



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 027 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 4, 2016

—
Chair

Mr. Robert Oliphant

Standing Committee on Public Safety and National Security

Tuesday, October 4, 2016

• (1635)

[English]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib.)): I'm going to call the 27th meeting of the Standing Committee on Public Safety and National Security to order.

Welcome to our guests. Thank you for coming to help our committee.

We are in the very early stages of framing our study on the national security framework of Canada and looking at how Canadians understand the need to balance national security concerns with maintaining our civil and human rights.

That is the framework we are doing. We'll have both the legislative review going on and recommendations to the government on what legislative changes need to be made to ensure that this is the balance Canadians are looking for. We are also going to be looking at other issues that may arise as we have hearings.

Our hearings will be in Ottawa and will be driven by a variety of individuals who have expertise as well as organizations and agencies that are engaged in this kind of work. We will also have five meetings across the country in various cities.

You are our first witnesses on this brand-new study. You have a wonderful and unique opportunity to shape our work.

We're going to begin with remarks from the Privacy Commissioner, Mr. Therrien, and then Professor Wark, and then the committee will ask questions.

[Translation]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair. Thank you to the committee for inviting me to appear before you today.

In particular, I will be focusing my comments on the government's Green Paper, which was recently released. We will present our formal response to Public Safety by December 1. In the meantime, I am happy to provide preliminary comments, in the hope these may be helpful as you prepare to engage with Canadians in several cities across the country.

The stated purpose of the Green Paper is to prompt discussion and debate about Canada's national security framework, which is broader than the reforms brought about by Bill C-51, the Anti-terrorism Act, 2015. I fully support the need to review the entire legislative framework, not just the changes brought about by Bill C-51. But to do that in a comprehensive way, the focus cannot be only on

addressing challenges faced by national security and law enforcement agencies. It must also take into account legislative changes and other developments that have had an impact on human rights, including international information sharing and the need to adopt rules to prevent another tragedy like the one lived by Maher Arar.

In order to ensure our laws adapt to current realities, it is important to consider all that we have learned since 2001, including the revelations of Edward Snowden regarding government information gathering and sharing activities, as well as other known risks regarding the protection of privacy and human rights, including those identified during commissions of inquiry. Obviously, we must also consider recent terrorist threats and incidents.

In my public statements on Bill C-51, I expressed significant concern with the broad information sharing authorized by the Security of Canada Information Sharing Act. I warned that the lowering of thresholds for sharing could lead to large amounts of personal information on law-abiding citizens being disclosed. Edward Snowden demonstrated how government surveillance powers can be used on a massive scale. Unfortunately, there is nothing in the Green Paper that addresses the lowering of legal standards for information sharing.

When Bill C-51 was tabled, the government maintained SCISA was necessary because some federal agencies lacked clear legal authority to share information related to national security. The Green Paper addresses complexity around sharing, which can prevent information from getting to the right institution in time. These references to the complexity of the old law do not clearly explain its shortcomings. Situations where there is no legal authority for sharing information related to national security can be identified, but so far they have not. I strongly urge this committee to ask specific questions on the subject. A clearer articulation of the problems with the previous law would help define a proportionate solution.

•(1640)

[English]

The green paper speaks of the challenges of law enforcement getting access to what it calls “basic subscriber information”, which is cast as relatively innocuous on the premise that it does not include the contents of communications. There has been extensive work done by my officials and other technical experts that finds that this subscriber information, or metadata, is far from benign. Daniel Weitzner, who founded the Internet Policy Research Initiative at MIT, considers metadata to be “arguably more revealing [than content] because it's actually much easier to analyze the patterns in a large universe of metadata and correlate them with real-world events than it is to go through a semantic analysis of all of someone's email and all of someone's telephone calls.”

The GCHQ, the British signals intelligence agency, has publicly stated that metadata is more revealing for intelligence purposes than the content of communications. If, as the green paper suggests, new legislation is to be informed by the privacy expectations Canadians have about metadata, Canadians should be clearly advised of the personal information metadata can reveal about them.

The green paper presents a scenario in which a police officer wants to obtain metadata from an Internet service provider but is unable to do so when the investigation is still in its early stages, and there is not enough information to convince a judge to provide authorization. While we appreciate that it might be useful information to have “at the outset of an investigation”, as it says in the green paper, it is unclear to us why neither the evidentiary threshold required to obtain judicial authorization via production order or warrant nor the exigent circumstances exception articulated in *R. v. Spencer* can be met.

