HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 037 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Friday, October 21, 2016

Chair

Mr. Robert Oliphant

Standing Committee on Public Safety and National Security

Friday, October 21, 2016

● (1405)

[*English*]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib.)): Good afternoon. I'm happy to call to order this 37th meeting of the Standing Committee on Public Safety and National Security in the 42nd Parliament. We are continuing our study of the national security framework.

In order that our guests and the public know, this is the first of two meetings today. At this meeting we have invited witnesses the committee would like to hear from, and they bring their expertise. In the evening, from 5:30 p.m. to 7:30 p.m., the public comes, again with expertise. Their expertise may be different from that of the so-called experts, but the committee equally wants to hear from them.

These are meetings numbers 9 and 10 of this week. We began in Vancouver on Monday, where we had two meetings. Then we went to Calgary, Toronto, and Montreal, and now we are in Halifax. This is fairly early in our study of the national security framework.

There are two consultations going on simultaneously.

The government is having a consultation. It has issued a green paper to the Minister of Public Safety and Emergency Preparedness. That green paper consultation is going on at a government and departmental level.

The parliamentary committee is doing its own study. We are obviously aware of the green paper, and it helps us frame our study, but we are not limited to that, nor are we from government. Even though some of us are from the government side of the House, others are from the opposition side.

I will simply have the members introduce themselves, starting at my far left, so you know who you are speaking to.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): I am Matthew Dubé, member of Parliament for Beloeil—Chambly in Quebec.

Ms. Dianne L. Watts (South Surrey—White Rock, CPC): I am Dianne L. Watts, from South Surrey—White Rock in British Columbia.

Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC): I'm Larry Miller, member for the riding of Bruce—Grey—Owen Sound in southwestern Ontario.

The Chair: I am Robert Oliphant, chair of the committee and member of Parliament for Don Valley West in midtown Toronto.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): I am Pam Damoff, MP for Oakville North—Burlington.

The Chair: We have one other member who will be joining us. He's apparently stuck in traffic. He is Colin Fraser, who is a substitute for Marco Mendicino, who is away today. Colin will be here shortly.

We have two witnesses today, who will each be given 10 minutes. We will begin with Michael and then continue with Christina. At the end of that 20 minutes, we go through questioning. Questions can go to either of you as we continue.

Please go ahead.

Mr. Michael Karanicolas (Senior Legal Officer, Centre for Law and Democracy): Thanks so much to the committee for the invitation.

I'm here as a representative of the Centre for Law and Democracy, which is an NGO based in Halifax that works to promote foundational rights for democracy. Our particular emphasis is on freedom of expression, so I'm planning on providing commentary from that perspective.

I'll say at the outset that I support the recommendations of Craig Forcese and Kent Roach regarding improving oversight of the system, as well as regarding sharing evidence. I also share the concerns of the Privacy Commissioner regarding the expanded scope of information sharing.

First, regarding the offence on advocating or promoting the commission of terrorism offences, it is well established under international law that there is an important difference between mere advocacy or promotion of something regardless of its harmfulness, and incitement to a harmful result. International human rights standards require a very close nexus between a statement and the risk of harm before the former may be legitimately prohibited. This standard ensures an appropriate balance between protecting free speech and protecting against harm.

An academic work, for example, may be said to advocate in favour of something by extolling its virtues and by setting out and weighing its relative benefits and drawbacks, and yet it would be rare for an academic work to actually incite others to harmful results.

The media, which have a professional obligation to report in a timely and comprehensive manner on acts of terrorism, could be deemed by some to be promoting terrorism offences by doing so. The use by Daesh of social media to promote itself simply by distributing videos and images has been widely commented on. This provision could potentially be applied to media reporting on their activities. Similarly, a very strongly worded poem may advocate for something, and yet it would be rare for it to create a genuine risk of harm.

There is clear authority under international law for the need to maintain, at least in relation to restrictions on freedom of expression, a clear distinction between expression which incites, and expression which merely advocates, promotes, or praises. I cite in particular article 20.2 of the International Covenant on Civil and Political Rights, which calls for the prohibition of advocacy of national, racial, or religious hatred, but only where it "constitutes incitement".

Article III(c) of the Convention on the Prevention and Punishment of the Crime of Genocide uses similar language. I cite the 2015 Joint Declaration on Freedom of Expression and responses to conflict situations by the special mandates on freedom of expression from the United Nations, the Organization for Security and Co-operation in Europe, the Organization of American States, and the African Commission on Human and Peoples' Rights.

There are also problems with the recklessness standard in the offence, which should be of particular concern to the media. The media would presumably rarely, if ever, report on terrorism with the intention of promoting it, but they might be deemed to have been reckless as to this possible result. We recommend that this provision be deleted, as it is unnecessary in light of existing anti-terror provisions in the Criminal Code and overbroad in its impact on freedom of expression.

Sections 83.222 and 83.223, which provide for the seizure and suppression of "terrorist propaganda" are also problematic insofar as they apply a substantially similar definition of what constitutes terrorist propaganda. Although seizing material is not as serious an infringement as arresting its author, the potential overbreadth of the restriction is of concern either way. Moreover, the standard for acting —that of there being reasonable grounds to believe it's terrorist propaganda—is a troublingly low threshold to cross. For a media outlet, having its material seized or suppressed for seven days and the requirement of going to court to obtain its release could lead to significant operational challenges, with the concomitant possibility of a chilling effect around legitimate speech.

We also note that unlike the 83.221(1) offence, which incorporates the protection of a *mens rea* requirement, there are no conditions or protections against abuse of the reasonable grounds standard. Given that this is analogous to an urgent action or interim measure, it should be incumbent on the legislator to include protective measures. These might, for example, require a clear risk of imminent dissemination of the material to be shown, along with a similar risk of incitement to an actual terrorism offence. In other words, this sort of measure should at the very least be treated as exceptional, and appropriate protections against abuse should be built into it.

Regarding investigative technology in the digital world, it's a bit troubling that the green paper treats the Spencer decision as a problem to be solved or circumvented rather than a definitive statement by the country's highest court to the effect that there is a significant privacy interest in Canadians' metadata. We agree with the Spencer decision, but the bottom line is that it is the law of the land and should be respected.

● (1410)

What is far more troubling is that the green paper appears to be opening the door to far more intrusive and problematic policies, such as requirements for intermediaries to retain the technical ability to decrypt information sent by their users. This should be a huge red flag to any Canadian who cares about digital security.

For years, authorities in the United States and elsewhere have sought a solution whereby official access could be enabled without compromising security. The technical community has been and remains unanimous in their position that this is not possible. It is impossible to build a back door that only the good guys can walk through.

Even if it were possible to limit access to state requests that followed a proper procedure, it is worth noting that we live in a world where many governments do not share Canada's lofty ideals. What would be the impact on global human rights if the governments of China, Russia, Egypt, and Saudi Arabia demanded a similar deal? If such a solution were to be developed, it would be impossible to keep it out of the hands of the world's repressive governments. Strong encryption keeps everyone safe.

The other highly problematic new proposal that the green paper contains deals with data retention requirements. Data minimization, whereby organizations seek to limit materials stored to what is strictly necessary, is a cardinal principle of modern digital security. Overstorage is one of the main reasons that the Ashley Madison hack and last year's hack of the United States Office of Personnel Management were so catastrophic.

The green paper mentions data retention requirements in Australia. It does not mention that in the run-up to their adoption, Anonymous hacked the databases of one of the country's largest ISPs as a demonstration of why the requirement is a bad idea.

The green paper also fails to mention significant resistance at the national level to the data retention directive in Europe even before it was struck down, including having been rejected by courts in Germany, Romania, and the Czech Republic. Sweden, among others, also flatly refused to implement the directive.

Although the online world certainly presents novel challenges to law enforcement, it is worth noting that the tool kit available to police today is vastly more powerful than their investigative tool kit 20 or 30 years ago. The idea of developing a digital trail that can be tracked back for weeks or months is only a novel challenge because police never had the ability to do anything comparable in the past. If a suspect came on the police's radar in 1993, there was no way for them to go back to track their movements and communications from 1992.

From this perspective, painting the modern digital landscape as an environment where law enforcement is increasingly powerless does not comport with reality. With modern data processing, the centralization of communications due to the spread of the Internet, and the proliferating digital trail that it leaves, law enforcement investigative techniques are more powerful, effective, and efficient then ever before, even if they are not as powerful as someone in law enforcement would like them to be.

The Chair: Thank you very much.

Go ahead, Ms. Szurlej.

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

At this point, I would like to commend the Liberal government for launching a public consultation to inform legal, policy, regulatory, and program-based changes to the national security framework. My testimony before the standing committee centres on the additional authority for domestic national security information sharing as established under the Security of Canada Information Sharing Act, hereinafter the SCISA, and its impact on the right to privacy under domestic and international human rights law.

Indeed, the most vital function of government is to ensure peace and security by protecting its populace and citizens abroad.

> States are faced with the challenge of protecting human rights and fundamental freedoms while suppressing small groups of interconnected non-state terrorists who operate in detached networks and have the capacity to commit massive atrocities with minimal resources. These elusive factors amplify the risk posed to the state and members of the public by masking efforts to identify networks of individuals who are involved in or associated with terrorism, detect potential terrorist threats, and prevent terrorism from occurring.

This, however, does not negate the state's duty to respect, protect, and fulfil its domestic and international human rights obligations. Under the Canadian Charter of Rights and Freedoms, Canada's populace is guaranteed the “right to life, liberty and security of the person”, not life and security on the one hand and liberty on the other. These protections are interdependent and non-hierarchal.

Let us consider guidance from the International Commission of Jurists, urging states to:

> adhere strictly to the rule of law, including the core principles of criminal and international law, and the specific standards and obligations of international human rights law, refugee law and, where applicable, international humanitarian law. These principles, standards, and obligations define the boundaries of permissible and legitimate state action against terrorism. The odious nature of terrorist acts cannot serve as a basis or pretext for states to disregard their international obligations, in particular, in the protection of fundamental human rights.

● (1415)

The Chair: Could I ask you to go another inch back from your mike, just for the interpreters' ears?

Ms. Christina Szurlej: I apologize.

The right to privacy is protected under article 17 of the International Covenant on Civil and Political Rights, to which Canada is a state party. Though there is no equivalent protection found under the Canadian Charter of Rights and Freedoms, the right to privacy is an enabling right to the fundamental freedoms set out under section 2, namely the “freedom of thought, belief, opinion and expression” and “freedom of association”. Privacy is likewise an enabling right for freedom of information and the “free unhindered development of one's personality”.

