HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 094 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 1, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, February 1, 2018

● (1100)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Good morning. Let's get started.

We have, as one of our first witnesses, for the Canadian Association of Chiefs of Police, Laurence Rankin.

You're out in Vancouver, so I hope we haven't gotten you up too early in order to be able to give testimony.

We also have Paul Martin, chief of the Durham Regional Police Service.

I understand you're going to split the time between the two of you. The floor is yours.

Chief Paul Martin (Chief, Durham Regional Police Service, Canadian Association of Chiefs of Police): First of all, on behalf of the CACP, I just want to thank you for the opportunity to be here today to speak to the committee. Laurence and I have been looking forward to this.

Laurence is going to start out by basically talking a bit about the CACP counter terrorism and national security committee's mandate. Then we'll talk about a few things just to set the context from the CACP standpoint. We'll be open to any questions after that.

I'm going to turn it over to Laurence, and he can start off.

Deputy Chief Laurence Rankin (Deputy Chief Constable, Investigation Division, Vancouver Police Department, Canadian Association of Chiefs of Police): [*Technical difficulty—Editor*] Canadian Association of Chiefs of Police, CACP, is to lead numerous efforts to promote coordination and collaboration amongst Canada's law enforcement community to address threats to national security. As part of these efforts, the CACP has implemented structures to help manage incidents and share information in support of a mutual goal to protect the safety of Canadians.

The counter terrorism and national security committee, which is part of the CACP, has a mandate to harmonize the work of Canadian police agencies throughout the country in identifying, preventing, deterring, and responding to criminal activities related to terrorism and national security threats.

This committee has five priorities or objectives: one, to “promote collaboration and integration among law enforcement agencies and with appropriate public/private security and intelligence partners”; two, to “improve ability to operate in a cooperative and integrated manner” with a view to addressing emerging trends with respect to counterterrorism and national security; three, to “develop processes and facilitate strong communication at all levels”, so at the municipal, provincial, and territorial levels; four, to “recommend legislative reforms”; and five, to “promote education and training in matters of counter-terrorism and national security”.

There have been a number of initiatives that the committee has worked on over the past year. I'm going to focus on three for today's presentation.

The first initiative is the provincial and territorial counterterrorism guide. This guide is designed to support the efforts in developing counterterrorism strategies at the regional, provincial, and territorial level.

There are 11 key activities within the guide that are focused on four key strategies. The first is to prevent individuals from engaging in terrorism. The second is to detect the activities of individuals and organizations that may pose a terrorist threat. The third is to deny terrorists the means and opportunities to carry out their activities. The fourth is to respond proportionately, rapidly, and in an organized manner to terrorist activities and to mitigate their effects.

The second initiative is the provincial and territorial integrated response structures. The co-chairs of the counter terrorism and national security committee have met with provincial and territorial chiefs of police across the country in an effort to encourage and develop an integrated provincial and territorial approach for each province and territory to investigate and respond to terrorist activities.

The third initiative is the subcommittee of the counter terrorism and national security committee, the countering violent extremism sub-committee, developed in August 2015. The subcommittee is focusing on building training material that's consistent, that addresses previously identified research gaps, and that has a built-in evaluation tool to determine the efficacy of the programs that we are rolling out.

Those are the three key initiatives.

Chief Paul Martin: Thank you, Mr. Chair. I'll continue.

Building on what Laurence spoke about in terms of harmonizing and working together as police agencies, from the federal agencies to the municipal agencies and the provincial in between, there are three major concerns for the committee to consider from the policing standpoint. There are perhaps many, but certainly three for your consideration: the terrorism peace bonds, the intelligence-to-evidence conundrum, and then encryption. I'll speak to them separately.

The terrorism peace bonds manage some of the threat posed to Canadian citizens but not all. They do help manage in some cases, but something to consider is that with the terrorism peace bonds there are conditions imposed. I can provide an example of an individual subject to the peace bond who is not permitted to use computers, or not allowed to access the Internet for a number of different reasons that I'm sure are obvious. There is no mechanism in place right now for police officers of jurisdiction to go in and ensure that the person is complying with those conditions, so that's something for consideration.

With respect to the intelligence-to-evidence conundrum, we know how the intelligence lives in one space and the enforcement piece lives in another space. It's my understanding, after talking to my colleagues, some more learned than I, who have been involved in this field for some time, that this discussion has been ongoing for more than 15 years in terms of how we can improve the speed, flow, and direction of this information so that we can share it in a quicker fashion. Incidents such as the Aaron Driver one made it very obvious to the policing field how fast information moves, and how fast it has to move in order to detect, deter, and ultimately deal with a threat nationally.

Something to consider is how that's going to happen. The 9/11 Commission was very clear on the fact that information needs to be shared amongst the different agencies. Police agencies right now do share a lot of information, but that's something for this committee to consider as this bill proceeds.

With respect to encryption, we've heard a lot south of the border as far as going dark is concerned. We've heard all these different terms, but encryption, whether it be in the hardware itself or with the use of applications that are encrypted end to end, poses a very difficult issue for policing and how to monitor people who would carry on criminal activity, whether it's for terrorism or for organized crime. We've seen a number of examples in our jurisdiction and throughout Ontario, and certainly across this country.

The important thing is that we must be focused on the principles and not the technology, and where an individual or group is using any form of communications to support terrorism or other designated criminal activity, this may be intercepted by specified authorities with the proper and appropriate judicial authority.

Laws regulating access to communication data would be, in principle, the same as those currently in place for other forms of telecommunication intercepts, companies ensuring data is available to access if required, warrants being issued by the appropriate authority, and then both time limits and regular scrutiny and review.

I throw that out to the committee to consider as we go forward and you talk about this bill. These are really the top three concerns that seem to spread generally across the policing community: the terrorism peace bond and the future of that, the intel-to-evidence conundrum, and encryption.

Thank you very much for your time.

● (1105)

The Chair: Thank you, Chief Martin and Deputy Chief Rankin.

Our first questioner is Mr. Spengemann. You have seven minutes, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Chief Martin and Deputy Chief Constable Rankin, thank you for being here. Thank you for your service and offering your expertise to the committee.

To begin, could you outline for the committee your sense of the current threat environment with respect to national safety and security? Your work is focused on terrorism and counterterrorism. Where does that rank with respect to other threats that the country is facing, including potentially cyber threats against our critical infrastructure?

Chief Paul Martin: It's always a consideration for us. Probably the biggest concern right now, as we discuss it at the committee level, is really the returning foreign fighters and the collapse of the caliphate overseas. That poses a problem. Certainly we can look to our European counterparts and others in the Five Eyes community to say what has happened there, what we can expect here.

It is always top of mind with us, but there are a number of different ways terrorism can occur. You've talked about the cyber-attacks. We have the physical attacks, what we've seen overseas, and even here for that matter, including in Edmonton, where people have been radicalized to violence, so it is always a concern for us.

D/Chief Laurence Rankin: Could I just add something? Recognizing that national security investigations are a federal responsibility, we as a municipal agency often are far more likely to engage or encounter the issue at the first point of contact. What we are finding is that the issues we're dealing with that could have a nexus to counterterrorism or national security are often incorporating the subjects we're looking at, cyber-enabled components of that crime. Just to add, these are issues that dovetail with encryption and that also have connections to radicalization that we are trying to mitigate at a municipal level but working in collaboration with the RCMP and in particular the integrated national security enforcement teams, INSETs, that we have members seconded to.

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

If it's fair to say that terrorism and extremism remain a prominent threat, is it also fair to say—you spoke about the imploding caliphate and returning fighters—that recruitment, either by right-wing extremist groups or by international terrorist groups like al Shabaab and the remainders of ISIS, remain a threat; in other words, fresh recruitment of Canadian youth who are particularly vulnerable to radicalization, to recruitment, and to becoming incorporated in these organizations?

● (1110)

Chief Paul Martin: I would agree with that statement. The fact is that individuals who are interested and motivated to recruit people and incite people to violence and to take action are using the cyber-world, and they have used it quite effectively. That is probably, next to the returning foreign fighters, one of the biggest concerns that we have as a committee. We do try to address that issue as well.

D/Chief Laurence Rankin: With the assistance of the federal government, at a municipal and provincial level, countering radicalization to violence is a key priority for the Ministry of Public Safety and Solicitor General's office in British Columbia, by way of example. We're creating a hub approach to this issue because we've determined that we have to address it before it goes from young people becoming radicalized to their actually acting upon those beliefs. The hub approach is a venue for various community service providers to work together, really with the aim to redirect individuals who may be on the path to radicalization.

Mr. Sven Spengemann: Thank you very much. That's extremely helpful.

I wanted to ask you a follow-on question. You've in a way pre-empted what I was going to ask about. From your experience as serving police officers, in addition to serving on the Canadian Association of Chiefs of Police, what are central levers at our disposal to mitigate the risk of being radicalized? I say radicalized with respect to the propensity to be subject to a right-wing extremist group, as we saw with the individual who committed the massacre in Sainte-Foy just over a year ago. There's no evidence that he belonged to a group, but there is certainly self-radicalization, one could say, and also Islamic terrorist groups. What do we know so far that would facilitate the work of preventing young Canadians from ever falling into this trap?

Chief Paul Martin: We've taken a multi-faceted approach within our police service. It's about educating our police officers on recognizing the signs of radicalization. Probably the more effective means is community engagement, making sure that our police services, especially the municipal and those closer to the ground.... I know the federal agency, as Laurence has pointed out, ultimately has authority for national security investigations, but it's the police of jurisdiction that's going to see this. Our activities are about engaging the communities for a number of different reasons, not the least of which is to make sure they trust us and feel there is legitimacy with the police services so that they can confide in us if they see that members of their community are being radicalized to violence.