I should add that preservation orders can be obtained on a reasonable grounds to suspect threshold, a very low standard indeed. In that context, we would urge the committee to probe government for precise explanations of why current thresholds are unreasonable and why administrative authorizations to obtain metadata, rather than judicial authorizations, sufficiently protect charter rights.

Encryption, another issue raised in the discussion paper, represents a particularly difficult dilemma. On the one hand, as a technological tool, it is extremely important, even essential, for the protection of personal information in the digital world. On the other hand, as a legal matter, individuals who use it and companies that offer it to their customers are also subject to laws and judicial warrants that may require access to personal information where legitimately needed in cases in which public safety is at risk. Ultimately, the issue is whether it is possible to enable authorized access for the state without creating technological vulnerabilities imperilling the privacy of significant numbers of ordinary citizens. Where it is not possible to do this, I think it is important to ask which of these two important public interests should prevail. We expect to have more to say on this by December.

The green paper lists accountability mechanisms, including ministerial oversight, judicial review, Parliament, and review by independent bodies of experts. On the issue of parliamentary review, I would note that Bill C-22, which proposes to create the national security and intelligence committee of parliamentarians, fills the

need for democratic accountability and brings us into alignment with other western democracies. I would note, however, that many agencies that have a role to play in national security or public safety are not currently subject to any independent expert review. This is an omission that, in my view, needs to be addressed.

As I mentioned, my office will be submitting a formal written response to this green paper once we've fully analyzed some of its newer proposals. In the meantime, I would be happy to answer any questions you may have. For instance, I think it would be important to discuss how monitoring of the Internet to prevent radicalization should not create a climate such that ordinary Canadians feel they cannot enjoy fundamental freedoms.

Thank you very much, and I look forward to your questions.

•(1645)

The Chair: Thank you very much.

Professor Wark.

Mr. Wesley Wark (Visiting Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual): Chair, and members of the committee, it's my pleasure to have the opportunity to present my views on the government's green paper on national security, and the online consultations that Canadians are invited to take part in.

I will focus my brief introductory remarks on the following four issues: the significance and importance of consulting Canadians on national security issues, proposals for utilizing the consultation process, the green paper, and some problems with the green paper.

The first is on the importance of consulting Canadians. All democratic societies seek to establish what is often called a balance between protecting the security of the state and its citizens, and protecting civil liberties. The search for such a balance cannot be left in the hands of government alone. It requires democratic engagement, and ultimately is based on a perception of democratic legitimacy. The Canadian practice for too long has been based on a notion of paternalistic governance on national security matters, rooted in requirements of near absolute citizen trust, in exaggerated concerns about protecting secrets, and assumptions about the inability of our society to fully grasp or even respond well to national security challenges: government knows best.

This set of attitudes is fundamentally outdated, and has been eroded, in particular by the rise of new security threats in the aftermath of the end of the Cold War, and with the ascendancy of global terrorism post-9/11. There are new expectations around citizen knowledge and engagement in discussions on national security that must be met.

When last in power, the Liberals issued Canada's first-ever national security strategy, in April 2004. It was an important effort at public education but proved to be an unfortunate one-off. Now the Liberal government has gone a step further and decided to engage in public consultations about Canadians' views on the effective construction of a balance of security and rights protections, framed in part in response to a very divisive parliamentary and public debate around the previous government's introduction of new anti-terrorism measures in Bill C-51.

I fully support the principle of public consultations on national security, particularly in the aftermath of Bill C-51. I'm also hopeful that these consultations can have a real impact, in two ways: first in terms of an improved public understanding of national security threats and responses; and, second, in terms of improved government legislation and policy. I do not accept the view that these consultations are an empty forum designed with a purely political objective in mind. If we decide, as some in the media would like, that public consultations and national security are a form of ragging the puck, then we are truly in a sad shape as a democracy.

The second issue, to raise it very briefly, is a question of how best to utilize the consultation process. A public consultation exercise on national security is historically unprecedented in Canada and has no counterpart that I'm aware of among our close allies. It is an experiment with an unknowable outcome. The government may well find that public responses exceed its expectations, at least in quantity. The Minister of Public Safety has recently stated that some 7,000 responses have already been logged, and there remain two further months before the online consultation is closed. The government has said it intends to use the consultations as a means to improve both policy and legislation, but has provided few details about how it proposes to handle the consultation material.