To exchange human rights, freedoms, liberties, and democratic safeguards for national security is not justifiable. “No law, no matter how well-crafted or comprehensive, can prevent all terrorist acts from occurring.” As such, the public must be mindful that the blind relinquishment of its civil liberties may not protect them from threats to national security.

A balanced approach is needed to ensure adequate measures are in place to prevent and address any such threats while protecting the fundamental human rights and freedoms of its populace. “When States fail to strike a balance between human rights and security in the context of countering terrorism, they risk impeding the very rights they purport to protect”, for what is national security without human security and what is human security without human rights?

According to the Special Rapporteur on the right to privacy, Professor Joe Cannataci, in limiting one's right to privacy in the name of national security, several factors must be considered, including the adequacy of oversight mechanisms, the distinction between targeted surveillance and mass surveillance, the proportionality of such measures in a democratic society, and the cost-effectiveness and the overall efficacy of such measures.

Introducing sweeping changes to the way in which personal data is shared among government agencies in Canada should be coupled with a commensurate review mechanism for ensuring the information shared is accurate, is done so within the limits prescribed by law, and is done so with minimal impairment to the rights and freedoms set out under the charter.

Distinguishing between targeted and mass surveillance is essential to preventing the net from being cast too wide and encasing innocent civilians undeserving of the erosion of their civil liberties. Failing to do so assumes in a sense that all are guilty until proven innocent, perverting a fundamental and long-standing principle of justice.

In terms of proportionality, there should be minimal impairment to the rights affected and the solution must not be worse than the problem. Has this test been met by the SCISA, wherein personal data can be shared across government agencies without any guarantee as to the accuracy of the information shared or express restrictions regarding the sharing of information with private actors and foreign governments? Much like a child's game of telephone, the original content of a message risks becoming distorted, potentially having significant consequences for the individual concerned.

In his first report to the Human Rights Council, Special Rapporteur Joe Cannataci expressed concern that:

> the ordinary citizen may often get caught in the cross-fire [of mass surveillance] and his or her personal data and on-line activities may end up being monitored in the name of national security in a way which is unnecessary, disproportionate and excessive.

The final point regarding cost-effectiveness is not one on which I can comment as an expert, though from a common sense point of view, concentrating resources where they are most needed—i.e., on targeted surveillance—limits the risk of overlooking a potential threat due to an information overload. In other words, we must ask ourselves what utility is served by mass surveillance? Does it result in greater protection for national security, or does an information overload spread resources so thin that it renders government efforts less effective in responding to potential threats?

● (1420)

As mentioned, Canada has international obligations to respect the right to privacy under the International Covenant on Civil and Political Rights. A corresponding treaty body, the Human Rights Committee, monitors the compliance of state parties with provisions within the covenant. In its concluding observations to Canada's periodic report, the Human Rights Committee expressed concerns that:

> ...Bill C-51's amendments to the Canadian Security Intelligence Act confer a broad mandate and powers on the Canadian Security Intelligence Service to act domestically and abroad, thus potentially resulting in mass surveillance and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards...including under the Security of Canada Information Sharing Act, an increased sharing of information among federal government agencies on the basis of a very broad definition of activities that undermine the security of Canada, which does not fully prevent that inaccurate or irrelevant information is shared....

In its general comment number 16, the committee has also clarified that:

> Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.

Before Bill C-51 was passed, the improper sharing of information by the Government of Canada led to serious human rights abuses against Canadian citizens, including Almalki, El-Maati, Nureddin, and Arar.

The SCISA develops further authority for the government to share personal data without developing corresponding legal safeguards to prevent the repetition of similar gross injustices.

Now that we have identified some of the inconsistencies between the SCISA and Canada's international human rights obligations, let us look to potential solutions.

● (1425)

The Chair: You have about one minute.

Ms. Christina Szurlej: I'll read very quickly.

Number one, clearly define the scope of activities that constitute a “security threat to Canada” under section 2 of the SCISA, as well as “advocacy, protest, dissent and artistic expression”, which are excluded from the scope of the act.

Two, strike out provisions within the act permitting inter-agency information sharing to prevent losing control over sensitive information potentially harmful to Canada's national security. If disclosing information sensitive to national security can be so harmful as to warrant the limitation of fair trial rights within the existing framework—i.e., non-disclosure of classified information to the defence in a criminal case—how is this risk mitigated by inter-agency information sharing among heads of agencies who are neither experts in the right to privacy nor experts in national security?

Three, establish an office of the national security adviser “to review all national security activity, and to ensure effective information sharing” from government agencies to CSIS and the RCMP.

Four, amend the Privacy Act to compel heads of agencies to share all information that will adversely impact Canada's national security with the Canadian service intelligence agency via the office of the national security adviser. It is problematic that discretion rests with the heads of agencies as to whether to disclose information regarding “activities that undermine the security of Canada”, as they are not traditionally experts in the field.

Five, introduce regulations to track what type of information has been shared, by whom, and for what purpose, via the office of the national security adviser.

Six, follow up on cases where an individual has been cleared and ensure all relevant government agencies and other entities with which information has been shared are aware of this.

Seven, set out clear access to a remedy where information shared has resulted in adverse consequences for innocent individuals or disproportionate consequences for guilty persons.

Eight, more intrusive information sharing should require authorization through the issuance of a judicial warrant.

If the SCISA continues to allow inter-agency information sharing regarding the activities set out under section 2, I likewise recommend that it ensure that revisions to schedule 3 adding or deleting a Government of Canada institution are accompanied by a clear justification, including an explanation of how the agency's duties directly relate to national security.

I wish to end with this final point: "...respect for human rights legal obligations is a prerequisite for effective security", not a hindrance. Canadian domestic legislation should reflect this by striking an appropriate balance between the right to privacy and the protection of national security.

Thank you.

The Chair: Thank you very much.

We begin our rounds of questioning with Ms. Damoff, for seven minutes.

Ms. Pam Damoff: Thank you very much.

Thank you both for being here and testifying before us.

I want to talk about cybersecurity and technology that you were talking about. It has come up a few times. Metadata has come up during our testimony. When the RCMP and CSIS testified, they described it as the information on the back of an envelope. Other witnesses have said it's much more than that.

I'm wondering if you can explain this to us. No one wants to hinder the police or the RCMP or anyone from getting information needed for an investigation, but by the same token you have a certain expectation of privacy.

Under the Spencer decision, how do the police go about getting information, and what are they allowed to obtain on your cybercommunications or electronic communications?

Mr. Michael Karanicolas: First, it's worth noting that metadata can be defined in many different ways. Depending on how it's defined or how it's framed in the legislation, there are different levels to which it can be somewhat invasive or highly invasive. If you consider metadata to include, for example, a list of the websites that you visited, then even if you're not getting the content of the communications through a particular website, the fact that you go to a website can reveal a huge amount of deeply personal information.

In terms of our recommendations, depending on the definition—it does depend on the definition—metadata can be an incredibly invasive insight into a person's life.

● (1430)

Ms. Pam Damoff: Do you think our legislation should have a definition of what is allowed to be obtained during a search, or is that becoming too specific?

Mr. Michael Karanicolas: You do get a challenge because of the general rule that laws should be written in as technologically neutral a fashion as possible to prevent them from having to be revised or revisited every year or two.

The way that technology changes does lead to challenges. In terms of a good formula, criminal procedure is not my specialization, but I will endorse the lawful access provisions that David Fraser has put forward as a way of providing for proper procedure for obtaining warrants to access subscriber information.

Ms. Pam Damoff: On encryption, we also had another witness. The chair said we need to stop thinking about encryption in World War II terms, where you encrypted code and that allowed you access to state secrets. Now it's much different. He described how it was more dangerous to allow encryption then than the way it is now, because, as you said, you don't know who is getting in the back door.

Encryption is also a real challenge for law enforcement. Is there a middle ground on it, or is it either you live with it and you work around it or you allow certain access to it?

Mr. Michael Karanicolas: It certainly is a challenge. Whether or not there's a middle ground generally is a technical question. Again, my background is in law and human rights. All that I can do is look to what the technical community has said.

For years, governments have been saying—and the U.S. government has been prominent in this—that we need to find a way whereby the government can obtain a warrant to access encrypted communication that won't undermine the general security of the information.

Time and time again this has been suggested, and time and time again the people who work on this have said it is not possible. Any illicit means of access, any additional means of access, provides an additional weak point that increases the vulnerability of the system.

Ms. Pam Damoff: Okay. If you don't have any information on this, it's fine, but no one has talked about the financing aspect. I'm just wondering if either of you has any expertise on that aspect to comment on terrorist financing, which is in the green paper. Does either of you have any comment on that?

Mr. Michael Karanicolas: No, sorry.

Ms. Pam Damoff: That's fine.

When we were talking about promoting terrorism, do you believe the existing offences that pertain to hate propaganda are sufficient? Also, are any other countries using the same language that we use in regard to promoting terrorism? You're not the first ones who've talked about the issues with journalists. I had an email from people in my riding who have the same concerns.

Mr. Michael Karanicolas: There are many countries that have laws against promoting terrorism, including Russia and Egypt. They generally come from the areas of the world that I wouldn't want to see Canada trying to emulate.

What I can say is that the key in terms of international human rights standards is to find that nexus where you're outlawing speech that has a direct cause-and-effect relationship with the harm, whether it's terrorism, whether it's racial hatred. That is black-letter international human rights law.

Whenever you move beyond that and talk to the broader area of something that might potentially and directly be used by somebody to carry out a terrorist offence or inspire someone to do so, it takes you into very grey territory. Generally speaking, human rights standards are very clear about requiring that nexus between the cause and the effect.

Ms. Pam Damoff: Thank you.

This is to both of you, and I only have about a minute left.

When we talk about the definition of terrorism, we tend to think of one subset of terrorist and terrorism, yet we've had testimony that talked about it being an arc that includes pandemics and climate change and a number of different things under that broad umbrella. Does either of you use a definition of terrorism when you're doing your work?

You spoke to it, so perhaps you could....

Ms. Christina Szurlej: All I would like to say on that point is that there is no internationally uniform definition of terrorism. That is problematic, because if we are introducing such significant limitations on fundamental human rights and freedoms and we don't even know what the definition of terrorism is, or we don't agree on it, it's problematic on a domestic level and also when we're co-operating with other states in terms of information sharing and investigating suspected terrorists.

● (1435)

Ms. Pam Damoff: Thank you. I think that's my time.