The other piece is putting out education to these young individuals who may be getting a message from one side to say that there is some glory or something that's good for them to go to this act of violence, to say that in fact, it's quite the opposite.

Mr. Sven Spengemann: If I can follow up, I only have a minute left with a more specific question along the same lines.

Is there a pattern, a profile—not to say a stereotype, but a propensity—that's identified so far that raises the risk of being radicalized or being recruited, in terms of socio-economic status; in terms of racial, religious, or cultural background; in terms of networks that one does or doesn't belong to? Is there anything yet that we can use as a sort of marker for the way forward?

Chief Paul Martin: Laurence can step in and correct anything I may say on this, but we've had this discussion at the committee level, and there's no specific profile of what a person who gets radicalized looks like.

Generally speaking, there are things where they are vulnerable, they perhaps feel disaffected, they don't trust people, and they're on their own—they're loners. That's probably the closest thing you're going to get to a profile, but as far as a specific socio-economic status or age, no.

● (1115)

The Chair: Unfortunately we're going to have to leave it there, Mr. Spengemann.

Mr. Motz, you have seven minutes, please.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chief Martin and Deputy Rankin, for being here today.

I want to go back to the comment one of you made earlier with regard to peace bonds. We know that Bill C-59 increases the threshold from “is likely” to “is necessary” to prevent a terrorist activity in order to even obtain a peace bond in the first place.

Determining that a peace bond with certain conditions is necessary to prevent an act of terrorism is a pretty high bar. The amount of evidence that would go into proving that is nearly the same as to prove a criminal charge, to lay an information.

Can you explain to the committee the importance of peace bonds, and if you've used them, how often you've used them? In your opinion, could this new, increased threshold be a risk to Canadians?

Chief Paul Martin: With respect, the RCMP has used peace bonds a total of 14 times that they have records of, five of which were the 810.011, which was the peace bond introduced as part of the Anti-terrorism Act of 2015. Currently there are none in effect, but those are the statistics.

There's always a concern if the threshold is made higher. As I said, peace bonds are not the panacea. They're not necessarily going to stop it, but they can help control and mitigate it. It's not going to stop all threats, but yes, there's obviously a concern any time the threshold is made higher. We feel that we currently have a number of tools that help us to detect, deter, and respond to terrorism in this country.

Mr. Glen Motz: Deputy, do you have anything further to add?

D/Chief Laurence Rankin: The benefit of them once they are imposed is the ability, among other things, to conduct full-time surveillance on the subject if there's GPS tracking involved, interview the subject, and monitor the individual. It's effective in managing some of the threats posed by an individual, but there are limitations, as the chief mentioned in his opening statement, in terms of enforcing conditions such as access to the Internet when they're using that computer device in their own residence.

Mr. Glen Motz: We have the peace bonds, but the other aspect now of Bill C-59 is the preventative arrests. We understand the language in the new legislation limits it to an arrest that "is necessary" to prevent a terrorist activity. Under the old Bill C-51, the threshold was "is likely to prevent", which was the language that was used. In fact, the committee heard from the justice department earlier in this study, and they confirmed that the threshold to make a preventative arrest was being raised. They said that, "It would require the police to present evidence of a greater link between the conditions to be imposed on the person or the arrest of the person and the prevention of terrorist activity."

Again, similar to peace bonds, do you believe that this higher threshold will make it more difficult for law enforcement to make preventative terrorism-related arrests?

Chief Paul Martin: My simple answer is that it could. The idea behind the preventative arrests and the recognizance is really to give the police time to determine whether the evidence is there, to see if in fact they are planning a terrorist act. Of course they also allow the judges to assess the evidence to determine if something is there. Every time you raise a threshold, there is a potential.

D/Chief Laurence Rankin: I'd like to add to that. The proposed increase of the threshold would limit the situations in which this tool could be used, as it requires us to demonstrate necessity in order to prevent terrorist activity. Yes, it would raise the threshold, and it would limit the range of our solutions.

Mr. Glen Motz: Thank you.

I have one last question for each you. I have about three minutes left.

Chief, you spoke specifically to the three concerns that you have as a police association with respect to terrorism peace bonds—which we've kind of covered off—the intel-to-evidence, and the encryption. We've heard from a few witnesses so far at this committee who have expanded upon their thoughts and given us some indication of what they would like to see more of or improved upon in this bill as it's currently written, which is why we're having the debate now, before second reading. We can make some changes, which is great.

If you were to change Bill C-59 in ways that you think would be absolutely critical for public safety—keeping in mind the balance between rights and privacy—what would those changes be, and how would they be accomplished?

I'd like to hear from both of you on that, if I could.

● (1120)

Chief Paul Martin: Are you speaking specifically to the encryption piece?

Mr. Glen Motz: Any aspect of this legislation.

Chief Paul Martin: Okay. I'll speak to the encryption piece and I'll let Laurence step in from there. I know the debates with respect to privacy and individual rights versus the collective safety and well-being. As I said at the outset, it's about the principles of intercepting those private communications, as opposed to the technology being used today, so that's what I've encouraged the committee to think about as it goes over this bill.

In the case of telecommunications companies, they are required to maintain this information for a period of time, subject to proper judicial authorization to look at this information. That may not currently exist with some of the applications and things that we see nowadays. As to how that is done, you're probably in a better position to answer that than I am.

It's about the principles of intercepting communication of people that intend to cause harm through terrorism or organized crime, as opposed to the technology used.

If I could sum it up very quickly, that's what I would ask the committee to consider.

D/Chief Laurence Rankin: Legislative reform is required to keep pace with the changing technologies—that's the bottom line—everything from data preservation standards for corporations that hold data, as they're getting shorter and shorter, so that it's more of a challenge for police to collect that data....

Again, enhancing powers to enable domestic production orders for foreign data and advocacy for effective lawful access.... We recognize that some ability to access evidence when judicial authorization is granted is required. We can look to Australia and the European Union, as to what they're doing in terms of cybercrime legislation. We recognize that secure data and communication enables commerce and social interaction in today's reality, but when we have a court order and we can't get the access to information on a computer that's been judicially authorized, then that's a problem for the police. That's not just for national security, but for the policing of organized crime in every other facet. I think more so now than ever before, every crime we seem to investigate, whether it's got a national security component to it or not, has a cyber-enabled component to it. At times, the challenges that we're facing seem insurmountable. Therefore, a balance has to be struck to recognize that if we're given access to enter a house with a court order, we can enter a house, but we can't enter a computer if it's encrypted.

The Chair: Thank you, Mr. Motz.

Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Chair, and thank you both for being here today.

When we debated C-51 in the previous parliament, one of the issues that came up was that a lot of talk is given to legislation for keeping Canadians safe, but often one of the pieces that's forgotten is actually providing proper resources for police. One of the things that comes to mind is the police officer recruitment fund from the federal government that existed to help provinces and municipalities, as you obviously well know, and provide additional funding. This is a fund that was cut that's never been brought back that we wish would be there and be permanent. How important is it to actually have resources, beyond all the talk of legislation and all the procedures, so you know that you have the ability to properly equip and train those men and women on the front lines in order to keep Canadians safe?

Chief Paul Martin: That's a very good question.

I've had discussions with our colleagues at the RCMP throughout the province and nationally through this committee and then, of course, locally. I would suggest to you that this type of threat that we're seeing with terrorism, which a lot of people attribute to the watershed moment of 9/11, has really drawn on our resources. I know for a fact that whether it's the RCMP or whether it's locally, we've had to redirect resources from other things in order to address this ongoing and serious threat. Depending on world events, that's scalable. It moves up and down depending on what's going on in the world.

We've dedicated resources to counterterrorism and anti-terrorism, but have not been able to backfill or replace those resources behind that to deal with other, more traditional things, such as organized crime and other things that the police deal with, either within jurisdictions or federally.

Therefore, it is very much an issue and it's one of those things—to use the analogy, you can only spread the peanut butter so thin and then what happens when things start to fall between the cracks.

I'll turn it over to Laurence before I get on my pulpit.

● (1125)

D/Chief Laurence Rankin : On the heels of the chief's remarks, looking at it again, and from a municipal perspective, we're attempting to increase our number of secondments to RCMP E Division INSET unit. We currently have only two members seconded. We're going to three, but I would like to see that increase even more.

Within the Vancouver Police Department over the last six years, we've increased the number of files that my unit, which looks into counterterrorism and national security files, from 13 files to 268 files, without an increase in our staff. In fact, it's a decrease because, as Chief Martin pointed out, we're having other issues, like a regional gang war that's going on right now, so we're very much stretched to the limit. We are called upon, in the first instance, to look at potential bomb calls; anti-government remarks regarding ISIS or al Qaeda; suspicious circumstances, such as people taking photographs of critical infrastructure; and then individuals who are involved in terrorism or radicalism. We, as a police jurisdiction, will look at those files initially, and if they meet the threshold for national security, then they are forwarded to INSET.

We're doing a lot of the training ourselves, in-house, whether it's a counterterrorism information officer training project or Operation SECURUS, working with the private sector to train businesses to become familiar with what to look for in terms of potential terrorist threats.

That said, our relationship with INSET has probably never been better. It's just that we're all at our end—and I won't speak on behalf of the RCMP—spread very thinly.

Mr. Matthew Dubé: Hypotheticals are always a dangerous thing in this line of work, in politics, and you might not want to go down this slippery slope, but how many of these cases would be dealt with simply by having more resources to deal with them, as opposed to actually bringing in legislative change?

Chief Paul Martin: From my perspective, it's about dealing with things in a more timely manner. I don't know if we'll necessarily.... We'll always redirect our resources to the higher priorities—if things are not at the highest priority, they may take a little more time to respond to—so obviously we're going to respond to them more quickly.