I would like to see two developments. One is for the government to create an independent expert advisory panel to study the public inputs and come up with their own summary and recommendations. I regard this as important to ensure that, in addition to the expertise provided by their officials, the government can hear other knowledgeable and diverse perspectives. The second desire is for the government to commit to producing a white paper on national security, a new national security strategy out of the green paper process. Beyond that, as part of a transparency initiative, I would like to see it commit to a regular process for the issuance of national security strategy statements to Parliament and the Canadian public. My hope, of course, is that the committee might endorse these ideas.

With regard to the green paper, green papers, as I'm sure you all are aware, are meant to be policy-relevant studies that consider a range of options or scenarios but do not indicate intended policy. The government's green paper entitled "Our Security, Our Rights" was publicly released on September 8, 2016, after a long and difficult internal birth. It comes in two forms: the shorter document, numbering 21 pages, and a longer background document weighing in at 73 pages. In addition, Canadians are encouraged to consult the terrorism threat statement issued just prior to the release of the green paper. The green paper itself was produced by a task force headed by the assistant deputy minister for national and cyber security at the Department of Public Safety and was conducted as an in-house exercise.

● (1650)

The green paper addresses 10 issue areas, to promote, as the minister's foreword indicates, a "framework that upholds both security and rights". I'm going to very briefly break down these 10 issue areas.

The first two deal with accountability and prevention, and these address Liberal campaign promises. The next four, threat reduction, information sharing, the passenger protect program, and Criminal Code terrorism measures directly address issues raised by the debates around Bill C-51.

There are two further issues around procedures for listing terrorist entities and terrorist financing. The background to their appearance in the green paper is a mystery to me, and I don't regard either of them as particularly amenable to public discussion. They're very technical and perhaps non-controversial.

The final two issues raised are what we might call unresolved and challenging legacy problems. "Investigative Capabilities in a Digital World" revisits a stalled legislative and public debate over what we have long described as lawful access. The intelligence and evidence problem dates back to the decision to create CSIS in 1984 and to separate security intelligence from police work. It was studied more recently and intensively, of course, in the context of Justice Major's Air India inquiry and report.

I would judge at least eight of the 10 issues worthy of public debate. They are both framework issues and, in some cases, directly relate to current anti-terrorism legislation. Of the eight issues identified, the most forward looking concerns investigative capabilities in a digital world. Canada needs a new approach to digital security and digital intelligence gathering, but one that must be embedded in strong privacy and rights protections. On the digital intelligence gathering side, we need a better understanding of metadata collection powers as exercised by Canadian intelligence agencies and of the use of social media intelligence, which is now widespread, and we need better controls to ensure privacy.

I do have some regrets about the green paper's construction. I think it narrows the frame of public discussion too much by its focus on terrorism-related threats alone. The green paper also fails to deliver enough information about the organization of the Canadian security and intelligence community and about the existing capabilities that that community possesses to deal with threats. We cannot find a balance between security and rights in Canada unless our knowledge is sufficiently well balanced to include an understanding of threats, an understanding of available responses to threats, and an understanding of rights.

To conclude, let me turn to some problems I've identified with the green paper itself.

The shorter version of the green paper presents itself as scrupulously neutral and asks very general questions in its conclusion. The longer background document suggests more of an effort to steer the public conversation through selective attention and raises questions, in my mind at least, about the degree to which the government has already made up its mind or been captured by official advice on some issues.

It is important, I think, that the government really listen to the consultation exercise and keep an open mind about policy and legislation in this very complex field. I see some problems in terms of potential closed-mindedness and bureaucratic capture in the following areas.

On accountability, the green paper does not sufficiently address the problems with the existing system of independent external review of security and intelligence agencies, and it does not address the questions of transparency, public education, and sustaining public knowledge.

On prevention, experts will caution against an over-commitment to a theory about radicalization to violence that does not fully reflect the research that has been done to date and may be a problematic concept in other ways.

On threat reduction, the green paper does not ask fundamental questions about whether threat reduction capabilities in the form created by Bill C-51 are needed and who should have the power to deploy them. It makes no distinctions between the very different circumstances of threat reduction activities at home and threat reduction operations abroad.

On domestic national security information sharing, no effort at all is made to genuinely question the changed definition at the heart of SCISA, the Security of Canada Information Sharing Act, which was part 1 of C-51, and that changed definition shifted from, as you will know, section two of the CSIS Act, "threats to the security of Canada", which has been long our understanding, to something different and admittedly broader called "undermining the security of Canada".