The Chair: Very good.

Go ahead, Ms. Watts.

Ms. Dianne L. Watts: Thank you very much, Mr. Chairman.

I just want to say thank you for being here and giving us your presentation.

I did have a question, and correct me if I heard this wrong. I can't pronounce your last name, so I'll call you Michael.

When we talked about the national security framework and the measures that would encompass, you said that in terms of intelligence gathering, there should be an imminent threat or imminent incitement.

Mr. Michael Karanicolas: I'm sorry; did you say "around intelligence gathering"?

Ms. Dianne L. Watts: Yes. It was that when we look at surveillance and gathering intelligence, the only time we should be doing that is if there is an imminent threat.

Mr. Michael Karanicolas: I think I said that in relation to the inciting terrorist propaganda or inciting terrorism provisions, not in terms of all intelligence gathering.

Ms. Dianne L. Watts: Okay, so you're just relating to propaganda, dissemination of—

Mr. Michael Karanicolas: It's speech offences, yes.

Ms. Dianne L. Watts: I needed clarification for that. I was a little taken aback.

Mr. Michael Karanicolas: No, I wouldn't say that intelligence should begin when there's an imminent threat.

Ms. Dianne L. Watts: Exactly. As we know, it takes a long time to undertake the planning of certain things. Also—and I think Ms. Damoff also mentioned this in terms of encryption and government trying to find a way to work through the encryption process—I would say that we've heard over and over again that it is not possible. I think we've seen the practices of Russia and China and North Korea and others around the world. We've seen that if there's a weak point, they're going to get in, so it's not just about giving one person that information.

In terms of the safety of the general public—and it comes back to information gathering—Christina, you mentioned there should be a judicial warrant for information gathering.

Ms. Christina Szurlej: Only when it's particularly intrusive.

Ms. Dianne L. Watts: Define "particularly intrusive".

Ms. Christina Szurlej: Well, that's if it goes beyond the scope of collecting metadata and there isn't a clear rationale for why the data is being collected, as in the likelihood that the individual is actually a terrorist or will commit a terrorist offence being very low, and when it would extend to an average citizen.

Ms. Dianne L. Watts: I think that when we look at the broader picture—and I just mentioned some of the practices of other countries, such as hacking into systems and selling or trading information—that is problematic. I would suggest that these countries have a lot of information on us already through those practices, and I think we certainly need to do something to address that issue.

I will ask this question to both of you. How would you square this? When we have to deal with the intelligence world and the information they're sharing, we're trying to restrict our end of things. There have to be some protections for our citizens as well on the global front. What are your thoughts about that?

● (1440)

Mr. Michael Karanicolas: I'm a bit confused, but I think you're asking how our intelligence agencies can compete with Russia and China.

Ms. Dianne L. Watts: I mean in terms of protecting. They're so far advanced in their capabilities, and there are virtually no laws regarding what they can gather.

Mr. Michael Karanicolas: You're talking about offensive operations against different states, which I don't think is necessarily what we're talking about here. It certainly wasn't what I was talking about. I think that's a different question.

Ms. Dianne L. Watts: I understand that, but I'm just throwing this question at you.

Mr. Michael Karanicolas: You're asking about foreign states using these techniques to attack Canadians?

Ms. Dianne L. Watts: Yes.

Mr. Michael Karanicolas: This is an argument for better security. That's what I'm hearing. This is an argument for why strong encryption is important in order to put up the strongest defence possible.

In terms of whether or not we should take a more intrusive stance against our people because Russia and China are going to take an aggressive stance against us—

Ms. Dianne L. Watts: No, that's not what I'm saying. I'm talking about looking at different intelligence agencies outside of our country, as opposed to the domestic ones, with regard to how they're operating and how we would protect our citizens from that intrusion.

Mr. Michael Karanicolas: Sure, and this is not just against citizens on an individual level. It's about structural networks. It's about data minimization at the federal level so that the government does not act as a giant warehouse of information that there's no necessity for it to keep, because when you make yourself a big target like that and a breach eventually occurs, it is much more damaging. For that reason, we need data minimization, strong encryption, and strong security protocols.

Again, to bring it back to the debate about the green paper, data retention protocols and weakening encryption move us in the wrong direction from that perspective.

Ms. Dianne L. Watts: Right. I agree with that.

Ms. Christina Szurlej: That also raises the issue of losing control over what other states do with the information that we share with them, as we saw in the Arar case.

Yes, we're maintaining a strong partnership with the United States in doing so, but we also risk having that information misused once an individual has been cleared, and having no control over other states taking the same approach and accepting the clearance we've put forward.

The Chair: Thank you very much.

Monsieur Dubé is next.

[*Translation*]

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

[*English*]

Thanks very much for being here.

The first question I want to ask has two parts.

My feeling is that when we give such expansive, unprecedented powers to national security agencies, there has to be a need. First, do you believe that they need to demonstrate that need and that the burden of proof is on them? Second, has CSIS, among others, done that, in your view? The question is to both of you.

Mr. Michael Karanicolas: This brings us a little to what we were talking about with encryption before. In terms of the need, one of the things that is important to remember is that encrypted information is only useful if it's in an unencrypted form. When information is in that encrypted form, it's inaccessible to law enforcement, but it's also useless to its user. Everybody has to unencrypt the information at some point.

We've seen law enforcement in the U.S. target the information when it's in that unencrypted space, as opposed to trying to crack the encryption. I guess that's a little bit roundabout, because you were speaking about police powers generally, but as to whether or not that need has been specifically demonstrated, again, I stand by the idea that intelligence agencies have a bigger tool kit than they ever had before. I think the Internet has vastly expanded their capability to monitor what people are doing, and I think the capabilities of targets have been enhanced as well, but not at the same rate.

I think our intelligence agencies are more powerful than they were 10 to 30 years ago, and I don't necessarily know that the need has advanced beyond that.

● (1445)

Ms. Christina Szurlej: I was wondering if you could be a little more specific about part one of your question.

Mr. Matthew Dubé: Some would argue that when you propose giving such unprecedented powers to these agencies, the burden of proof is on them to show that they need it and that it's not just happening in a vacuum.

In other words, does CSIS need to demonstrate that it actually needs these broad, expansive powers before our government puts them place?

Ms. Christina Szurlej: The short answer is yes, absolutely. The government needs to demonstrate that any action taken is reasonable and proportionate, particularly when it results in an infringement on charter rights. It must also demonstrate that the impact of more intrusive measures will result in a higher level of security.

Mr. Matthew Dubé: Thank you.

My other question is again for both of you.

We're talking a lot about information sharing, and both of you mentioned information sharing with foreign entities. The Arar case is one of the most infamous ones, we should say, and tragic ones, but now we're seeing CSIS having information-sharing agreements with Global Affairs regarding, for example, Canadians who are detained abroad. It's important to specify that information for consular services is being shared with CSIS.

How concerned are you, since Canadians don't benefit from the same legal protections in other jurisdictions? Even in the United States, despite its being an ally, there's very little to no legal protection for Canadians' rights, including their right to privacy.

Ms. Christina Szurlej: One point I'd like to make is that there is another reason that information sharing, even with our close allies, is very problematic. My view is that these allies are not accountable to our voters, unlike our politicians here, who represent the best interests of Canadians. That is one issue.

Second, I do believe that any increase in government powers to investigate and act needs to have commensurate legal protections in place. These protections include review bodies, as well as mechanisms where individuals who are either innocent or who have faced disproportionate consequences can seek a remedy, as is required under international human rights law.

Mr. Michael Karanicolas: I'll just briefly add to that.

Yes, I completely agree with the statement about the privacy aspect. There's a global trend of countries tending to offer some privacy protection to just their own people. The U.S. is a really obvious example. There are some privacy protections that it offers to its people, and it offers virtually none to foreigners. This is particularly troubling when you think about intelligence-sharing arrangements. If Canada can spy on the British and on Americans, and the U.S. can spy on the British and on Canadians, and the U.K. can spy on Canadians and on Americans, and everybody's sharing information, then these sort of protections don't necessarily kick in. It kind of becomes a free-for-all.

There is one more thing I'll mention very briefly, because it's not my particular area of expertise. I referenced Roach and Forcese earlier in this meeting. I want to mention what they said about the problem of silent oversight, particularly when you have a large degree of inter-agency co-operation. If a particular oversight body is only looking at its agency and not potentially seeing the broader picture of what's going on, that can present a challenge.

Mr. Matthew Dubé: That was one of Justice O'Connor's recommendations for the integration of oversight.

As one last quick question, you spoke about the definitions of "promoting terrorism" and how broad in scope and vague some of these aspects of Bill C-51 are, since it has become law.

One point that has been raised is how increasing the criminalization of different aspects and lowering thresholds can become a challenge for counter-radicalization. People who might want to raise a red flag and intervene with a youth who is becoming radicalized in any form of political ideology, and not anything specific, might not want to do that for fear of criminalization, given how open these definitions now are. Is that something you would agree with? Perhaps you could expand on that in the short time we have left.

Mr. Michael Karanicolas: Yes, certainly.

One of Daesh's main sales pitches is this idea that Muslims are under siege in North America and in the west, and that Muslims are being attacked. The increasing breadth of these laws and their inevitable application to groups that are marginalized groups is very troubling from that perspective, I would say.

● (1450)

The Chair: Thank you.

This gives me a chance to welcome Colin Fraser, MP for West Nova. He unfortunately was delayed, and because he didn't get to hear your presentations, I'm going to take over the questioning, and Mr. Miller is going to assume the chair.

Mr. Colin Fraser (West Nova, Lib.): Thank you.

I'm sorry for being late. I'm very embarrassed, but it's nice to be with you.

The Vice-Chair (Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC)): Mr. Oliphant, your seven minutes starts now.

Mr. Robert Oliphant: I'm rusty at this. It's kind of fun.

Thank you for your work, and because Mr. Karanicolas is here, I want to spend a bit of time on the digital world stuff.

We're trying to scope out our big study on the national security framework, and one section is security in the digital age. We're not even sure what questions we should be asking, and I'm not sure. The green paper outlines four areas: basic subscriber information, interception and the requirement of service providers to allow that, encryption, and storage retention.

We've heard testimony on some of this. You haven't talked about basic subscriber information, or BSI. I'd be happy to have you comment on that, and also to have your comments on helping us frame our discussion.

Your work has been largely on access to information and making sure the public can get what the government has, and not as much on the government getting our stuff. Have you any comments on what we should be asking ourselves, or what questions we need to ask?