I think the question came up that it's not just returning foreign fighters, that it's not just radicalization to violence that we've seen on the Internet, but there has been right-wing extremism in this country, and it's rising again. We've seen it in the United States in some of the acts there, and of course in Quebec. All of these things are happening at the same time.

To answer your question simply, I think it's about dealing with more priorities in a more timely fashion, if we had the resources to do that.

Mr. Matthew Dubé: You mentioned intel-to-evidence, but there is also this issue even with regard to terrorism charges. With the situation in Edmonton, if I'm not mistaken, the terrorism charges in many of these cases become moot because the other crimes that have been committed, the different forms of violence, provide enough charges where the prosecution can proceed without having to go down that path.

How challenging is this notion of identifying what is or isn't terrorism, and how does that pose any challenges for the work that you do?

D/Chief Laurence Rankin : Chief, can I jump in?

Chief Paul Martin: Go ahead, please.

D/Chief Laurence Rankin: On the point you just made, to prove a component of a threat to the security of Canada, we're looking at having to collect evidence that demonstrates the crime was motivated by political, religious, or ideological objectives within Canada.

The issue we have—and, again, you've appropriately noted it—is that investigators are looking at an offence that involves perhaps the murder of an individual. While there could be a national security component, the elements of that traditional offence for murder are met and that investigation is launched.

The other issue we're dealing with now, whether it's traditional crime, if you will, or national security or terrorism, is that we have the Jordan decision out of the Supreme Court of Canada that sets prescribed timelines from the moment a person is arrested and charged until they're convicted, so the clock is ticking for collecting evidence. If we have the evidence at hand to prove a murder charge versus having to dig deeper to collect the evidence for political, religious, or ideological elements of that offence, that poses a challenge, and then police have to make that decision. Of course, it's in discussion with the RCMP because of the nature of the act, but those are the challenges we face.

If I could just add one more thing, the additional challenge—

● (1130)

The Chair: Can you add one more thing on another question, please, possibly in response to Ms. Damoff?

Ms. Damoff, you have seven minutes.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): I just want to start by thanking you both for your service and for being here today with your testimony. It's much appreciated.

I first want to start on the encryption piece because when we were doing our study on the national security framework, the chiefs of police were here talking about the need to have access to encrypted data. Then when we subsequently went on the road with the committee across Canada and had further witnesses, we heard overwhelming testimony that encryption isn't what we used to think about during the First World War or Second World War where it's encrypted data and somebody breaks the code and everything's good. It's actually when we give a back door to the good guys, like you folks, we actually are giving a back door to the bad guys as well. I've had numerous conversations with people who work in that field who said that's absolutely true.

You're in a bit of a conundrum here, as you don't want to make it easier for the bad guys to have access to data. I'm just wondering if you want to comment on that and if there's anything in this legislation that would be able to assist you without also assisting the bad guys from getting access to data.

Either of you would be fine.

D/Chief Laurence Rankin: I'll start. I don't know if there is an easy answer to that question.

I'd say that the barrier of encryption prevents us from obtaining a full picture of the evidence that is in the possession of the individual the police are investigating. I've talked to some of my tech crime people and they say you can have encryption technology today that will eventually be defeated and there will be a workaround or, though research, we'll be able to find a way, if you will a back-door way, to defeat the encryption. I think that whatever we will come up with, the bad guys will find a way or discover it in the same manner. I think what we find now is that police are simply not equipped to deal with it as effectively, in some cases, as the bad guys. That's the position we find ourselves in time and again.

Ms. Pam Damoff: We are talking about terrorists. We've already brought up 9/11, ISIS, al Qaeda, that side of it, and certainly you were talking about the far right. We've seen it in Sainte-Foy, in Las Vegas in the United States, and we tend to not focus on that. I'm just wondering if you could comment on the challenges you're facing. When the minister was here, he said these types of acts are by lone wolves and they're very difficult for law enforcement or Public Safety to deal with, these lone wolves who've been radicalized, but we are seeing quite a few of these radicalizations to the far right and we don't talk about them quite as much.

Could either of you speak to that?

Chief Paul Martin: I'm fortunate to live in a jurisdiction where one of our professors at the university is a subject matter expert on right-wing extremism, so I have a little bit of knowledge from her. The one thing about right-wing extremism is it cannot be underestimated here or elsewhere.

The biggest difference, to my understanding, between right-wing extremism and what we're seeing from Islamic extremism is really how organized they are. So when you talk about them being lone wolves, there's perhaps a little bit more to that, but they're not quite as organized nationally and internationally perhaps as others. That's really the biggest difference, as I understand it, but it cannot be underestimated and it is still a threat within this country and elsewhere.

Ms. Pam Damoff: Turning to the legislation itself, we have had testimony on this, as well as an open letter that was talking about the new offence that was in Bill C-51 on advocating or promoting the commission of terrorism offences in general and the broad definition of "terrorist propaganda". When we had the minister here, he talked about how, in Bill C-59, we've amended that wording because it was actually too vague and no charges had been laid because they weren't enforceable in court.

Do you feel these changes will assist you in actually being able to lay charges that can be enforced in court?

● (1135)

Chief Paul Martin: It is a change. It's a bit of a different threshold, but "counselling" to an offence has a firmer position in law than what we see with "advocating". When you talk about advocating, probably the closest thing I can think of is the hate crime legislation. There has been rarely, to my knowledge, but certainly some activity or some prosecutions under that legislation as well. From my perspective with the CACP, "counselling" has a firmer place in law and probably is going to be better to move forward, should we want to lay those charges.

Ms. Pam Damoff: We certainly want you to be able to lay charges and then have them go through when it gets to court.

Chief Paul Martin: It's going to be a little more restrictive, as opposed to just advocating on YouTube and then promoting it. From what we can determine, it'll probably be more successful in the end.

Ms. Pam Damoff: We also heard about challenges caused by law enforcement working in silos. You have the RCMP, CSIS. Do you think the proposed national security and intelligence review agency created in Bill C-59 will help ensure that information will be shared in a timely manner? Have you looked at that aspect of it?

Chief Paul Martin: I know that at CSIS national security headquarters, there's a constant flow of information between CSIS and the RCMP. The only thing I've heard, in my own jurisdiction, is that the disclosure letters go directly to the RCMP. They don't share them with other intelligence agencies, like the provincial anti-terrorism squad here in Ontario.

Through the national security headquarters, there is a constant flow of information between the RCMP and CSIS. I think the information flow is very good at the top end, the federal end. Then it's just what it takes to move from the federal to the rest of the agencies across the country.

The Chair: Thank you.

Mr. Paul-Hus.

[*Translation*]

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

My thanks to the witnesses as well.

Your testimony on national security is very important. Our primary objective is to see whether Bill C-59 will allow the police forces you represent to continue to do their work.

As I understand it, terrorism and the return of ISIS fighters worries you a great deal. On the one hand, without giving much away, the government has confirmed that some safeguards are in place, but on the other hand, you seem to be saying that there is a problem.

Can you give me more information about this? Is there a problem with communication between Canada's intelligence services, the RCMP and the police forces you represent at more regional and municipal levels?

[*English*]

Chief Paul Martin: I wouldn't say that there's an issue with respect to communications, if you're talking about the returning foreign fighter phenomenon. It's not so much the information-sharing that's causing the problem. It really comes down to whether we have the resources. If they come back en masse, we need the resources to determine what their activities are within this country, and if their intent is honourable or not.

Other countries have experienced greater numbers of these people than Canada has, but when the returning foreign fighters come back here, we have to make sure to determine what they're up to. Right now, as I understand it, there have been—and I can check the numbers—very few people who have been charged *in absentia* or have been charged after they've returned here. We had evidence to support the charge when they returned to our soil.

A lot of these people are returning from theatre. We don't know what their activities were in their entirety, but we knew they were there and they were up to something. We don't have the evidence to prosecute. As Deputy Rankin said, it comes down to whether we have the resources to do surveillance and make sure that they're not carrying on activities that are going to be harmful to Canadian citizens.

Laurence.

● (1140)

D/Chief Laurence Rankin: Four high-risk travellers have been charged *in absentia*. As Chief Martin said, trying to collect the evidence of what foreign fighters were up to overseas is difficult in a theatre of war. We may collect evidence or be provided evidence, information, or intelligence, but this comes with a series of caveats that often makes it impossible to use. The fear is that the people who provided that information may have their lives placed in jeopardy, or that investigative techniques used by an agency may be released.

Oftentimes information is given the RCMP, which may turn it over to police in jurisdictions. Basically, however, it's kept in secret because of the caveats in place. Ultimately, if we do lay a charge against an individual, all this information that has been collected or utilized by the police of jurisdiction or the RCMP has to be disclosed in court. These are the hurdles that have to be overcome before we can have a successful charge. We have to look at all these factors and determine whether the investigation can stand on its own if we peel away certain pieces of information that can't be released in open court.

[*Translation*]

Mr. Pierre Paul-Hus: You just talked about people who went abroad to join the jihad and then came back; that's one problem. Another is the domestic issue in Canada. You said that, in Vancouver, the number of identified individuals has gone up from 13 to 268, and that there is a problem with resources.

For the purposes of our study, we need to know whether parts of Bill C-59 may be reducing your legal capacity to intervene. You talked about the need to request a warrant from a judge in order to intervene if the possibility of a terrorism offence is detected.

Do you think Bill C-59 contains problematic provisions that are likely to interfere with your work on the ground?

[*English*]

The Chair: That's an important question. Unfortunately, you have about 20 seconds to answer it.

Chief Paul Martin: We've addressed it to some degree, but yes, whenever you raise some of the thresholds, it does make it a bit more difficult to convince a judge that we need to proceed with this. Any time the thresholds are raised, it could cause some issues. That remains to be seen, but that said, we do have a lot of tools at our disposal currently to fight terrorism in this country.

