we do have on the books, which are fairly comprehensive.

Mr. Glen Motz: Thanks very much to you both.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Motz.

Mr. Spengemann, you may go ahead for five minutes.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you, Mr. Chair.

My questions are for Mr. Mostyn and Mr. Matas.

[*English*]

Mr. Mostyn, can you give us an overview of the strategic threats assessment that this bill is situated in? It's called a national security act, it's broad, and it's supposed to encompass any threats that come our way.

The committee heard a lot about cyber-threats, it heard a lot about terrorism and radicalization and violence. Is that the entire basket? Are there others, and how would you rank the two in relative proportion to each other, vis-à-vis your own concerns?

Mr. Michael Mostyn: Obviously those are very strong threats. There are other threats. Radicalization just doesn't take place online. It does take place via individuals, even here in Canada. That's why with the lack of prosecutions there is also a lack of cases going up the way from police forces. The real question is, how do we deal with that? B'nai Brith itself has exposed situations and rallies publicly where there has been vile hate speech spoken in the streets, often with children, sometimes children who are kept home by their parents to listen to this and who are chanting slogans themselves. There are institutions that have charitable status in this country that are posting on their own YouTube channels hatred targeting an identifiable group, Zionists. B'nai Brith exposed the MAC, which has charitable status, in Vancouver. They had an imam up there. It was on their YouTube channel. We complained to the CRA. They were calling Israelis an impure gang and Zionists the worst of mankind. There is a lot of evidence out there of incidents happening here in Canada. I think that not just the Jewish community but all identifiable groups in this country want to see the law upheld and justice be done and the protection of our society when there are real incidents of groups being targeted for hate.

Mr. Sven Spengemann: This will be a complex question and answer, but to what extent are these concerns linked to international terrorist organizations like ISIS, like Al Shabaab, like Abu Sayyaf, who are preying primarily, almost exclusively, on young people downside of the age of 30? Are the domestic threats generated in Canada or are they strongly linked to what's going on outside our borders?

Mr. David Matas: Obviously there are both. I think we have to look at the intermediaries because a lot of this communication is obviously done through the Internet, so the question is, what is the responsibility of the means of communication? If it were in a newspaper, it would be easy because we have laws developed about that, but when it comes to the Internet intermediaries, they are mostly considered not responsible and you have to go to the source, which gets you...were is the source?

All of these Internet companies that communicate this have a presence in Canada. I think one of the things when you're dealing with this problem is looking more closely at the responsibility of the intermediaries in dealing with this issue.

Mr. Sven Spengemann: Thank you very much.

The time is very limited. I want to ask you about the relative importance of the counterterrorism, counter-violence work, and your expectations of the Canada Centre for Community Engagement and Prevention of Violence in juxtaposition with the law enforcement, criminalization, and prosecution framework that we're building, which is also very important. How does the former compare to the latter?

Mr. Michael Mostyn: B'nai Brith is very supportive of that initiative, and we look forward to working more closely with them. I think they should engage with many civil society groups. You're right that it's the other side of the coin when you're talking about prevention. That has to be taken care of in addition to, obviously—

● (1300)

Mr. Sven Spengemann: Do you have some precise expectations or ideas, or a framework for that centre?

Mr. Michael Mostyn: We're in dialogue with them. I would be happy to provide some further information to you about that.

Mr. Sven Spengemann: That would be helpful to the committee.

I think that's it, Mr. Chair.

[*Translation*]

The Vice-Chair (Mr. Pierre Paul-Hus): Thank you, Mr. Spengemann.

Mr. Nesbitt, from Calgary, and Mr. Mostyn and Mr. Matas, thank you for your input today.

The meeting is adjourned.