Mr. Michael Karanicolas: You're absolutely right that a lot of our advocacy—and I'll mention this at the outset—has been on access to information within Canada. That's been our focus, but as an organization, CLD works on foundational rights for democracy. We do quite a lot of work on freedom of expression, and digital security has been part of that. Privacy is increasingly part of that, as well, and yesterday I was at the parliamentary committee on the Privacy Act reform in order to talk about that issue. It does tie into this when you talk about things like data minimization and carrying out privacy impact assessments as part of standard government operations, and a requirement that government agencies should only collect and store information if there is a necessity that you can point to for doing that.

I'm not sure about commenting more broadly about what we should be thinking about with regard to how to frame the discussion about digital security.

Mr. Robert Oliphant: Encryption would be one of the strong concerns, in that anything reducing encryption heightens our security problems, as opposed to solving our security issues. That's the trade-off we've heard from you.

Mr. Michael Karanicolas: Yes, absolutely. My expertise is in law rather than the technical side, but that is what you'll hear from the tech people.

Mr. Robert Oliphant: Please comment on the basic subscriber information and how we work around problems of cyberbullying, child pornography, trafficking, or those kinds of things, and how you get the right to basic subscriber information or the right for interception.

Mr. Michael Karanicolas: The cyberbullying question is an interesting one. It's an area in which we've been engaged here in Nova Scotia. As I'm sure you are aware, we had the Cyber-safety Act here, and then that was struck down, and now they're considering different solutions.

Generally speaking, the problem we had with the cyberbullying law is that it was too broadly defined. It's a similar problem to what you find here. It's a cardinal principle of freedom of expression that any restrictions on speech need to be as carefully defined as possible, first of all to avoid any potential chilling effect, so that people have a clear idea of what they can do, but more than that, to ensure that they are catered to the necessity of the restriction. It's a cardinal principle, and it is in Canadian constitutional law, as well as internationally, that restrictions need to be carefully tailored so that they don't infringe on the right more than is necessary.

Mr. Robert Oliphant: How is my time?

The Vice-Chair (Mr. Larry Miller): You have a little less than three minutes.

Mr. Robert Oliphant: I want to go broadly for a second to both of you, and after that I'll have more narrow questioning.

We are now in meeting number nine of this tour. Human rights groups, civil rights groups, and legal groups have been pretty clear and unified in their concern about the overextension in the form of Bill C-51 and our need to rebalance. We get that. Why are you not afraid of terrorists?

● (1455)

Mr. Michael Karanicolas: I work in Pakistan and Afghanistan, so I spend a lot of my time in countries where the terrorist threat is considerably higher than it is here. I wouldn't say I'm not afraid of terrorists, but having been in countries where there is a stronger threat, I would say that maybe my guard is a little lower when I'm in Canada.

Beyond that, I do think it's important to tailor the restrictions that we put in place to the threat that's there, and I'm not sure that the threat from terrorism today is worse than it was 20 or 30 years ago.

Mr. Robert Oliphant: Based on a threat analysis, really, the threat analysis that you perceive does not warrant an overreach into our rights and freedoms.

Mr. Michael Karanicolas: That's part of the idea of proportionality in human rights law, which says that certain civil rights can be suspended in times of emergency—for example, if we were at war, with tanks rolling in the streets. You see that happening and it's not necessarily illegitimate, but when you suspend something like that for something like the threat of terrorism, which is an indefinite threat that we're going to be facing, then there are real challenges. These suspensions and exceptional circumstances need to be taken in a time-tested manner.

Mr. Robert Oliphant: Without wanting to lead you too much, does the provision under the former Bill C-51 that indicates that it is okay to infringe upon charter rights bother you?

Mr. Michael Karanicolas: Yes, I think that's a problematic provision.

Mr. Robert Oliphant: Do you have any comments?

Ms. Christina Szurlej: I do.

Every day I'm concerned about the protection of my privacy, particularly working in the field of human rights. Never have I woken up in the morning and thought to myself that I hope I don't die in a terrorist attack today.

Mr. Robert Oliphant: Fine.

That's probably my time.

The Vice-Chair (Mr. Larry Miller): You have about 20 seconds.

Mr. Robert Oliphant: I'll yield it to my colleagues. I'm that kind of person.

Ms. Christina Szurlej: May I make a final point about a question that was previously raised regarding security in a digital age?

I think one of the key questions that needs to be raised is on what the role of business is here. In considering that, you may want to take a look at John Ruggie's protect, respect, and remedy framework, and how that would impact.

Mr. Robert Oliphant: Perfect. Thank you.

The Vice-Chair (Mr. Larry Miller): Do you want to take the chair, Mr. Oliphant?

The Chair: I quite miss getting to ask questions.

Go ahead, Mr. Miller.

Mr. Larry Miller: Thank you, Mr. Chair, and thank you to both Christina and Michael for being here.

To your second-last comment, Christina, I don't wake up every morning worried about dying in a terrorist attack either.

To carry on from something you said, Michael, you wondered if the terrorist threat was any worse than it was 20 years ago. I guess my comment would be that in 2006 we had the group of 18 in Toronto; two years ago we had Warrant Officer Vincent killed in the Montreal area and Corporal Cirillo in Ottawa; then just recently, not that far from where I live, a couple of hours to the south, there was a would-be terrorist, so I would say, respectfully, that the threat is probably there.

You were certainly correct that we can't compare it to Afghanistan, or even to some of the recent happenings in Europe—in Paris and what have you—but I think we do live in a different world today. You're nodding your head, so I presume you agree with me there.

Carrying that out, until we started these meetings earlier this week, I hadn't heard the term “metadata”. Of course, “encryption” is a word that we've heard lots of times, but not with the meaning that comes up here.

You made a comment earlier about strong encryption, which sounded like a good thing to a degree. Some of the criticism that comes out of Bill C-51 on some of the securities is about that encryption. Can you explain to me the difference between strong and good encryption, and how we deal with it, and the opposite?

● (1500)

Mr. Michael Karanicolas: I'm not sure that BillC-51 itself deals with encryption, but I can certainly answer that question.

Think of encryption as being like a safe. You can put material into it and you can lock it, or you can open it and have the material accessible. When you talk about strong encryption, you are minimizing the ways in and out of that safe, as opposed to allowing for a different way of access or multiple different combinations. Every change that you make other than that one single way in or out weakens it by necessity.

The reason this is so important is that it's the same encryption standards that are guarding Gmail messages or instant messages that are going back and forth, that are taking care of government's messages, that are taking care of your bank integrity when you're online banking, that are taking care of personal information when you're on the Internet. For that reason, it's very difficult to design a system where.... If you undermine a particular type of encryption, if you undermine the encryption standards that are widely available, that are widely enforced, if you require them to have a back door into them, then that will necessarily weaken the encryption that everybody's using.

Mr. Larry Miller: Are you saying that it's proposed to weaken that encryption?

Mr. Michael Karanicolas: That's an idea that's been floated quite a lot. There's been a lot of discussion about that in the U.S,. and it always comes up against the wall because there's very strong resistence from the technology community, which says this will weaken everybody's security. Generally the government has asked for it a bunch of times and backed down a bunch of times.

Mr. Larry Miller: Okay, so it's being asked for, but it's not actually happening at this point.

Mr. Michael Karanicolas: That's right.

Mr. Larry Miller: Okay.

I'll move back to metadata. That word almost sounds all-encompassing. Can you have metadata and exclude some things that would solve some of the concerns that you too may have?

Mr. Michael Karanicolas: You can restrict it to search for particular information, but it will be difficult to craft a legislative formula forward that allows for warrantless access, I think, in the wake of the Spencer decision.

Mr. Larry Miller: Christina, do you have any comment on that?

Ms. Christina Szurlej: Not on that point, no.

The Chair: That's it from our first round. We're going into the second round now. Thank you for joining us today. It makes the trip to Halifax worthwhile. We'll be coming up with the report, and I'm hopeful you'll see yourselves reflected in it.

We're going to take a brief pause as we say goodbye to these witnesses and welcome our next table.

Thank you.

● (1500)

(Pause)

● (1505)

The Chair: We're going to reconvene.

Thank you to the witnesses who are here for our second panel. I don't think you were in the room when we started, so this is just to put this into context.

We are doing a study on the national security framework of Canada, and that is a large study. It's being done at the same time as the government is doing a study. They've issued a green paper on national security and how we reframe it. Our study is related to that, but not part of it, so we're not here as government. The green paper informs our study, but it does not encompass our study. Our study can be broader. It can be more foundational.

We're already having the first piece of legislation to deal with, and that's Bill C-22, around oversight. We're anticipating more pieces of legislation, and as a result of this study we may be recommending legislative changes to the government. However, we are not doing their consultation. This is our consultation.

The members of the committee have been travelling. As I've said, we've been in Vancouver, Calgary, Toronto, and Montreal this week, and we are delighted to be in Atlantic Canada.

There was some miscommunication, but we'd like to give each panellist would 10 minutes, so I'd like to go to about 4:10 or 4:15, if that's okay with the committee, so that we can have enough time for questioning as well.

Some hon. members: Agreed.

The Chair: Perfect.

I'm going to suggest that we begin with David Fraser for 10 minutes, and then we'll go to Brian and Andrea. Thank you.

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

Thank you very much to this honourable committee for inviting me to provide my thoughts on this very broad consultation that the committee is undertaking, one that has obviously been influenced and affected by the green paper issued by the Department of Public Safety.

Though I have previously appeared before this committee on behalf of the Canadian Bar Association, particularly its national privacy and access law section, I am here today as an individual. I will not be speaking on behalf of my firm, any associations of which I'm a member, or any of my clients.

For some background, I am a lawyer in private practice with the firm McInnes Cooper, based in Atlantic Canada. I'm also a part-time instructor at Dalhousie law school, where I teach Internet and media law, and law and policy for e-commerce. I've also taught privacy law.

As you might be able to guess, my practice is exclusively devoted to privacy law and Internet law. In that capacity, I regularly provide advice to public sector and private sector clients from across Canada, and actually around the world, on their obligations under Canadian laws. That includes companies that are exclusively in the technology sector, the telecommunications sector, and other sectors. This means I'm often providing advice to my clients on interactions with law enforcement and national security agencies in Canada, where the police and national security authorities are seeking access to my client's customer information and information about others of their stakeholders. I have seen many things that inform the testimony I am about to give.

In my personal capacity, I am a strong proponent of a free and democratic Canada that is founded on the rule of law and rooted in our constitutional traditions. I am not associated with any political party, and I feel free to speak my mind on matters such as these from my heart, and hopefully informed by some serious, informed reflection.