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

Mr. Fragiskatos, you have five minutes, please.

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

For the understanding of all of us, I want to go over something we just heard. Without clear evidence, it's hard to arrest, prosecute, and convict suspected foreign fighters, correct?

Chief Paul Martin: Yes.

Mr. Peter Fragiskatos: Okay, and that was the case under this government and under the previous government, because a number of foreign fighters returned under the previous government.

Chief Paul Martin: Yes, and going back to my point about the three issues, it's the intelligence-to-evidence conundrum, really. Laurence spoke to it a bit more eloquently than I. Some of this information is gathered in theatre. It's difficult, first of all, to protect the identity of the individuals who are providing it, where it's coming from. The caveat behind this intelligence is that it can't be used as evidence.

Mr. Peter Fragiskatos: I appreciate that, sir.

Chief Paul Martin: That's where the problem lies.

Mr. Peter Fragiskatos: I don't mean to interrupt you. I have just five minutes and a few questions, but thank you very much.

You're talking about how, in theatre, it's very difficult to extract evidence from conflict settings such as Syria or Iraq, or countries in that type of situation.

Chief Paul Martin: That's right.

Mr. Peter Fragiskatos: My colleague Mr. Motz brought up the matter of preventative arrests. The preventative arrest measure, first introduced in Canada in 2001, has never been used, correct?

Chief Paul Martin: I don't have that.

● (1145)

Mr. Peter Fragiskatos: I'm just quoting legal analyses from a number of commentators. We've heard from Professors Roach and Forcese at this committee, who have examined this and have been very clear that the preventative arrest measure has never been used.

D/Chief Laurence Rankin: That's correct.

Mr. Peter Fragiskatos: A higher threshold was indeed put in place in Bill C-59. That responded to a long-standing concern among civil rights advocates who were of the view, and I think it's a reasonable position to hold, that to detain someone without a warrant for up to seven days, without applying a criminal charge, as the preventative arrest measure allows for, is questionable. In a democracy, you can at least have that debate.

The government has looked at Bill C-51 and introduced a change. Under Bill C-51, as we heard, an arrest could happen when it was "likely to prevent" a terrorist act. Now, in Bill C-59, an arrest can be made when, on reasonable grounds, there is suspicion to believe a terrorist act might be taking place. You still have that ability to lay an arrest, and in emergency situations it's there. This isn't preventing you from acting as police, correct?

Chief Paul Martin: No, it just changes the threshold, as you pointed out.

Mr. Peter Fragiskatos: Okay. Thank you very much.

We heard from the British Columbia Civil Liberties Association a few days ago, who told us of a number of concerns. In a subsequent article that was written since their testimony there was concern expressed about Bill C-59 on cyber-operations that could be conducted by the Communications Security Establishment. Since you focused today a great deal on the technological aspects of terror and how that can jeopardize Canadian security, I want to ask you about that.

Their view is that Bill C-59, by empowering the CSE to conduct cyber-operations against foreign actors, constitutes a danger. Specifically, it would normalize state-sponsored hacking. Can you speak again to the importance of cyber-operations from a security perspective? How critical is this? The nature of security is changing. Canadians deserve to be protected. We have to make sure that our approaches are keeping up with changes that are under way.

Chief Paul Martin: I think the simplest way for me to sum it up is what Laurence mentioned. Really, nowadays, either technology is the target or it enables the crimes to be committed. Everything we do and everything we encounter from a policing standpoint involves some form of technology at this stage of the game.

Mr. Peter Fragiskatos: You would agree that going down this road of allowing CSE to conduct cyber-operations against foreign actors is a welcome change?

Chief Paul Martin: Go ahead, Laurence.

D/Chief Laurence Rankin: I can't speak for the CSE, but I would say that if you're looking at it in terms of law enforcement in Canada, we're having to seek judicial authorization to obtain this information. We're being challenged day in and day out by encryption.

We're not arbitrarily going in and searching people's computers without the requisite permission or authorization. What CSE is doing and what we're doing are really two different things. I'm not in a position to comment on that. I am in a position to say that we have a number of challenges, encryption being one of them, as is trying to collect that evidence in a timely manner. Legislation isn't keeping up. Technology is speeding ahead. We're having to adhere to court decisions out of the Supreme Court—such as Jordan—which place an addition burden on law enforcement—

Mr. Peter Fragiskatos: Thank you.

The Chair: Thank you, Mr. Fragiskatos. You always ask the most difficult questions at the end.

Mr. Brassard, welcome to the committee. Five minutes, please.

Mr. John Brassard (Barrie—Innisfil, CPC): Thank you, Mr. Chair. I'll get right into it.

As an opposition, we have been asking the government on numerous occasions about the returning foreign fighters. One of the responses that was given by Minister Goodale is that "our government uses a variety of tools to combat terrorism, including the Global Coalition against Daesh, security investigations, surveillance, monitoring, intelligence gathering, lawful sharing, collection of" information.... He also said "peace bonds".

One of the things you said, Mr. Martin, that was quite disturbing to me was the fact that currently there are zero peace bonds that exist in Canada, and yet there are returning jihadists that we're aware of. We're not aware of the exact number. Do you find it problematic that we're not issuing peace bonds to monitor returning jihadist terrorists at this point?

● (1150)

Chief Paul Martin: There would have to be a threshold in order to get a peace bond for one of these individuals in the first place, so they'd have to demonstrate something. I can't speak to any specific cases or things that are being looked at, but yes, currently there are none in effect right now. There have been, and should it be appropriate to do so and we have the evidence to get it, that's what we would be seeking.

Mr. John Brassard: My question, then, is, if this piece of legislation asks for that threshold to increase from where it was previously, is there the potential or the risk that law-abiding Canadians are being placed at risk at this point, given the fact we are aware—the government is aware—that there are returning jihadists? We don't know the number, but we know they're out there. Is the Canadian public at increased risk because of the increase in that threshold?

Chief Paul Martin: Well, any increase in the threshold will make it a little more difficult for law enforcement to potentially get a peace bond. What we'd have to use is one of the other tools at our disposal. Perhaps that is surveillance or some other tool that is available to law enforcement and that we could use at that time. Law enforcement—and I'm sure I can speak for our RCMP brothers across this country—is not going to allow Canadians to be at risk if we can do something about it and we have tools at our disposal.

Mr. John Brassard: I want to go back to something you said earlier about resources. Currently, how stretched are your resources to deal with this issue?

Chief Paul Martin: My service specifically is stretched to the maximum in dealing with traditional crimes, as Laurence would describe them, such as homicides and those types of things and the increases in certain types of crimes, and also dealing with these emerging issues, such as human trafficking, terrorism, and all these types of things that are relatively new on the horizon. It's stretching us to the limit. We try to prioritize and triage these types of investigations and make sure that we deal with the ones that are most imminent.

Mr. John Brassard: Thank you. That's all I have.

The Chair: Thank you, Mr. Brassard.

[*Translation*]

Mr. Picard, you have five minutes.

[*English*]

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

I have a lot of questions. Something popped up in my mind: my colleague here has suggested a very good idea. Patrolmen and -women have the challenge of being on the street and facing everyone on a daily basis. Based on that knowledge of what goes on on the street, what is your interpretation of the level of risk or danger the Canadian population faces? Has this changed, increased, or decreased over the last five or six years?

Chief Paul Martin: What is my assessment of the risk to front-line officers, to the public?

Mr. Michel Picard: Is the Canadian population more at risk now than it was six years ago?

Chief Paul Martin: With the returning foreign fighters, the prolific use of the Internet to try to incite people or get people to radicalize, I would suggest that yes, in my estimation the risk to the Canadian public is higher than it was six or seven years ago.

Mr. Michel Picard: To your knowledge is this situation very recent, or did we start to look at those issues five years ago? The Internet for example, propaganda, and....

Have you looked at cases where we start to see more Internet propaganda messages? Without knowing how to quantify one person travelling abroad, apparently we have a possible foreign fighter coming back. We didn't start to look at that last year, did we?

D/Chief Laurence Rankin: Chief, can I just interject?

Chief Paul Martin: Yes.

D/Chief Laurence Rankin: More so now than even in the last few years, I think we're looking at what appears to be the end of the caliphate. Where do these fighters go? I think what you're seeing in Europe and in the U.K. and potentially in the United States, could very well be reflected in what we see in Canada. I think that is the issue. Foreign fighters or others whom we may not be aware of yet are coming back because they have nowhere else to fight.

That is becoming more prominent.

● (1155)

Mr. Michel Picard: That triggers an interesting exchange of information among different levels of police forces. Is security clearance an issue in those communications?

D/Chief Laurence Rankin: At the municipal level, the members who are liaising with INSET, at the RCMP, have top secret security clearance. Again, information is going from national security headquarters to the respective INSET. We are updated on certain files on a regular basis. Our members who are working on these types of investigations from a municipal perspective are liaising with our INSET investigators on a regular basis, exchanging information, providing them with information.

Mr. Michel Picard: Does the need-to-know basis limit some information accessible to you when you approach someone, if you expect the person to be a potential foreign fighter? Does that change your position and the means that you have at your disposal to act toward this person? What is your interpretation of what we call foreign fighters from the street standpoint, the patrol person standpoint? When you look at someone and you say he might be a foreign fighter, what are the means at the disposal of the police force on the street then?

D/Chief Laurence Rankin: Certainly we've embraced training related to that front-line encounter within our own department. It's sponsored largely by the RCMP with the first responder terrorism awareness program. That's providing training throughout the country. Front-line officers are aware of what to look for with respect to potential foreign fighters, not just with Islamic foreign fighters, but right-wing extremists as well.

Mr. Michel Picard: Thank you, gentlemen.