On passenger protect, Canadians need a commitment to transparency around the no-fly list so that fears of it burgeoning out of size and control can be allayed. I do not mean absolute transparency but an annual reporting of global, anonymized figures for the SATA list, plus more publicly available information about how the SATA list is actually built.

• (1655)

On investigative capabilities in a digital world, this is an important conversation that we need to build into the discussion of controls around metadata collection and the use of social media intelligence.

On intelligence and evidence, it's important to understand this issue is a matter that extends well beyond legal considerations, to include our historical context and the relationship, in particular, between the RCMP and CSIS.

I have not enlarged on any of these concerns but would be happy to address them in questions. I would hope to have a future opportunity to discuss these issues with the committee, particularly when specific amendments to Bill C-51, or new policies and legislation see the light of day.

Thank you.

The Chair: Thank you very much.

I just want to take the opportunity to assure both the witnesses that this parliamentary committee is independent of government. Our review of the national security framework will be informed by the

green paper but certainly not limited to it. That is why we are engaged in this process. This is just to make sure people are clear about our independence from that.

We're going to begin with questioning from Mr. Mendicino for seven minutes.

Mr. Marco Mendicino (Eglinton—Lawrence, Lib.): Thanks to the witnesses.

This is to build on the point that the chair made. Not only will this committee act independently, and not only will it be informed by some of the broad parameters of the green paper, but we will be informed by your testimony, and those of future witnesses, which is of course given to us, we expect, objectively, dispassionately, to a certain extent. We will reflect on that evidence in shaping our report and whatever recommendations that may flow.

I hope you take that assurance, Professor, in good faith, because it is certainly delivered with that intent.

Let me ask a few quick questions because I don't have a lot of time.

Mr. Therrien, I read your department's most recent annual report. There's a recommendation there that Parliament address the question of oversight. You address that in your written remarks. To what extent does Bill C-22 not address those concerns? Do you have any residual concerns? On your read of it, do we have the balance right?

Mr. Daniel Therrien: Bill C-22 is progress in that it would create a committee of parliamentarians. It is important that departments and agencies that work in the national security area be supervised, monitored, and reviewed by elected officials. The democratic legitimacy of that committee is extremely important. I do not think that it is sufficient. Parliamentarians bring democratic legitimacy, but they are not substantive experts.

I think we need both review by elected officials and review by experts in these national security issues, human rights, etc. On the expert review side, Bill C-22 does not deal with that issue. We are left with three national security agencies being the subject of expert review. The majority of the 17 national security agencies, if we look at that world, able to receive information under SCISA, are not the subject of expert review.

I think to have a complete picture it is important that all agencies involved in national security be the subject of expert review and oversight. On the mechanics of this, is it one review body? Is it several? It would need to be discussed. My point is that all departments and agencies involved in national security should be the subject of expert review.

• (1700)

Mr. Marco Mendicino: Would you agree that this is a first step and that as part of the mandate, which will be given to the oversight committee, the members of that committee will, over time, develop the substantive expertise that you, I think, envision? Isn't this very similar to the legislative process and journey that other jurisdictions have had to undertake themselves?

Mr. Daniel Therrien: It is certainly a good first step, but I maintain that expert review will continue to be required to review the activities of, say, the Canada Border Services Agency, which did not have much jurisdiction in terms of national security pre-9/11, but is now a very important player in the national security area. I do think it is important that the CBSA, and others, but particularly the CBSA, because it has an important role in national security, be the subject of expert review.

Mr. Marco Mendicino: Let me move to the second general area that I'd like to ask you about, and that is with regard to SCISA.

In your report, you recommend adjusting the legal threshold, or the policy threshold, that would allow various agencies within the public sector and right across government to share information. Currently, if I understand the statute correctly, departments can share information so long as it's relevant to the recipient organization's mandate. Your recommendation is that we elevate it to necessary to fulfill that recipient organization's mandate.

Can you explain to us why you think that adjustment needs to be made, and if you have time, can you provide us with an example of how it might apply in a practical situation?

Mr. Daniel Therrien: Sure.

The issue with the relevance test, in my view, is that it is such a low threshold that it ultimately creates risks for people who are not suspected of criminal or terrorist activity.

To take a step back for a second, greater information sharing to detect national security threats is a good thing. I do not have a problem with the objective of linking information sharing with the detection of national security threats. In order to achieve the proper balance between threat identification and reduction on the one hand and protection of privacy and human rights on the other, the threshold that authorizes sharing between departments is important. It may look somewhat technical, but it is very important.