I have some mixed feelings about where we are today. The current government campaigned and was elected on a platform that advanced scaling back Bill C-51, the Anti-terrorism Act. I would have hoped we'd be discussing a piece of legislation that would be doing that rather than continuing the long-standing discussion that I expect will extend into the next year.

The information-sharing and disruption powers that the act contains have now become the status quo. We've heard testimony from others, and you've certainly heard it reported in the media, that these powers are being used. We are told they are working, but since we're dealing with the RCMP, CSIS, and CSE, we're not being given any real information about how they are being used. We're being kept in the dark, as usual.

That brings me to my first point. Our national security apparatus in Canada needs effective, accountable oversight. I think Bill C-22 is critical. Our system of government is a parliamentary one, in which Parliament makes the laws that set the limits under which the national security agencies operate. Parliament cannot do this job if it has blinkers on or if it's only given access to unclassified information, and in that case even information that only those agencies deem to be appropriate for Parliament to see. A committee of parliamentarians should have unfettered access to all information it deems relevant to carry out this critical job.

I would, however, suggest that we may need an officer of Parliament to oversee all the national security agencies, something in the model of the Information Commissioner, the Privacy Commissioner, or the Auditor General, who reports to Parliament directly. It may look like a super-SIRC, Security Intelligence Review Committee, that would have oversight over all of the agencies, because the line between CSIS, the RCMP, CSE, and others only depends upon who signs your paycheque, perhaps, or what's written at the top of your paycheque. They collaborate hand in hand. This oversight agency needs to be fully independent of the agencies and has to have unfettered access to everything. It should have the power to report to Parliament on its own initiative and to take any questions before any of the designated justices of the Federal Court on any question about lawful activities.

Our national security agencies by necessity operate largely in the shadows. The only way that we as Canadians can have confidence that they're doing their jobs appropriately is if we have confidence in the organizations that oversee them. I'm not sure we yet have that.

We saw recently a case in which CSIS, with the approval of the Department of Justice, knowingly lied under oath to a Federal Court judge in order to get a warrant. We cannot allow that to happen. We saw a situation in which our federal police department was found to have created terrorists through entrapment. This can't be allowed to happen. Dozens of police officers every year are disciplined for inappropriate and unlawful access to CPIC, the Canadian police database. That shouldn't be allowed to happen. We need to be able to assume the good faith of the individuals who act on our behalf in our police departments and our national security authorities, but it's only through effective oversight and accountability that this can actually be done.

I read with great interest the green paper, and I read with great interest its backgrounder. I could tell who the author was. It was drawn directly from the wish lists of public safety bureaucrats, folks like Commissioner Paulson and the Canadian Association of Chiefs of Police.

● (1510)

It advocates, in a one-sided manner, a whole bunch of police powers that have been debated back and forth over the years and ultimately have been dismissed.

You'll recall that Canadians roundly denounced the lawful-access provisions, the interception capabilities, and other things that were embedded in the Modernization of Investigative Techniques Act that was tabled by Vic Toews and ultimately left to die on the order paper.

I found that the green paper and its backgrounder on advocacy was disguised as consultation, and it's clear that somebody was looking to revive these lawful-access powers, notwithstanding that the Spencer decision was pretty clear about access to basic subscriber information and rights of privacy that individuals enjoy on the Internet. We're still hearing advocates of this sort of thing talking about phone book information—and I'm happy to talk about metadata as well—which was thoroughly debunked by the Supreme Court in that case. The fact that this discussion is taking place in terms that fly in the face of what in fact is the last word on the supreme law of the land from the Spencer decision further reinforces to me that strong oversight is required.

I'm happy to talk about the topic of warrantless access to subscriber information, a topic that I've done a lot of research into, as well as the topic of going dark through encryption.

Ultimately, to allow additional time for questions to make sure that everything the committee wants to hear is heard, we need to be careful that this wish list doesn't come at the expense of our rights. We need to be very cautious, and this committee has a very important job. The threat of terrorism is a threat to our democracy, but we cannot create a self-inflicted wound by marching towards a police state or undermining our democratic values.

I very much look forward to the discussion we're going to have.

● (1515)

The Chair: Thank you very much.

Go ahead, Mr. Bow.

Mr. Brian Bow (Director, Dalhousie University, Centre for the Study of Security and Development): Thanks to the members of the committee for this opportunity to provide input to the committee's ongoing consideration of Canada's national security framework.

I'm here in my capacity as the director of the Centre for the Study of Security and Development at Dalhousie—the successor research centre to the Centre for Foreign Policy Studies—but the views I'll be expressing here are my own, rather than those of the centre as a whole.

One of our core projects now is a comparative study that looks at the way that cross-national networks manage different kinds of internal or homeland security issues in both the North American and European regional contexts. It's a very broad study that takes in a number of different policy areas, and today I'm going talk a little about one slice of that. It's going to take us a little away from the themes that have been covered in some of the previous presentations. The argument I want to make here is based on an interest in broadening our view of what security questions we want to consider here as well as making the case for broadening and balancing our focus and thinking about how we want to weigh counterterrorism operations against other kinds of security priorities.

I'm going to be focusing mostly on cross-border cooperation and on border control questions, particularly the policing of cross-border criminal activity, with special attention to the trafficking of people, money, guns, and drugs.

The main point I want to make here is that some of the mechanisms for coordinated surveillance and enforcement activities that were set up in the immediate aftermath of 9/11, which were important initiatives, have been undercut over the last 10 years by reallocations of resources and shifting priorities by some of the agencies involved, and that has led to a diminishing of some of those law enforcement activities, or at least the cross-border coordination of them. I want to make the argument that it isn't necessarily a bad outcome, as long as those initiatives are replaced with new ones that respond more effectively to what we understand about how some of these illicit transborder flows actually work and are based on a different set of strategic priorities, which I will try to explain.

After 9/11, the top priority on both sides was demonstrating that the border was as tightly controlled as possible and, on the Canadian side at least, also that this was being accomplished without massively disrupting trade and travel or undermining Canadian sovereignty.

That led to the creation of a number of technical working groups on a variety of issues that were designed essentially to create new standards and procedures for border control and border patrol activities. These were enormously complicated and important policy coordination efforts. They were also very slow-moving, and in many cases dull and technically not very exciting politically, and for the most part they didn't get a lot of political or media attention. We tended to focus on cross-border law enforcement activities instead, and particularly a small number of initiatives that were flagship efforts, I guess, some of which predated 9/11, but many of which had been played up in the immediate aftermath of 9/11 as representative of a new approach.

Here in particular I'm thinking about the integrated border enforcement teams—the IBET program—and the shiprider program. These were played up politically, mostly based on having a particular symbolic value that came out of showing highly integrated operations at the front line, which could be reassuring to people who were worried about the adequacy of those border enforcement efforts, and also because they consistently produced tangible results in the forms of arrests and seizures. They looked good and they seemed to represent that the problem was being resolved.

Over the last 10 years or so, those programs have been diminished. They still exist on the books and people are still operating on those files, but far fewer resources are going into them. Here in particular I'm thinking of personnel, and that's because a lot of the people who had previously been assigned to these things, particularly on the west coast, have been reassigned to other things, and that is representative of a larger reallocation of resources within the law enforcement community.

● (1520)

There are two parts of this that I want to highlight for you.

One of them is a shift of priorities in terms of the RCMP's overall strategy for Canada drug operations and a tendency to refocus away from catching that one guy with the pickup truck at the border and thinking more about this as being part of a larger criminal network. It's thinking about how cases can be built that attack transnational criminal organizations at the centre and thinking about it more in terms of finance and building cases based on intelligence that lead up to the top of the pyramid, aiming at the head instead of at the toes of the organization.

At the same time, within the RCMP there's also been a redirection of resources away from organized crime in general and towards national security files, in particular on the intelligence side. There's a shifting both in terms of money and also personnel over to the intelligence side on national security files. Obviously, there are good reasons for that to happen, but there are significant consequences to the withdrawal of those resources from the organized crime files.

On the American side, there have also been some developments that have changed the landscape a little bit as well.

The main one, particularly on the west coast, has been the withdrawal of agency commitments to the IBET program and reallocation of those resources to the BEST, the border enforcement security teams, which is a model that was originally developed on the U.S.-Mexico side and has been now transplanted and spread to other regional directorships. Whereas the IBET program involved a number of different law enforcement agencies on the American side, none of which had a kind of clear lead within the program, the Department of Homeland Security's HSI, Homeland Security Investigations group, really dominates the BEST program and organizes it in a way that makes sense for them as an organization. That has consequences not only in terms of how they do their business but also on the participation of different agencies from both sides of the border.

One of the main things is obviously that the HSI's focus is on border patrol activities and law enforcement activities that are focused on the border area, and the RCMP just has fewer incentives to invest resources in that than it did in the previous version of the IBET-driven border co-operation. That, in combination with the shifting of resources within the RCMP, has meant that there's been a withdrawal of the commitment on the Canadian side from the BEST-centred border control activities. That is not necessarily a bad thing, because as much as the IBET looks great symbolically, they were really very much focused on catching low-level distributors and smugglers, and they really didn't do much damage to any of these larger transnational criminal organizations.

Obviously there's still a continuing need to have law enforcement activity at the border to manage those things, and I'm not suggesting we would give up on that entirely; however, there ought to be a shifting of resources to other things. I think the RCMP's larger strategic shift toward combatting criminal networks as networks makes a lot of sense, but it has to be followed through with a substantial investment of resources to support that activity; otherwise it looks, as it does in the eyes of many of the U.S. agencies that participate in, for example, the BEST, as a cop-out or rationalization for the withdrawal of participation altogether.

I want to make the argument here that there needs to be a shift of resources back into organized crime co-operation and that this shift has to be adapted to the new reality and new strategic priorities of the agencies involved. That means thinking about more of a task force model that involves cross-border co-operation built around attacking particular patterns of flows or particular organizations, and mostly it's going to focus on tracking money and long-term building of intelligence-driven cases against the leadership of some of these criminal organizations.

This is a costly and demanding thing, and it involves all kinds of political obstacles based on the differences in our disclosure rules and privacy rules. There are all those kinds of obstacles, but none of those diminishes the need to work out some kind of an understanding and to have a renewed commitment to resources to back it up.

● (1525)

The Chair: Could you wrap up quickly?

Mr. Brian Bow: Yes, it's the very last sentence, actually.