The Chair: For the last few minutes, we have Mr. Dubé, please.

Mr. Matthew Dubé: Thank you, Chair.

Deputy Chief Rankin, did I hear you correctly earlier when you said that even with a warrant you couldn't gain access to laptops, computers, or things like that?

D/Chief Laurence Rankin: Yes.

Mr. Matthew Dubé: Can you explain what you mean by that?

D/Chief Laurence Rankin: The encryption on the device, whether it's a phone or a computer, is such that we don't have the technology that would allow us to circumvent or overcome the encryption. The evidence that could be contained within that device is kept from us. That's one issue.

What we'll find in investigations, and I can speak more from traditional criminal investigations, is that we will then often liaise with other police agencies, including the RCMP, to determine if they have technology that could assist us in defeating the encrypted device. That is a significant issue for a criminal investigation, but it would also impact national security investigations, where we lay a criminal charge and then only discover additional compelling information or evidence a year later when we're able to get into the device. We may not be able to disclose that information in a timely manner without jeopardizing the convicting charge—

Mr. Matthew Dubé: Thank you.

The comparison might not be appropriate, but looking at the debate that goes on about looking at peoples' cellphones at the border, many have argued that having a cellphone is not like having a suitcase. When you cross the border, you have an expectation that your suitcase will be searched, that it's okay to look through clothes and things like that, whereas on a cellphone you can have banking information, health information, all kinds of information that puts someone's privacy in jeopardy in a different way. Notwithstanding any crime that may or may not have been committed, is there a concern about accessing, for example, laptops and phones? Then by decrypting that, you're getting access to a whole swath of information that casts a fairly large net.

The Chair: Reply very briefly, please. Thank you.

D/Chief Laurence Rankin: There is a danger in that, and I think we have to be precise in terms of the affidavit that's being drafted to gain access to that device, and in terms of the understanding of the justice or magistrate who's issuing that warrant that we're prescribed about where we can search and what data we could look at.

● (1200)

The Chair: Thank you, Mr. Dubé.

That'll have to bring our session to a close. On behalf of the committee I want to thank you, Chief Martin and Deputy Chief Constable Rankin. Your testimony has been very valuable to the considerations that this committee is undergoing.

With that we'll suspend.

● (1200)

(Pause)

● (1200)

The Chair: Colleagues, can we come back to order? We have as witnesses the Canadian Bar Association represented by Mr. Edelmann and Ms. Carter, and as an individual, Christina Szurlej from the Atlantic Human Rights Centre, who is not presently here.

We'll go with the Canadian Bar Association, and we look forward to your presentation.

Ms. Gillian Carter (Staff Lawyer, Legislation and Law Reform, Canadian Bar Association): Thank you, Mr. Chair and honourable members of the committee. My name is Gillian Carter, and I am a staff lawyer with the law reform directorate at the Canadian Bar Association. Thank you for inviting the CBA to discuss Bill C-59 with you today.

The CBA is a national association of more than 36,000 lawyers, notaries, law teachers, and academics. An important aspect of our mandate is to seek improvements in the law and the administration of justice, and that is what brings us here today.

The CBA has offered its views and expertise at many stages in the development of Canada's national security and anti-terrorism regime. Our written submission on Bill C-59 was prepared by multiple sections of the CBA, including the criminal justice, immigration law, charities and not-for-profit, military law, and privacy and access to information law sections. With me today is Peter Edelmann, a member of the immigration law and criminal law sections and a lawyer specializing in immigration law.

I will now turn it over to Peter to address the main points of our submission.

● (1205)

[*Translation*]

Mr. Peter Edelmann (Member-at-Large, Immigration Law Section, Canadian Bar Association): Thank you very much for inviting me to appear before you today.

Bill C-59 proposes complex and major updates to national security law. It would address several decisions of the Federal Court of Canada, and widespread concerns expressed about Bill C-51 in 2015.

The Canadian Bar Association generally supports the goals and structure of Bill C-59 as a positive change, modernizing the legal framework for Canada's national security infrastructure and increasing transparency, oversight and review, features that have previously been lacking. Our comments and analysis of the proposals in Bill C-59 are offered in hopes of further improving the bill.

[*English*]

Our written submissions provide a number of specific recommendations and I would refer you to those for the more technical amendments we propose. I will use my time today to focus on two or three areas of broader concern.

First of all, we support the creation of the national security and intelligence review agency, the NSIRA. I just have a couple of comments with respect to it but in particular with respect to the mandate. While we commend the decision to avoid language that would unnecessarily restrict the agency's mandate, an overly broad mandate could hinder the agency's ability to focus and assess its performance against its mandate.

In the way that it's drafted now, the NSIRA has responsibility for broad review of any activity of "a department that relates to national security or intelligence". "Intelligence" is a very broad term. It could include things that are done by anything from the Canada Revenue Agency to Fisheries and Oceans, police departments, etc.

"National security" is also problematic given the multiple definitions that we see in different pieces of legislation. In particular, we remain concerned about the SCISA, the Security of Canada Information Sharing Act, or with the amendments that we have today. The breadth of the definition of an "activity that undermines the security of Canada" in section 2 is still very broad and notably it's different from the definition in the CSIS Act of "threats to the security of Canada". Having two definitions is not helpful. It's confusing and it doesn't provide a clear mandate for national security agencies and in particular for an oversight or review agency.

I would also note in passing that the amendment to the exception in section 2(2) of the SCISA is troubling as it actually substantially reduces the protection under the current version. Several legitimate political activities might be seen on their face as undermining the sovereignty or territorial integrity of Canada.

In the past, we've recommended that there be one coherent, clear definition of "national security" and we continue to be of that view. It's also unclear whether certain other activities fall under the definition of "national security" at all. For example, the Secure Air Travel Act, SATA, does not refer to national security and it's unclear whether the review of SATA activities would fall under the NSIRA or not. In other words, is this national security legislation? Does it fall under NSIRA?

The coordination of the work of the NSIRA with other review agencies is obviously key although we would note that there remain significant gaps in the review framework. The problem is particularly stark with the Canada Border Services Agency, and we've expressed concerns about this lack of independent review of the CBSA in several past submissions.

CBSA remains one of the largest law enforcement agencies in the country and has no independent oversight or review at all. This is not a role that NSIRA should take on although it does highlight the problem of having a vague definition of "national security" because arguably everything that Canada Border Services Agency does could fall into a broad understanding of national security in a vague sense.

Everyday complaints about problems at the border should not be burdening NSIRA and its resources. A specialized review agency is required.

We also have concerns, in particular, with respect to NSIRA's access to information, and in particular that NSIRA would have access to any information other than a cabinet confidence that it deems necessary to conduct its work. This would extend explicitly to information subject to solicitor-client privilege, professional secrecy of advocates and notaries, or litigation privilege, creating an open-ended mechanism to review legal advice given to the government. This is of significant concern to the CBA.

The role of solicitor-client privilege is fundamental to the functioning of our justice system and this is as true for government actors as it is for private actors. It has been argued that privileged information must be made available because the practices of security agencies often depend on the legal advice they receive.

● (1210)

However, without assurances of privilege, legal advice will be sought less often, based on less candid disclosure by client agencies, or worse, sought and received but not documented.

The other problem with respect to the disclosure of solicitor-client privileged information is how the NSIRA then deals with it in its reports. It's not helpful for the NSIRA to have solicitor-client privileged information. What they need is information about how this is actually deployed in the agency, not the advice that was given behind those decisions.

Concerning the intelligence commissioner, the CBA supports the creation of an independent specialized office for the oversight and authorization of activities by the CSE and CSIS. We have generally called for judicial oversight, but we recognize the advantages of a dedicated commissioner with staff and resources to allow effective ongoing oversight.

The nature of the review mandated by sections 14 to 21 of the proposed intelligence commissioner act does create some concerns for us because there's a system of nested reasonableness findings. Instead of the normal process in front of a judge for a warrant where a judge would find whether there are reasonable grounds to issue a warrant, what the legislation currently foresees is that the minister would make a finding on reasonable grounds, and then the intelligence commissioner would review that on a reasonableness standard.

This creates two problems from our perspective. First, it's unclear how much deference that implies. There's an extensive debate in the courts right now around the application of the reasonableness standard at all and how that plays out in terms of deference.

There's no need to bring that confusion into this area, and there is not that confusion around the reasonable grounds standard, so there's no reason for this nested reasonableness finding other than creating a level of confusion as to how much oversight is actually being provided, in particular because it's going to be provided behind closed doors. It's important for Canadians to understand what the intelligence commissioner is doing and that it be clear.

With respect to the CSE, the CBA generally supports the more detailed mandate of the CSE, and we support the structure as it's being proposed. There are several elements of the proposed mandates that are in tension with one another, in particular, the offence and defence in cyber-operations.

We would recommend that there be an explicit vulnerabilities equities process as part of the mandate of the CSE, so that the balancing can happen in a transparent way. The U.S. has a process in place that might work as a model, or at least give ideas with respect to that.

With respect to CSIS, we continue to have concerns around the disruption powers. In particular, giving kinetic powers to CSIS comes away from the mandate of creating CSIS in the first place, after the McDonald Commission.

I'll refer you to our written submissions with respect to our concerns around section 12.1(3.2). We continue to have concerns similar to those we've had in the past with respect to these warrants limiting charter rights in that context.

Finally, I would note with respect to the Criminal Code provision of counselling of terrorism offence, in my view, following the jurisprudence of the Supreme Court in Hamilton, the counselling offences in the Criminal Code already cover everything this offence covers. There is no need to further complicate the Criminal Code. It's already too complex. It ought to be simplified, and the counselling offence covers everything you're hoping to cover here.

Thank you very much for your time, and I apologize if I went a little bit over.