Mr. Marco Mendicino: To pick up on that, isn't it precisely because the threats that exist today are different from what they were 20 or 30 years ago, and even more recently, that we need a threshold that is appropriately flexible so that we're not paralyzing departments from sharing information?

Mr. Daniel Therrien: I don't think that raising the bar through necessity would paralyze departments. It is important that individual agencies within government be able to share information with a view to—

• (1705)

Mr. Marco Mendicino: Can you quickly give us an example of how it might apply? What does "necessary" mean in your opinion?

Mr. Daniel Therrien: First of all, the necessity standard is used in Europe, for instance, and so it exists. It's also used in certain provincial legislation and in privacy legislation that is not national security centred, so that threshold exists.

The Chair: I'm going to caution members that we will be having hearings on Bill C-22, and we'll be taking an extensive amount of time. If we use our time here on Bill C-22, we're not going to be able to get as much on the national security study, so try to keep your questions on our study.

Mr. Miller, for seven minutes.

Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC): Witnesses, thanks very much for being here.

Welcome back, Mr. Therrien. You were here just last week, I believe.

You have come out critical of Bill C-51. I have an article here from the Canadian Press about information sharing. It says:

Citizenship and Immigration Canada, the Canada Border Services Agency, the Canadian Security Intelligence Service, and a fourth agency whose name is blacked out of the records have all used the provisions.

The article goes on to say that, even though you've been critical of Bill C-51 and the sharing of information, you've been engaged throughout the whole implementation phase.

Seeing that you're involved in that implementation, are you still critical of it? That seems contradictory.

Mr. Daniel Therrien: I would have a different view of my level of involvement and engagement, I must say.

I'm not involved greatly in the implementation of SCISA, or what was Bill C-51. What I'm involved in is conducting an independent review of how the executive branch and departments are using and implementing this piece of legislation. I'm not involved in implementing it. I'm involved in reviewing how it is implemented.

Mr. Larry Miller: Fair enough.

I have another question I want to ask you. The general consensus, from anything I've read and heard on Aaron Driver, the would-be terrorist who was caught in Strathroy, all agencies, or most, have commented that without the sharing of this information, Mr. Driver may not have been stopped in this case.

A lot of people will say that when it comes to the sharing of information.... I'm as private a person as there is and I don't like the idea of it, but we live in a different world today. In general, if I'm not doing anything wrong, I don't have anything to worry about as far as that kind of thing goes, and if it helps catch another Mr. Driver, then it's a small sacrifice.

Could you comment on that sharing of information and the likelihood that it did help to catch Mr. Driver, and how you can still criticize it?

Mr. Daniel Therrien: I don't have the facts surrounding what happened to Mr. Driver. What this suggests to me is that these assertions that SCISA, or Bill C-51, have helped or were necessary.... I'm open to a demonstration of that, but neither—

Mr. Larry Miller: I'm talking about the sharing of information here.

Mr. Daniel Therrien: Yes. What I'm saying is that the then government.... You're saying that greater information sharing may have assisted in identifying Mr. Driver as a terrorist, and I'm open to a demonstration of that. I would encourage you strongly, as a committee, to ask government officials or others, including the national security agencies, if they could please demonstrate how the previous legislation was deficient in that regard.

What is it in the previous legislation that prevented the type of information sharing that you say is necessary? I'm not disputing that information sharing is useful. It is useful, but there needs to be a demonstration that the previous law was deficient and how it was deficient, so that as parliamentarians, you can then assess how the previous law needed to be changed to reach the goal.

• (1710)

Mr. Larry Miller: Okay, I'm going to run out of time.

Here's my last point on this before I turn it over to Mr. Brassard. I'm not an expert in the field but I was in the parliamentary precinct on October 22 two years ago. A lot of law enforcement and so-called experts say that if they'd had some of the powers then that Bill C-51 gives them, including sharing of information, there's a good chance that Corporal Cirillo would still be alive today. Maybe the would-be terrorist would still be alive, but that's another story. I feel it is very necessary to point that out.

I'll turn it over to Mr. Brassard at this point.

Mr. John Brassard (Barrie—Innisfil, CPC): How much time do I have, Mr. Chair?

The Chair: You have two minutes.

Mr. John Brassard: Okay, very quickly, Mr. Wark, you spoke about the problems with the green paper with respect to "suspiciously neutral" and that it tends to steer public conversation to a precluded decision, but on the other hand, you talked about this being an unprecedented process in Canada with the 7,000 responses that have been logged.