I just want to make the point that in general there was this productive spillover effect in the immediate aftermath of 9/11, when resources that had been sunk into counterterrorism activities spilled over into other areas, such as organized crime, emergency management, and other things. That has diminished now. That wave has crested. What we are seeing is a kind of overall shrinking of the resource pie.

I want to conclude by saying that as much as it's important to sort out all of the complicated questions surrounding counterterrorism, all of that has to be done thinking about the way that the redirection of resources into the solving of those problems has consequences for other kinds of security challenges that are out there.

The Chair: Thank you.

The floor is yours, Ms. Lane.

Ms. Andrea Lane (Deputy Director , Dalhousie University, Centre for the Study of Security and Development): Thank you very much for inviting me today. It's really an honour to present to you. My name is Andrea Lane, and I'm the deputy director of the Centre for the Study of Security and Development at Dalhousie University, although today I am appearing in my capacity as an individual.

I would like to speak to you about research that I have conducted that seeks to contextualize the broader discussion of anti-terrorism legislation, radicalization, and counter-radicalization measures. This research was funded by a bursary from Public Safety Canada under the Kanishka research affiliate program.

My research examines so-called single-issue terrorism—that is, terroristic violence used in the pursuit of an issue, such as environmental protection or white supremacism or the outlawing of abortion. It blurs the lines between right-wing and left-wing extremism, and this kind of terrorism is very often understudied, with public attention and law enforcement attention directed more on Islamic terrorism.

In particular, my research examined why some activists choose to use terroristic violence as a protest tactic, and how those activists differ from their non-violent counterparts. More importantly, it asks how security agencies could tell the difference between violent and non-violent activists before the bang—that is, in order to prevent attacks.

My conclusions provide some suggestions as to how costly surveillance and law enforcement assets could be used more effectively. It's difficult to summarize a year and 120 pages of the research into 10 minutes, but I'm going to try, so bear with me.

My research was testing a sociological theory of mobilization—that is, of how people come to be involved with a particular social movement or group, in this case terrorist groups. The theory was that people only become mobilized into activism or terrorism when several conditions are just right for this to occur, and not, as is more commonly thought, when they start to have beliefs or ideas about an issue.

● (1530)

We tend to think about radicalization into violence as belief before action. The theory that I was testing actually posited instead that it's actions before beliefs, so that people's beliefs, radical or otherwise, actually come about only after their participation in an activist group.

People who are at a turning point in their life—and it doesn't have to be a negative crisis, and it could be something as simple as moving to another city for a job or obtaining a divorce—who come into contact with an activist group, almost on a lark or accidentally at a time in their life when they're more receptive to certain ideas or new people, can be mobilized. Both of those conditions have to be met. If they have contact with a group while they are not at a turning point in their life, they're not mobilized. If they are at a turning point but they don't have contact with a group, they are not mobilized.

I tested this theory using the 1980s Canadian terrorist group called Direct Action, also known as the Squamish Five. I compared them with members from non-violent groups whose issue areas overlap those of Direct Action, including anti-nuclear and anti-resource development groups. I conducted interviews and collected evidence from court proceedings, newspapers, and groups members' own writings to see whether the theory of mobilization held true and could explain the difference between violent and non-violent radicalization.

My research found three things that are important for members of this committee to know as they go forward with a review of Canada's national security framework.

The first finding is that activists are moulded by the groups to which they belong. A group like Greenpeace or the Canadian Centre for Bio-Ethical Reform is not only a political group but also a social community with its own sets of traditions regarding the way its members should think about an issue and a corresponding set of traditions regarding protest behaviour.

For example, the CCBR believes abortion to be a social justice issue like slavery in the U.S., and it advocates for its supporters to use leaflets, bumper stickers, letters to their newspapers or MPs, and seminars to spread its message. Greenpeace, on the other hand, believes raising public awareness is key in effecting environmental change, and it encourages its members to participate in high-profile public stunts. This means that current members of non-violent protest groups are highly unlikely to commit terroristic violence because they are extensively socialized against it. In that case, violence is almost unthinkable for them because it violates the social rules of their group.

That brings me to my second point. Activist groups like Greenpeace, Earth First!, and Idle No More, who use what could be termed violence against property, are in fact valuable assets in the efforts to prevent violence against people. The conflation of violence against property and violence against people in terms of legislation or in crime prevention efforts does more harm than good, because in fact looking at non-violent groups that don't advocate violence against humans but that might advocate violence against property, for instance, is one of the best ways of finding out who within their larger groups might actually be at risk for being radicalized into violence against humans. If you alienate those groups by conflating property destruction and actual intentional violence against humans, then you lose a valuable asset. Those are my second and third points, because I recognize that I'm running out of time.

Thank you very much for your attention. I look forward to answering any questions you might have about my research or any other aspects of single-issue terrorism in Canada—which I gather isn't the sexy form of terrorism these days—and radicalization into violence more generally.

Thank you.

The Chair: You do have more time if you want to take it, but we also can move to questions.

Ms. Andrea Lane: It's really difficult to know which parts of my research would be most useful to what you're talking about.

The Chair: Then I suspect that the questions will evoke that.

We'll begin with Ms. Damoff.

Ms. Pam Damoff: Thank you very much.

Thank you to all three of you. It's been really interesting, and you've brought some different points of view to us, which is also much appreciated.

Ms. Lane, you said activists are moulded by a group. There's the violence against property versus people, but what was the third one?

Ms. Andrea Lane: The third finding is that in lieu of spending a lot of money looking at activist groups from the outside and attempting to decide who among them might be willing to commit violence, it would be more useful and much less expensive to develop relationships with these mainstream non-violent groups like Greenpeace or even Earth First! in order to be able to say to them "we recognize that your members, as they stand now, are not likely to commit violence, but you might have the best sense or information as to who might have left your group recently because that person was expressing radical views. You might know of members who have gone through a life change in the course of which they may have come into contact with people who advocate violence.

If you were going to embed an RCMP officer in a group long term, that would be incredibly expensive and would raise concerns among the public. Instead, you could say that you don't like that they advocate for vandalism, for instance, but laying that aside, you're primarily interested in stopping people from dying in those kinds of attacks, so you could work together. You want to develop a relationship in which they are free to say that they had a member last year who went through a really hard breakup and moved to Windsor and they want you to know that the member may have been in contact with people who do advocate for more extreme violence.

It's really about picking battles.

● (1535)

Ms. Pam Damoff: That would require quite a bit of trust between the group and policing, right? How do you raise that level of trust? I would suspect that people would say, "I don't want to tell you about that, because you're going to come after me for the vandalism", for example.

Ms. Andrea Lane: Yes, there are really two ways of thinking about that. One is that it starts as a bottom-up process in which you engage in low-level interactions. The alternative mechanism could be a top-down thing, in which you go through anti-terrorism legislation very closely and say that right now, as it stands, people who might be advocating hard-core vandalism and might accidentally injure somebody are treated the same way as a terrorist group that is actually advocating shooting people directly, putting it within the legislation that there is that finely grained detail as an opening statement to groups that might be less willing to participate.

I recognize we're talking about the difficulties of making a bridge between law enforcement culture and activist culture. I'm not under any illusion that it would be easy to do, but there are ways to make a venue for that kind of narrative to develop.

Ms. Pam Damoff: Mr. Fraser, you were talking about our cybersecurity, and it came up briefly with Mr. Oliphant in the previous panel. I'm on the status of women committee, and one of the things we've been looking at is cyberviolence. We had the chiefs of police come asking for the same things that the RCMP and CSIS were requesting when they appeared before us.

When we talk about the basic subscriber information—and I'm not a lawyer—they say they can't get it, but when we had the BC Civil Liberties Association appear before us when we were in Vancouver, they said there is a way for law enforcement to get that information. People always seem to perceive this issue differently when you bring in the issue of cyberviolence against women, but we do want police to be able to perform their jobs, whether it's in that context or in a terrorist context.

Is there a way under that Supreme Court decision that the police can get that information?

Mr. David Fraser: Absolutely, and it just requires judicial authorization. That's what it takes. Before the Spencer decision, there was a patchwork system. A number of Internet service providers decided that if the police said it was an investigation into a child exploitation offence, then the Internet service provider would hand over the customer information when provided with the IP address by the police. Every Internet service provider in Canada followed that except for two, both of which are based in Atlantic Canada.

Investigations were able to proceed here because we have been able, for the last 10 years or longer, to go to a Justice of the Peace and obtain a production order that requires the Internet service provider to hand over that information. That process was actually made easier under Bill C-13. That bill is best known for dealing with the non-consensual distribution of intimate images, but it also lowered the threshold for a number of production orders that allow a Justice of the Peace to provide that information.

I find it surprising that I hear from law enforcement that it's now more difficult.... Well, it is more difficult, because you used to just ask and get it, but it was in only a very small subset of cases that they were able to get it. They're saying it takes longer to get it from the Internet service provider, when in fact a production order includes a timeline that's a court order. Before it was just voluntary, and they were hopping to it.

They can get access to this information, and if there is a problem with the amount of time or paperwork or whatever that is required for them to get it, the solution is to have more Justices of the Peace and to create a streamlined process or to fine-tune or tweak what's in Bill C-13, rather than throwing the charter out the window.

They say they're only looking for basic subscriber information, a customer name and address, but as the Supreme Court of Canada decision said, they're looking to connect that name and address with an activity that's unlawful, such as trading child pornography, cyberbullying, or something like that.

● (1540)

Ms. Pam Damoff: This applies to terrorism as well, right?

Mr. David Fraser: It absolutely would. Certainly one can get a production order under a terrorism offence, and CSIS could also get a warrant under the CSIS act from a designated justice of the court.

One final point is that they can require this information without a warrant if there are exigent circumstances or there's imminent risk to somebody's life or property.

Ms. Pam Damoff: Because the Internet is international, concerns were expressed about treaties as well as about the 18 months it takes to get information from other countries. Do you have any comment on that?

Mr. David Fraser: I'm not sure that anybody is in a position to circumvent that. A Canadian court order is not effective against a U. S. company, and in the United States it simply can't be enforced.

Canada has, among the community of nations, negotiated treaties for mutual legal assistance in criminal matters. We have one with the United States and with most of our other allies. Maybe we can tweak that process, or we can expedite it for certain kinds of orders in connection with our multilateral obligations for cybercrime conventions and things like that.

It may become that you don't have to go through Global Affairs Canada for these kinds of warrants and you will just go from one justice department to another, but it's an important check, because the alternative without that is that Chinese courts could order access to Canadian information, as could Iranian courts, Egyptian courts, and others. “International” cuts both ways.