● (1215)

The Chair: Thank you very much.

Now Ms. Szurlej has arrived from the Atlantic Human Rights Centre at St. Thomas University.

You have 10 minutes, please.

Dr. Christina Szurlej (Endowed Chair, Atlantic Human Rights Centre, St. Thomas University, As an Individual): Mr. Chair, Mr. Clerk, and honourable committee members, thank you for the opportunity to testify before you regarding Canada's national security framework.

Following a set of national consultations regarding the Anti-terrorism Act, formerly Bill C-51, the Liberal government drafted Bill C-59, An Act respecting national security matters to replace the Anti-terrorism Act.

I have reviewed the bill and will comment on it through a human rights lens. Securing the safety of its populace is a fundamental function of government. It is without question that government and its agencies must be equipped with the means necessary to prevent, counter, and address evolving threats in the digital age. In that same vein, a balance must be struck between securing public safety and respecting rights, ensuring any limitations placed on rights are necessary, proportionate, and reasonable.

As a human rights professor, I am pleased to see language recognizing the need to maintain respect for the Canadian Charter of Rights and Freedoms, the rule of law, accountability, and transparency within Bill C-59. The establishment of a national security and intelligence review agency with a mandate to review national security activities, consider complaints, and advance investigations is arguably the most significant advancement.

The bill also establishes an intelligence commissioner to review the reasonableness of Canadian Security Intelligence Service and Canadian Security Establishment authorizations regarding, *inter alia*, intelligence gathering and cybersecurity. Though Bill C-59 has addressed some shortcomings found in the Anti-terrorism Act of 2015, concerns remain regarding its impact on human rights, particularly the rights to privacy, freedom of assembly and association, freedom of expression, liberty and security, democratic rights, due process rights, and anti-discrimination protections.

Due to time constraints, this testimony focuses on concerns with amendments to the Canadian Security Intelligence Service Act regarding the collection, querying, exploitation, and retention of datasets. The act defines a “dataset” as the collection of information stored as an electronic record and characterized by common subject matter. A dataset could thus encompass any thematic electronic documentation, provided it is a publicly available dataset, relates primarily to non-Canadians living outside of Canada, or constitutes an approved class.

Though it is reassuring that a newly established intelligence commissioner would review classes of datasets to safeguard against abuse, the remainder of section 11.05(2) is read with caution. Use of the term “publicly available dataset” is misleading, as it can include information that is considered private under the Privacy Act, but is available in the public arena, potentially without the consent or knowledge of the person concerned. In other words, publicly available data can extend to private information made public on request, by subscription or by purchase. Rather than exploit this vulnerability by legitimizing and encouraging the commodification and exploitation of the public's data, the Government of Canada has a positive obligation to protect its populace against infringements by third parties that may compromise individual privacy in exchange for profit.

Granting government authority to collect publicly available data appears innocuous, but can reveal highly personal information in violation of the right to privacy. I also caution Canadians against blindly accepting mass government surveillance of foreigners. Though targeted surveillance may be necessary to thwart legitimate threats to peace and security, mass surveillance opens the door for foreign nations not accountable to Canadian voters to collect information about Canadians and share it with our governments, other nations, or corporations.

Under these circumstances, the Government of Canada could also place foreigners in danger by revealing compromising information to governments with poor human rights records. Differential respect for the privacy of Canadians versus non-Canadians outside the country also constitutes a violation of non-discrimination under the international covenant on civil and political rights.

● (1220)

The United Nations special rapporteur on the right to privacy has maintained that the distinction between one's own citizens and foreigners is not in compliance with the principles of the universal right to privacy.

Failing to properly restrain invasions of privacy could prompt charter violations of section 8 protecting against reasonable search or seizure or the promotion of presumption of innocence under section 11(d). In order to satisfy that such limitations are “demonstrably justifiable in a free and democratic society”, the onus is on the Government of Canada to prove these limitations are of sufficient importance, rationally connected to the objective, minimally impair rights, and produce an outcome that outweighs the gravity of the problem it seeks to address.

Though protecting public safety and national security is of sufficient importance to warrant a well-defined, targeted invasion of privacy, the mass collection of data that could lead to results that are relevant to the performance of CSIS's duties and functions is not sufficiently important to encroach on constitutionally protected rights.

Similarly, blanket collection of datasets merely "relevant" to the duties and functions of the service fails to demonstrate a direct rational connection to protecting public safety. If there is no direct connection to maintaining public safety and national security, why does the Government of Canada consider these proposed powers to be a necessary component of the national security framework?

The United Nations special rapporteur on the promotion and protection of human rights while countering terrorism has warned that "restrictions falling short of being necessary...constitute 'arbitrary' interference" with the right to privacy. The special rapporteur further stressed that, "for a restriction to be permissible, it is not enough that it serves one of the enumerated legislative aims; it must also be necessary for reaching the legislative aim." Given that the aim of Bill C-59 is to protect national security, the blanket collection of any data relevant to the work of CSIS does not satisfy this test.

Information respecting the protection of public safety and national security in Canada should be narrowly defined and collected only "to the extent that is strictly necessary" and when there are reasonable grounds to suspect a threat to the security of Canada. If we allow the bulk collection and storage of personal data without a person's knowledge, consent, or ability to challenge the nature and authenticity of information collected, the next step could be to misuse, alter, deliberately conceal, or manipulate information.

Indeed, the Canadian Security Intelligence Agency Act allows a CSIS director to authorize designated employees to commit direct "acts or omissions that would otherwise constitute offences" in carrying out their duties and responsibilities. Theoretically, the minister could authorize the collection of datasets intended to assist CSIS employees with carrying out otherwise criminal activity. Are these powers consistent with the preamble of Bill C-59, which claims to respect the Canadian Charter of Rights and Freedoms, the rule of law, as well as accountability and transparency, while championing national security?

Amendments to the act do advance safeguards, but the nature of these safeguards raises concerns. The bill includes provisions calling for this service to delete information and datasets regarding the physical or mental health of an individual, information subject to solicitor-client privilege, and material in foreign datasets regarding Canadian citizens. This suggests some datasets will encapsulate information that should be accorded the highest degree of privacy.

The question is, why would the minister and intelligence commissioner approve a dataset that could potentially reveal this type of information about someone who has done nothing wrong? Further, the amendments should expressly state that accidental collection of such data will result in its total destruction, which clarifies the desired outcome more precisely than using the term "delete".

The Supreme Court of Canada has emphasized that "the protection of privacy is a prerequisite to individual security, self-fulfilment and autonomy as well as the maintenance of a thriving democratic society." Though not constitutionally protected itself, the right to privacy is essential for the maximum expression of most rights found under the charter, including freedom of expression; freedom of peaceful assembly; freedom of association; the right to vote; the right to life, liberty, and security; fair trial rights, including prevention of unreasonable search and seizure, protecting the presumption of innocence, and maintaining solicitor-client privilege as part of satisfying the right to a fair trial, particularly, the provision against self-incrimination.

● (1225)

Acknowledging the impact on constitutionally protected rights, any limitation of privacy rights should be justified under section 1 of the charter by applying the Oakes test. If the courts identify—

The Chair: Ms. Szurlej, you're past your time, but could you wind it up in the next 30 seconds?

Dr. Christina Szurlej: Sure.

What I'll focus on instead are my recommendations. They are as follows:

Ensure any limitation of human rights conforms with Canada's national and international obligations. Any encroachment on human rights must be necessary, proportionate, reasonable, and justifiable in a free and democratic society.

The government must ensure any collection of personal data is directly linked to protecting public safety and national security, rather than being tangentially connected to the duties and functions of CSIS or any other agency.

Legislation should be introduced to protect the Canadian populace from third party commodification of personal data through payment or subscription.

The national security and intelligence review agency should be provided with the authority to render binding decisions.

The role of the intelligence commissioner should be elevated from part-time to full-time status to reflect the breadth of the portfolio.

The Chair: Thank you, Ms. Szurlej.

Dr. Christina Szurlej: I need to say some final words and then wrap it up.

The Chair: The problem is that you end up cutting into members' time, and then they get mad at me, which is not really a good thing, in my view. So I'm going to turn—

Dr. Christina Szurlej: My final point is very important.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Maybe I can help her.

The Chair: Okay, you can help her with that final point, Ms. Dabrusin. I'll leave that between the two of you.

Ms. Julie Dabrusin: Can you briefly provide me with your final point, please?

Dr. Christina Szurlej: Thank you kindly. I greatly appreciate that.

Though I cannot in good faith support legislation permitting mass surveillance, for the reasons outlined above, if this option is advanced, the following is recommended. Clearly and comprehensively define “dataset”, “publicly available data”, and “exploitation of data”. Keep a record of every time a dataset is created, queried, and exploited, and by whom. The precise purpose for doing so should be recorded to enhance accountability. Records of such use should be sent periodically to the intelligence commissioner for review.

Ms. Julie Dabrusin: Thank you. What you can do is actually provide us with a written submission as well, and then we will all get it and we'll all be able to review it, but unfortunately, I don't have very much time and I had—

Prof. Christina Szurlej: You had other questions. Thank you very much.

Ms. Julie Dabrusin: I'm happy you were able to get that in.

I've mentioned this before over the past hearings. One of the big issues for people in my community, one of the things that has come up a lot, is ensuring that there is proper oversight across our national security agencies.

I wanted to start with a point that you had raised, Mr. Edelmann. You suggested that in fact NSIRA is overly broad, which is a different perspective from what I've often heard. It seemed to me that the idea of having a broad institution that breaks across the silos was exactly what we were trying to get to. Would that be solved by having a different definition for national security? You had mentioned national security as being part of the problem.

Mr. Peter Edelmann: The concern we have with the vagueness of the mandate is how NSIRA is to measure how it is being effective in relation to its mandate, and how it is to deploy its resources. If you have an overly broad definition of intelligence and national security in general, it covers such a broad swath of things that, where there is an actual requirement for oversight, the NSIRA may find itself overwhelmed with complaints about the Canada Border Services Agency, for example, or looking into intelligence activities of the Department of Fisheries and Oceans, or—

Ms. Julie Dabrusin: But how would we cure it? At this point we have legislation in front of us. From your perspective, what would you like to see us do to dig into that problem?

Mr. Peter Edelmann: What I would suggest is that there be one clear definition of national security and threats to national security. The definition in the CSIS Act has been used for a long time, and it's only with Bill C-51 that we ended up with another definition that created a lack of clarity with the Security of Canada Information Sharing Act. If the information sharing act is going to be that broad, there's no question that there does need to be oversight, and so it may be that the broader definition from the information sharing act is the one that ought to be used with respect to NSIRA.

Our view is that definition is overly broad and vague.

● (1230)

Ms. Julie Dabrusin: Looking at the CSIS Act definition might be something that would help.

Mr. Peter Edelmann: Correct. In terms of looking at the definitions that are there already, we have the definition already in the CSIS Act. With NSIRA there may be some concerns as to whether the CSE's mandate is somewhat broader, and there are some aspects of what the CSE is doing that might be outside of that. There may be some thought that might need to go into exactly what it is that NSIRA is overseeing and where the gaps are with the other oversight agencies.

In terms of what it ought to cover, or what ought to be covered by other agencies, in our submission, most of what CBSA does, for example, should just be covered by another oversight agency.

Ms. Julie Dabrusin: I like that you raise that point because it's something I'm also interested in. We now have NSIRA covering all the agencies, but I just wanted to confirm that you would need a separate entity for an independent review of CBSA..

Mr. Peter Edelmann: That's correct.

Ms. Julie Dabrusin: We were lucky to have the Information Commissioner come by. We saw someone from the OCSEC on Tuesday I believe, and I asked some questions. I was wondering what you would think of this. Right now there's an obligation in the commissioner's role in this new act to have written reasons when an authorization is turned down, but there isn't that same obligation when the commissioner says yes and approves an authorization. Do you think it would be helpful to have written reasons for the approvals as well as the turn-downs?

Mr. Peter Edelmann: Yes.

Ms. Julie Dabrusin: The other part is for emergency authorizations. Everyone seems to accept that emergency situations may come up and you don't want to go through the regular process. What about having an after-the-fact review by the OCSE commissioner?

Mr. Peter Edelmann: I think that ought to be done and ought to be a part of the mandate, given the particular expertise that the OCSE commissioner or the Information Commissioner would have.

Ms. Julie Dabrusin: Thank you.

An interesting thought raised in a citizen's lab report I was reviewing was about having a security-cleared amicus curiae review in private—this isn't a public review—decisions made by the commissioner.

What do you think about that? Have you looked at it?

Mr. Peter Edelmann: There are certain circumstances in which the courts will bring in an amicus curiae or special advocates with respect to specific concerns the courts have.

At the CBA, it's not something we've considered with respect to this particular framework, but it's definitely something that ought to be open and has been opened in the past to the federal court when bringing an amicus in with respect to specific concerns. If you look at the Re X decision, which underlies a lot of the concerns here, my recollection is that amici have on occasion been brought in to provide some submissions.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you for that, Ms. Dabrusin, and thank you for allowing Ms. Szurlej to use some of your time.

Mr. Paul-Hus.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you very much for joining us today.

In my naivety, I am trying to understand one thing. In my view, the two largest intelligence agencies in the world are Facebook and Google. I think we can agree on that. Moreover, most Canadians are on those networks.

When you sign up on Facebook, you must approve a list of regulations, which no one reads and to which everyone agrees. Details about your life are then published and you can be tracked and followed everywhere. People see no problem with that. Google and Facebook employees, be they in California or elsewhere in the world, can find out everything about our lives and no one makes a big deal out of it. However, people want to put restrictions and roadblocks on the work of the professionals in our intelligence agencies, who want to ensure that our society is protected.

How do you explain the fact that people are not concerned about Facebook or Google, but that there is a kind of restriction on the work of our intelligence officers?

● (1235)

Mr. Peter Edelmann: As I see it, there are two major differences between Google and Facebook and CSIS.

First, and most important, those are private companies and they do not carry out the powers of the Canadian state or any other state, nor do they have police powers.

Second, you say that everyone agrees to provide their personal information to Facebook or Google. But not everyone does. I agree with you that most Canadians, maybe even a large majority of Canadians, choose to do so, but it remains a choice.

However, when an individual's personal information ends up in CSIS' database, it is not the result of a choice. Moreover, people choosing not to provide their personal information to CSIS are exactly the ones whose personal information you would most like to see in that database.

Think about police states. As a lawyer practising in the field of refugee rights, I can tell you that China, North Korea, Iran and countries that repress rights and freedoms use the information we are talking about here in a non-transparent, uncontrolled way, which makes those freedoms fictional and nonexistent. By that, I do not mean that Canada is acting in that way, but we are actually talking about protecting ourselves against it.

Mr. Pierre Paul-Hus: By no means do we want Canada to become a police state, to start acting like North Korea or China, which are absolutely deplorable. That said, the objective is to protect ourselves. The world has changed, as have the threats to the world; these darned networks like Facebook are tools for hate-filled propaganda. And it does not necessarily come from here, it may very well come from elsewhere.

Let me go back to the act. Let us suppose that someone posts a video on YouTube in which he suggests attacking Canada or setting off a bomb, but without asking anyone specific to do so. In your opinion, should that individual be charged with counselling an attack?

Mr. Peter Edelmann: I recommend that you read the Supreme Court decision in *R. v. Hamilton*. Mr. Hamilton produced a CD containing instructions on ways to commit fraud, especially using credit cards. He had not counselled specific people to do so. For $30, he was selling online a CD explaining how to defraud the banks. The issue was whether he had counselled an offence. The provincial court, I believe, determined that he had not done so because they were not specific offences.

However, the Supreme Court held that it was a crime. What you are talking about here is already a crime just like any other crime, not simply in terms of terrorism. We could examine all the details of the Hamilton case, but the principles are already established in law. You cannot counsel—

Mr. Pierre Paul-Hus: Amendments have been made to the wording of Bill C-59, in order to make it more specific or broader.

Mr. Peter Edelmann: In my opinion, if you are looking to make it broader than the Hamilton decision, it is a problem. Actually, you would then be at the point where you might wonder whether it is even possible to discuss crimes or other subjects. Could you even talk about them, could you wonder whether when something or other could be done, could you discuss what constitutes a crime, or could you refer to other events?

You could get to a point where freedom of expression would become an issue again, which would be a problem.

● (1240)

Mr. Pierre Paul-Hus: Now I would like to go back to Ms. Szurlej.

Bill C-59 amends part 5 of the Security of Canada Information Sharing Act. You spoke about it a little. In terms of the threshold, could you tell us the difference you are making between "reasonably necessary" and "strictly necessary"?

Could you give us a concrete example of that?

[*English*]

Dr. Christina Szurlej: I would recommend that the standing committee look at the jurisprudence of the Supreme Court of Canada to determine what the threshold for reasonableness is, because it would surely remain consistent regardless of the crime.

If we're talking about invading the privacy of an individual, normally a warrant is required in order to do that. Yes, there might be exceptional circumstances in certain cases, but the Charter of Rights and Freedoms is in place for a reason—to constitutionally protect those rights—and any infringement must be reasonable.

Simply saying that the collection of data relates to the functions of CSIS doesn't meet that threshold. Perhaps clearly demonstrating that there is an actual threat to national security may cross that threshold.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Thank you.

[*Translation*]

Mr. Dubé, you have seven minutes.

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

One of the questions that often comes up deals with publicly available information, as we find in parts 3 and 4 of the bill. Could you tell me whether Canadian legislation or case law contains a definition of what "publicly available information" means?

Mr. Peter Edelmann: The case law provides a lot of room for discussion on what is publicly available.

For example, in terms of public access to the courts, one principle upholds the public nature of the debates in court. It is called the "open court principle".

There is a lot of discussion on what that means. It does not mean that the entire content of court proceedings must be available online. It just means that a person can apply to the court to ask for a copy of the proceedings. There is no general definition of what is publicly available, to my knowledge. This is one example that deals with public accessibility.

The Access to Information Act talks a lot about what should or should not be available to the public. There is a lot of case law on the limits of what should be accessible under the Access to Information Act, for example.

Mr. Matthew Dubé: Okay, but the bill, in paragraph 24(1)(a) of part 3 or in subsection 11.24(1) of part 4, refers to publicly available information. Part 3 deals with the CSE and part 4 deals with data collected by CSIS.

Do you consider that publicly accessible information is defined in the bill? Is there a need to define what exactly is understood by "publicly accessible"?

Mr. Peter Edelmann: With publicly accessible information, there are problems with private databases, for which an access fee must be paid. A little earlier, Ms. Szurlej spoke about the fact that a fee has to be paid for access to some databases, particularly abroad. In the United States, for example, huge databases are accessible to the public.

For background checks, you can pay to get access to quite major databases. You can also pay to get into Twitter or Facebook. A little earlier, we were talking about Facebook and Google. They sell their data to the public. Anyone can buy the data. The identity of the purchaser makes no big difference for Google or Facebook.

Perhaps the procedures with data that are not public should be reviewed, to the extent that they are not published. There is also the question of the kinds of data. We are talking about general information, which is public. But the restrictions are on personal information.

In terms of the data that can be obtained, and that are not technically personal data, the differences are quite major. For example, data coming from Statistics Canada, from Google or from Facebook are not personal data in the eyes of the law. However, those data provide a lot of general information.