Ms. Pam Damoff: Thank you very much.

The Chair: Thank you.

Mr. Miller is next.

Mr. Larry Miller: Thank you.

To all three of you, thank you very much for being here.

Mr. Fraser, you talked about the oversight committee and the need for it to report to Parliament. Do you know of any developed jurisdiction in the world where it doesn't happen like that?

Mr. David Fraser: Certainly there are a number of mixed models and multiple accountability mechanisms in a number of different jurisdictions. Not having done a comprehensive survey across the OECD or across the United Nations, I think we are an outlier by currently having very weak parliamentary oversight. This committee's hands are essentially tied in a number of ways, when it should be one of the most robust ones.

As I mentioned, these services, by necessity, operate in the shadows. They have to. However, they have to become accountable, because the powers they have are significant and could be abused. That accountability to Parliament needs to be augmented as well as possible.

Mr. Larry Miller: Okay.

Britain, for example, has had a framework in place for some time. In 2013, they made some major changes to it. Can Canada take some lessons from that?

Mr. David Fraser: I haven't had the opportunity to study that fully in depth.

Certainly I think they've faced a number of the questions, a number of the concerns that we have. Although we come from a common constitutional lineage, I think we have a more robust and better-defined constitutional situation. I think that anything is going to have to be tweaked for our own context. Even though we're probably closer to Australia in a number of structural aspects of our democracy, I think we don't need to slavishly follow what somebody else is doing. However, absolutely, learning from the experience of other jurisdictions makes perfect sense.

Mr. Larry Miller: Okay, thank you.

You also touched on the green paper, and you made the comment that it looked as if it had been written by bureaucrats. Unfortunately, whether it's Agriculture Canada, Transport Canada, or the Justice Department, that happens way too much. It doesn't matter what government is in power, these bureaucrats write things the way they want.

How do you fix that problem? You can't just fire them all. Do you have any suggestions there?

Mr. David Fraser: There are some absolutely very capable people in the public service of Canada. There's no—

Mr. Larry Miller: I'm not saying there aren't.

Mr. David Fraser: —doubt in my mind.

However, they come from a long experience with different masters in a number of different political environments. I think that maybe, in one way, they could be suffering—whether they're Agriculture, Fisheries, or Public Safety—from being perhaps a little too siloed and a little too constrained in the audience they're hearing from. They're hearing constantly from the police. They're hearing constantly from CSIS. They're not hearing constantly from Canadians, from privacy advocates. I think that informs them.

I do think that ultimately the decision of what legislation is introduced rests with the minister, the cabinet, and the government, with a committee providing some significant opportunity and input. I think it's a matter of simply being consistent with one's election platform, with one's principles, with what one expects Canadians to do. It's ultimately looking at the best interests of Canadians, recognizing that while you might get very well-informed advice, it comes from a particular perspective, and those are the same advisers that were giving advice to the people you just won an election against.

● (1545)

Mr. Larry Miller: Great. Okay, thanks.

I want to leave some time for Ms. Watts.

Ms. Lane, you talked about violence against property versus persons. You almost said that as if that was okay. It's still terrorism, is it not?

Ms. Andrea Lane: Violence against property, you mean?

Mr. Larry Miller: Yes.

Ms. Andrea Lane: Yes, it certainly can be terrorism if it's done with the eventual goal of effecting political change by forcing governments to pay attention and that kind of thing. Certainly as written in Canadian law, then, property destruction can be terrorism.

The difference is that terrorism is a rainbow. There are all sorts of things that are called terrorism. If you want to prevent people from being injured or killed by terrorism, then you have to ask, if you have all of those things included in the bundle of terrorism, if that is actually the most efficacious way of stopping the things you're most concerned about.

I'm not in any way saying that we shouldn't care about property destruction or that it shouldn't be the subject of law enforcement, but the way terrorism is discussed and policed means that you might be sacrificing more effective prevention of human injury by pursuing property destruction under the terrorism framework.

Mr. Larry Miller: Okay.

Ms. Dianne L. Watts: Actually, Mr. Bow, this is the first time that we're hearing about border security in the hearings across the country, and I'm happy, particularly as my riding covers the Peace Arch border crossing, the Douglas crossing. As the former mayor, I've dealt with many of the issues that you spoke about in terms of the criminal activities—the drugs, the weapons, the human trafficking—and of course the famous tunnel that was built right across the border, and I would agree with you 100% in terms of the reallocation of resources and the number of the programs that have diminished or have been rejigged.

We look at the border crossing at Windsor, we look at the one at Peace Arch and then all the space in between, and we see some significant issues. It is around national security, because I think what we're seeing right now is a lot of the fentanyl and stuff, the drugs that are coming up from Mexico and coming through a variety of different areas. When we look at that impact just in British Columbia, we see that over 600 people are dead right now in the first part of this year because of the flow of those drugs.

I know there's been a lot of work around different strategies, around border integrity and all of those things. In terms of the strategy, can you talk about where we're at with those things now? I know that years ago it was very robust. I remember as a former mayor testifying before Homeland Security on a lot of those border issues, but as things have been diminished and resources pulled away, where are we at right now, in your estimation?

The Chair: I'm afraid I can't let you answer. That's your full time. Your preamble was your full time, but it was interesting.

Monsieur Dubé is next.

[*Translation*]

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

[*English*]

I know you acknowledged how difficult it is, particularly with the limited time, and I also understand that it's a complicated issue, but I have to say that I do find it a concern when there's always that possibility of profiling certain groups.

I'm from Quebec, and this to me sounds a lot like that slippery slope that leads to when the RCMP is stealing membership lists from a political party, which eventually then leads to the War Measures Act and people with any affiliation whatsoever with a certain community being detained. I know that's not what you're advocating for, and I don't mean to imply that at all, but I do have a concern when I hear that we want to make a link between legitimate groups and those who, for lack of a better word, fall off the wagon, because that's almost how I hear this narrative going.

This was part of the debate around Bill C-51. I know you're looking at it from a more sociological perspective, but I just want to hear from you on this point. When Bill C-51 was being debated, part of what I and folks in my party said is that while terrorism has a political element, political activity, even when it's civil disobedience, is not terrorism. I'm very concerned that when we look at it this way, when we start making links, even though they're stretched between the two, that's when we start getting lost as legislators, by putting these kinds of definitions—flawed definitions, in my opinion—in bills.

Again, I know it's complicated, but could I have your thoughts on some of those comments I've just made?

● (1550)

Ms. Andrea Lane: Sure.

I guess what I'm advocating for is actually a better situation than is currently existing with legitimate protest groups and government law enforcement. It is extraordinarily adversarial, and it's also combative and really expensive.

During the Vancouver Olympics, the budget for surveillance and following protest groups like Greenpeace or others who might have wanted to interrupt what was going on at the Olympics in a quasi-violent way was millions and millions of dollars and person-hours spent on this, because there existed this complete wall between protest groups and government.

You're perfectly right that if you go down this slippery slope of nailing every type of behaviour as possibly criminal, the end result is the criminalization of legitimate protest.

What currently exists is a fairly broad umbrella of what is defined as terrorism in Canada, and then this grey area where law enforcement is able to use terrorism-related language and assets to pursue groups who, yes, are advocating for property destruction and a bunch of things that most people and legislators would rather not have, such as big protest marches and things like that. As it currently stands, it's the worst possible scenario. You have that legislative criminalization and terrorization of that activity and you have no mechanism in which to speak to each other in a way that isn't really expensive, and it plays badly in the public eye as well.

Mr. Matthew Dubé: I'm hearing the cost effective side, but there's also...it's democracy. In the example you gave of Vancouver, it's not only about how much it cost to have those people surveilled; for lack of a better term, there's also the democratic cost. I guess that's what I'm asking: does it really need to be policed?

What we've heard from other witnesses, for example, and even from some folks we met in Montreal at the centre there for the prevention of radicalization, was that even though criminal acts may be taking place sometimes, there is a degree and sometimes there's a way to help rehabilitate someone, as opposed to criminalizing something. I guess I don't see where that possibility exists in this situation.

Ms. Andrea Lane: Now you're asking me to pitch my speaking points to a different audience.

When I originally conducted this research, I was very aware that coming in with my research findings and saying "Hands off protest groups, and just allow vandalism to happen" was not a message that was going to be embraced at any level of government or law enforcement.

You're absolutely right that there are social costs to any kind of law enforcement attention being paid to protest activities, but that isn't anything that expert testimony can decide. That's for Canadians to decide, and for you as lawmakers to decide. I have my own opinions on the social costs, but I can certainly help to explain where the tangible taxpayer costs are. On social costs, you're on your own, I'm afraid.

Mr. Matthew Dubé: Thanks for that answer.

Mr. Fraser, I don't want to spend too much time on Bill C-22 because we are going to study it, but inevitably it comes back again and again as part of this study because it is an important component.

My colleague Murray Rankin and I are working on what we think are some appropriate amendments to the bill, and some of that involves points that were raised about the fact that at the end the committee is answerable to the Prime Minister and cabinet, who have the final say over the content of the report. I believe you alluded to that in your comments.

The other question is in relation to public trust. For example, there are things like the election of the chair, as opposed to the chair being selected by the Prime Minister, in order to ensure more independence on behalf of the committee. Perhaps you'll share your thoughts on that and anything else you might want to add.

● (1555)

Mr. David Fraser: I think independence is absolutely key. If the chair is beholden to somebody for their position, then that ultimately does compromise the independence, and it may in fact also set up a situation where that posting, and it's just one of those structural concerns, may become a bit of a plum patronage thing. It's repaying a favour, so there's some level there.

I like the notion of a structure in which officers of Parliament are accountable to Parliament. This is a very important thing. Currently, my sense is that too much is structured in the supposed executive branch of our government. Really, in a parliamentary democracy you don't have an executive per se, but too much can happen outside of the purview of the core of our democracy, which is Parliament.

It really does need to also not be beholden to one particular side of the House. Obviously you're going to have ebbs and flows with respect to the composition of the House, but it's ultimately to the institution of Parliament on behalf of Canadians that I think the line of accountability needs to be drawn.

The Chair: Thank you.

Next is Mr. Fraser—the other Mr. Fraser.

Mr. Colin Fraser: That's right. Thank you, Mr. Chair.

It's great to be here. I'm not a usual member of this committee, so you'll forgive me if I ask any questions that are obvious to some of the other members of the committee, but thank you very much for being here.