For example, those data could be used to design a deep learning algorithm or a neural network so that it can learn to determine people's sexual orientation or religion. However, at the end of the day, the algorithm contains no personal data. If you buy the algorithm, or access to it, are you buying personal data? Those are issues that have to be dealt with.

It is a very good thing to want to update the legislation in terms of databases and of current technology. However, in criminal law, we always try to use neutral language and present things in a neutral way from a technological perspective.

The legislation should be drafted in a way that can be applied to a "holodeck" or any other technology of the future, so that we do not have to update the legislation once more.

What does that mean for the algorithms and the technology? I am not an expert in the area, I am expert in legislation; but in my opinion, a number of questions need to be asked about what databases, and the various tools used by intelligence services, can represent.

Those are really different questions from those about what is or is not public, or about who can have access to what.

● (1245)

Mr. Matthew Dubé: I have a minute left. You can answer, Ms. Szurlej.

[*English*]

Prof. Christina Szurlej: I'd like to express my concern about the use of algorithms and the impact it can have on democracy.

If we're talking about the collection of information en masse, it means the agency that has access to that information is able to reasonably predict how an individual may vote. If they're undecided, they may determine what factors may push them to vote one way or another. That sort of information can be gained from analyzing these types of algorithms. That's why it's so important to safeguard the privacy of Canadian citizens and ensure the preservation of democracy in Canada.

The Chair: Thank you, Mr. Dubé.

Mr. Fragiskatos, seven minutes please.

Mr. Peter Fragiskatos: Thank you very much, Chair, and thank you all for appearing today.

You're an academic, Ms. Szurlej. Mr. Edelmann and Ms. Carter, you're lawyers, but you are focusing on security issues, so I think it is important to ask you about the nature of the threat environment that Canada faces today. We've heard from a number of witnesses who have testified to what I believe to be a fact, that it's a multi-faceted threat environment, and that as we try to create and craft legislation to confront that threat environment, we should not only be focused on one manifestation of terror, for example, Islamic radicalism, if you want to call it that, or Daesh in particular and groups like it. Witnesses have said we ought to take a wider view and particularly look at the nature of hacking and the cyber element that terrorists are increasingly taking on.

What is your view on this? Where should responsible government be focused from a threat perspective—from a security perspective?

Mr. Peter Edelmann: From a threat and security perspective, it depends on the departments you're talking about and the types of threats that you're.... Is the threat in North Korea, for example, of concern? Those are things that are obviously of concern to Canadians in terms of proliferation of nuclear weapons and things like that. It's within the ambit generally of the CSE, in collaboration with other agencies, that we have these international types of threats that are dealt with. That's where we have different agencies that deal with different aspects of the threat environment.

The CBA recognizes the need for balance in the sense that there are concerns around security, and there are concerns around having an infrastructure that people can be confident in and that Canadians feel they can trust. In particular with respect to domestic threats, it's important that the agencies have the trust of the communities they're working with, whether they're Canadian or non-Canadian communities.

● (1250)

Mr. Peter Fragiskatos: I don't mean to interrupt you, Mr. Edelmann. So you're of the view that, ultimately, at the end of the day—you mentioned North Korea, for example—it's a multi-faceted threat environment that we face.

Ms. Szurlej.

Dr. Christina Szurlej: In short, I would say that if we're talking about the threat of terrorism, you are more likely to slip and die in the shower than you are to be the victim of a terror attack in Canada. Does that mean we need to regulate showers and ensure that there's surveillance in showers?

We certainly need to ensure that there is a balance. The charter protects life, liberty, and security, not life, liberty, or security.

Mr. Peter Fragiskatos: Thank you very much.

In September, the government issued new regulations to Canadian security agencies to the effect that intelligence that may have been obtained through mistreatment or torture should not be used. There is an exception for preventing the loss of life or significant personal injury, but prior to this directive it was the case that such information could be used to secure property, for instance.

Now, these are regulations. Would you advise that the government consider taking those regulations and implementing them in legislation? As you well know, legislation is much more difficult to change.

Mr. Peter Edelmann: Yes. I'll just leave it at that: yes.

Mr. Peter Fragiskatos: Okay, fair enough.

Unless, Ms. Szurlej, you had something, I'll go with a lawyer on that.

Dr. Christina Szurlej: I would just like to express my view that I don't think information obtained via torture should ever be used, because it's not reliable and there are a number of other factors that I don't have time to get into.

Mr. Peter Fragiskatos: Okay. I would push you on that, because I do think when it comes to preventing the loss of life or significant personal injury—

Dr. Christina Szurlej: If it's not reliable, it won't have that effect.

Mr. Peter Fragiskatos: It's a slippery slope; we're going to debate that all day.

Dr. Christina Szurlej: Okay.

Mr. Peter Fragiskatos: Mr. Edelmann, I have a question for you in the time that I have left here. You talked in your opening remarks about your concern regarding legal advice, solicitor-client privilege, and the national security and intelligence review agency. You had a concern on that.

Yes, NSIRA does have the power to compel information from any agency it investigates, including legal advice. However, some commentators have made the observation that this is not unjustified because if that legal advice to the government, let's say, on a security matter, happens to be wrong and could open the door to an infringement of rights, it would be good to review that so we can learn from it. It would serve as a safeguard.

What do you think about that?

Mr. Peter Edelmann: There are two concerns around the issue with respect to privilege. One is with respect to the government documenting and seeking legal advice. The first step is, will the government seek legal advice and should the government get...?

Usually when I give legal advice to a client, my legal advice is not, “This is, this isn't; this is the way it is, and this is the way it isn't.” What legal advice often looks like is, “Here's where you're at no risk whatsoever”, and then there's a spectrum as you start to get closer to the line. How much you want to push coming close to the line is a decision made by the person, and it's often a discussion and dialogue that happens between counsel and the individual getting advice.

I'm not saying it helps people to push the line, but what will happen if these discussions are going to be disclosed is that instead of getting advice with respect to where the line is, either that advice will not be sought at all or it will not be documented. That undermines the whole purpose of the minister, or the person who is making a decision, doing it in an informed way. If the person is going to cross the line, that should be done in an informed way, with access to full, frank legal advice.

In terms of having the protection of the privilege, it allows for those frank discussions to happen. If that privilege is going to be breached or is going to be reviewed by this agency or other agencies in the future and that privilege becomes meaningless, the process of being able to get that advice is no longer going to function. I would submit that it's just as important for private actors to be able to know the law, find out the law, and get a sense of what the law is.

The privilege belongs to the government, not to the lawyer. If the government decides that they did this thing and their lawyers told them to do it, you can disclose that. It's not the lawyers' privilege.

When the CBA comes forward, we're not trying to protect a privilege that belongs to us as lawyers. My clients can disclose my advice whenever they want. It's a privilege that belongs to the client, because the client has a right to speak to me in a frank and fulsome manner, tell me everything they want to know about, and I can explain the law to them so they can make decisions.

● (1255)

The Chair: Thank you, Mr. Fragiskatos.

Mr. Peter Edelmann: Sorry. That was a lengthy answer.

The Chair: We were having a Law 101 lesson there.

Mr. Peter Edelmann: I apologize.

The Chair: Mr. Motz, you have the last three or four minutes, please.

Mr. Glen Motz: Is it three or four minutes?

The Chair: Well, it depends on how quickly you speak.

Mr. Glen Motz: Thank you.

I have a couple of questions.

Ms. Szurlej, I would hope that you're not asking the Liberals to regulate showers.

Dr. Christina Szurlej: I'm certainly not. That was a joke.

Mr. Glen Motz: If you do, they just might consider it, so let's not go down there.

The Chair: You have two minutes now.

Mr. Glen Motz: Sorry, I couldn't help myself.

Mr. Edelmann, I want to ask you questions given your background. If you were to add something to Bill C-59 that you think is absolutely critical for public safety, balancing the need for rights and privacy, what would you suggest that be?

Mr. Peter Edelmann: We have 30 recommendations in our written submissions.

In terms of public safety itself—

Mr. Glen Motz: Can you respond in 30 seconds or less?

Mr. Peter Edelmann: I'll be very quick. In terms of the public safety mandate or aspect, I would say that the mandate of the NSIRA is something that ought to be clarified. Some of the things I talked about at the beginning, regarding the lack of clarity with respect to the definitions around national security, actually do undermine the overall functioning of the infrastructure. Therefore, in terms of the broad picture, the one thing that I would fix is to make sure that you get the forest right. I have a whole bunch of recommendations around trees. That would be my recommendation around the forest.

Mr. Glen Motz: Thank you very much.

For my last comment, I can't help but suggest, Ms. Szurlej, that regarding your analogy to the shower, your shower has never threatened to blow you up because you live in a democracy. The whole issue of national security, the whole issue of terrorism, and the risk that we have in this country is serious. Obviously, as a committee, that's something that we are taking very seriously, so I appreciate the comments that all of you had to make.

Mr. Fragiskatos asked the question about all of your assessments, in regard to the risk of terrorism globally. Please respond with yes or no. Have you had any training or operational experience on risk assessments of terrorism?

Mr. Peter Edelmann: Other than in my work in national security cases, no, I do not have training in risk assessment.

Mr. Glen Motz: Or experience.

Mr. Peter Edelmann: I recognize that there are multi-faceted risks from a number of different places.

Mr. Glen Motz: Thank you.

The Chair: Thank you very much.

On behalf of the committee, I want to thank each of you for your efforts to come here and share your insights with us, as we study this very important bill. With that, I'm going to adjourn, but I will remind those who are on the subcommittee that we are meeting immediately after and it is in camera. I would ask for co-operation in emptying the room from those who are not entitled to be here.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: http://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : http://www.noscommunes.ca