I'd like to start with you, Mr. Fraser, because I like your last name, first of all, but also because I would like your thought on Bill C-51 in particular, which required CSIS to obtain a warrant from the Federal Court for certain disruptions of terrorism measures.

My understanding is that it had been stated by the Department of Justice that really it's reconciled on a section 1 analysis of the charter. Do you agree with that, or do you think it should be done in a different way whereby we don't look only at section 1 of the charter to save it, but at the charter rights themselves, and that whether to grant the warrant or not could fall down just based on the charter values themselves?

Mr. David Fraser: There is a very interesting discussion to be had in terms of how that gets implemented in practice. Is it a mechanism by which a judge is going to decide, on a proportionality analysis, that this disruption activity is actually of sufficient benefit to society as a whole that it justifies overriding an otherwise constitutionally protected right or another kind of lawful right, an interest in property or otherwise?

I think it's also worth taking a step backwards and asking if there is a place for such disruption activity, and if there is, whether it properly belongs in CSIS. One of my concerns is that so much happens in the shadows that it's difficult to determine what path it's following. Some of the activities the RCMP was undertaking prior to the McDonald commission really do seem like disruption, which is why it was taken out of the RCMP and moved into CSIS in the first place.

If we are giving CSIS the ability to burn down barns—just to pull an example out of a hat—that does seem to undermine the significant way our national security apparatus was set up. I wouldn't want to have that happen in just one bill, like Bill C-51. If we are going to rejigger our entire national security apparatus and change the nature of CSIS, I think that needs to be the topic of a much broader discussion.

Mr. Colin Fraser: Thank you very much.

We'll move to Mr. Bow.

You mentioned two elements—shifting priorities away from smaller enterprises to larger criminal organizations and a redirection away from organized crime to more terrorism-related activities—and reallocating the resources based on those priorities. Are we seeing this in most western countries? Are they doing this shift, and what impact does that have, in your opinion?

Mr. Brian Bow: I don't do enough comparative research in other places to say definitively that there is this sort of broader trend, but my expectation is that the answer is probably yes. Certainly there has been reallocation of resources into counterterrorism operations throughout the western world since 9/11, and there is nothing surprising about that.

The larger question is whether those increases have come at the expense of other kinds of law enforcement capacities or security activities. My impression is that in the United States, for example, that has not been the case. There hasn't necessarily been any diminishment of those capacities. If you look at the budgets for agencies like DEA , ICE, and the FBI, you'll see that there have been shifts there, but nothing like the kind of shift we've seen within the RCMP and its funding priorities over the last 10 to 15 years.

I don't know what the broader pattern is, but if we make that comparison with the United States, there has not necessarily been the same—

● (1600)

Mr. Colin Fraser: You touched briefly in your comments on the integration of security networks. I'm wondering, between Canada and the U.S., do you feel we should be better integrated? Should there be more sharing of information between our two countries?

Mr. Brian Bow: I think there should be. This is always a difficult thing, especially if your starting place is thinking about counter-terrorism and the RCMP in particular sharing intelligence with their American counterparts. Certainly there have been lots of times when this has gone awry and when we have deliberately changed the rules in order to limit that sharing or tighten up the rules that govern it.

On the particular side of organized crime, the legal protections and the disclosure rules are very well established, and to the extent that they are an obstacle, it's a well-known one and there are workarounds in place, which are sort of tacit ones, I guess. What needs to be figured out is a new system whereby there is a formal structure for information sharing that's relatively efficient but has oversight mechanisms built into it. Instead of thinking about fixing the problem of problematic information sharing by just cutting it off, we could be thinking about a mechanism for having more extensive information sharing through which there would be some vetting, some thinking about what is being shared, by whom, and under what circumstances, and there would be more checks in place that could work relatively rapidly in order to make for timely information sharing.

Mr. Colin Fraser: All right, thank you.

Ms. Lane, I'll turn to you for a moment. I appreciate your research on this issue. It's very interesting.

You mentioned that you don't want property violence and people violence to be conflated. Those are both reprehensible activities, in my regard, but I guess your point is that one is worse than the other. You say you don't want to conflate them. What do you mean by that? Is that happening now, and can you give examples of how it is happening?

Ms. Andrea Lane: It certainly is being conflated now, especially if you look at Canada's anti-terrorism legislation. Property damage that is political in nature and might be done by a group like Greenpeace or Earth First! counts as terrorism, because it is being done ostensibly to coerce a civilian population or to make a government make a decision.

The main problem with that is that there are social costs, but it's also not the most effective way to allocate resources. If you're focused on stopping the kind of terrorism in which people are killed, then adding this other area of law enforcement under the heading of terrorism means that in addition to wasting resources, you're using the resources you have to combat property destruction poorly, because you are alienating groups you could be working with.

There's a moral or a social question about whether or not property destruction should be counted as terrorism. More practically, though, it's just not a great way of stopping either the kind of terrorism in which people die or the property-damage style of terrorism.

Mr. Colin Fraser: In theory, that may sound reasonable to some, but in practice, do you think it would be hard for the security agencies to figure out which is which?

Ms. Andrea Lane: No. It's interesting that the Squamish Five, a 1980s group I used as a case study, were never convicted of terrorist acts. They weren't considered a terrorist group at the time. They blew up a power station in B.C. and there was a truck bombing of a Litton Industries' plant in Toronto. They were obviously a terrorist group, but there wasn't any kind of legislation in place that identified them as terrorists. They were never convicted as terrorists. They weren't charged under terrorist legislation, but law enforcement had no problem finding them, surveilling them, and stopping them. They were actually stopped on the way to a different attack in Cold Lake, Alberta, so it's not necessary to identify these activities as terrorism to effectively prevent them.

As well, there are opportunity costs that go along with identifying this is as terrorism.

● (1605)

The Chair: Thank you, Ms. Lane.

Ms. Watts is next.

Do you remember the question?

Ms. Dianne L. Watts: He's had time to think about it.

Mr. Brian Bow: There are a million things I could say about that, but I'll just make a couple of points.

The first thing is that the overall pattern on organized crime is that there are ad hoc efforts to build teams around particular cases. Most of the initiative for those things comes from international partners, and the RCMP participates in those in an ad hoc way. They very much are about providing support for multinational operations.

There are two kinds of negative consequences to that approach. One is that it tends not to build sustained professional networks. People move into these groups and they work on an operation until their part is done, and then they lose the connections. There's very little long-term relationship-building that might provide some of the trust that makes it easier to establish functional information-sharing relationships.

The other thing is that there's no strategic priority-setting in an arrangement like that. The operations that they participate in are, for the most part, ones to which they've been invited by law enforcement agencies in other places, particularly the United States, so rather than having a set of strategic priorities, they're essentially piggybacking on other operations.

I would suggest that we ought to be thinking about having a program for setting up a set of long-term campaigns driven by Canadian priorities on these things. We should identify the organized crime problems we want to address, build task forces around them, and then make connections to law enforcement agencies in other countries to pursue those cases.

Ms. Dianne L. Watts: I was involved in one case involving the cross-border sexual exploitation of children and youth up to Calgary and Vancouver and down to Seattle and that whole piece down there. At that time, it was ad hoc. I would think a strategic plan with strategic priorities is required, because once the resources are pulled away into counterterrorism, it leaves a vacuum on all of these other things, which could actually be a gateway for terrorism to occur. We shouldn't be leaving the vacuum, especially when we're talking about organized crime involvement in weapons, drugs, human trafficking, and things like that.

In your estimation, because you're doing some research on some of that and you've just spoken about some of the recommendations, what would you do immediately?

Mr. Brian Bow: What would I do immediately? I suppose what I would do is put pressure on the RCMP to think more seriously about how their new set of strategic priorities in terms of Canada drug operations translates into a strategy for co-operating with the U.S. and other partners.

Most of it is framed in terms of how Canadian assets are going to be used. Very little of it involves any kind of a substrategy. Given that most of this is going to be driven by collaboration with agencies in other countries, how does that work and how are we going to make a case for allocating a second set of resources to sustain those relationships over time?

Ms. Dianne L. Watts: Right, and I think that's the whole thing. I think we've heard Bob Paulson say that a lot of his resources have been pulled away and that therefore other things are sliding off the edge of the table. I think that's very valid, and when we do talk about national security, our border integrity is, bar none, one of the most important things.

I just want to switch to Ms. Lane. You made a comment—and I think my colleague here drilled down on it—about the different activities and different organizations in terms of forging relationships and getting information. It seems to me that these organizations, coming from where they come from, would really want to be protective of people's information and rights, and they wouldn't want to share that with the police. By making them do so, you're, in essence, making them informants.

● (1610)

Ms. Andrea Lane: Yes.

Ms. Dianne L. Watts: I mean, that's exactly what you're doing, right?

Ms. Andrea Lane: Yes.

The Chair: You have one minute left.

Ms. Dianne L. Watts: It seems to me that doing that would be counterproductive to what you're actually trying to accomplish. Can you comment on that?

Ms. Andrea Lane: Sure.

You're right: it is asking people to potentially inform on former group members or on people that they know of in their community. However, I think if you had a candid discussion with some of these groups, as I did as part of my research, you would see the scrutiny that they live under now. They're well aware that law enforcement assets are trying to infiltrate their groups. They know that their emails are being read or their phone calls are being listened to.

If you ask them to participate in more of a dialogue, more of a partnership, in which both government and these groups have a common goal to not see this kind of violence diminish the impact of legitimate protest activity in Canada, that's something that people would be willing to work towards, with the caveat of not talking about property destruction as terrorism.

Nothing could be worse than the relationship that civil society groups and protest groups have with law enforcement and government now. It certainly is worth a try. You're right that it is kind of asking these groups to become informants, but they're already—

Ms. Dianne L. Watts: Which would be fundamentally against their core belief system, I would think.

Ms. Andrea Lane: That depends on the group.

Ms. Dianne L. Watts: True enough.

The Chair: We're going to have to end there. We're well over time.

Ms. Dianne L. Watts: I was just going to ask if she could submit her research paper.

The Chair: Absolutely. We'd be delighted to have any of your research work.

If any of you have anything you'd like to submit in writing to the committee, it would be very helpful. It would be helpful for this study, as well as for Bill C-22, so if you have something, that would be very interesting for us.

We're actually not bad for time with our extension.

Thank you for your help with our study. I'll remind those of you in the gallery today that we'll be reconvening at 5:30 p.m. That's an opportunity for anyone from the public who would like to speak to the committee to do so.

Thank you very much. The meeting is adjourned.