You also spoke of an independent expert advisory panel to look at those responses. Are you suggesting that an independent expert advisory panel also look at some of the discussions this committee is going to have across the country and disseminate those results and come up with a conclusion?

Mr. Wesley Wark: Mr. Brassard, thank you.

It certainly could do. What I had in mind was that if the government is going to be faced with a virtual deluge of responses, which would be the best outcome from a public consultation of this kind, and if perhaps, as the science indicates, they are not ready with a plan as to how to deal with that volume of information, then it might be very helpful to have an additional set of critical eyes on the inputs from the consultation process.

Mr. John Brassard: What would the makeup of that advisory panel look like? What types of experts would you recommend?

Mr. Wesley Wark: I would be looking for people who have expertise in national security law with regard to national security practices, with regard to law enforcement, with regard to intelligence, with regard to civil liberties and privacy issues. I think you could put together a useful, diverse group of that kind, and perhaps there would be other voices that would need to be heard there. The main idea behind this suggestion is that it could be of great value to the government in sorting through the responses they've had. It would give more legitimacy to how the government might respond to those inputs. It might give them some new, original, creative ideas to deal with as they proceed down the road to policy and legislative changes.

In my mind, it's a practical suggestion, and certainly its mandate could reach out beyond just the inputs themselves, if the government decided or the committee suggested to include the kinds of things your committee will hear as you go on the road and talk to Canadians.

The Chair: Thank you, Mr. Wark.

Monsieur Dubé, go ahead.

[*Translation*]

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair. Thank you to the witnesses for being here.

I must admit that I have a sense of déjà-vu because we're hearing the same concerns that were expressed last year in the committee.

My first question is for both of you. We talk about the importance of expert oversight. The CSIS inspector general position was eliminated. Can that type of position be reinstated? I understand it's one of many positions. However, I'm mentioning it as an example of a position that should be reinstated to ensure independent oversight.

Mr. Daniel Therrien: The inspector general certainly played a useful role. I have no particular opinion on the system—once again: one committee, several committees, how to divide oversight roles—other than to say that all the agencies working in the field should be monitored. If all the departments are monitored, there can then be different system models that are more or less effective and more or less costly. However, if all departments are subject to actual and serious oversight, I think that would be satisfactory.

[*English*]

Mr. Wesley Wark: Monsieur Dubé, I would add that we probably have to keep our attention focused on the problem we are trying to deal with. The inspector general was a small office within what became the Department of Public Safety to provide reporting directly to the minister on the activities of CSIS.

The real problem I think we have to address is something the commissioner has already raised, which is that in the existing system we have for independent expert review, we have created this very siloed system with different independent review bodies looking at single agencies without any capacity to link those views into a kind of strategic overview, and without any capacity to address the broader Canadian security and intelligence community.

Once upon a time, the Canadian security and intelligence community was small. Now it's large. I think the government has some difficulty in even deciding how large. The count is between 17 and 20 agencies that have different kinds of national security and intelligence functions.

I don't have a solution to this. The public safety minister has mused about the idea of creating a super-SIRC, as he has called it. Disappointingly, from my perspective, there is no reflection on these possibilities in the green paper itself. In fact, one of the ways in which I would say the green paper steers the conversation a little too vigorously is that it steers it away from a discussion about enhancing independent review and making sure it's strategic and capable of linking all the activities. There is even a hint of a suggestion that if you create this new committee of parliamentarians in Bill C-22, you may not need an additional layer of independent review, which I think would be a terrible backward step.

• (1715)

[Translation]

Mr. Matthew Dubé: Thank you.

Mr. Therrien, I want to go back to the troubling information obtained by the Canadian Press through the Access to Information Act. The issue concerns the information being collected by CSIS regarding Canadians detained abroad who turn to consular offices.

Is that an example of situations that could be reviewed because too much leeway is given to the authorities? Take Mr. Arar's case, for example. There could also be a situation involving a Canadian who has simply lost his passport and found himself in a turbulent situation somewhere in the world.

Mr. Daniel Therrien: I'll refer to my opening remarks. I think it's a good thing that the Green Paper goes beyond Bill C-51.

However, the Green Paper and the discussion paper on information sharing, for example between Foreign Affairs or Global Affairs Canada and CSIS, addresses only information sharing within Canada. It does not address information sharing at the international level, with countries where our diplomats work.

The entire legislative framework and all the relevant national security policies must be reviewed to have a clear idea and to ensure the lessons learned—I hope—from September 2001 are applied. It's not enough to take into consideration only Bill C-51 and information sharing within the country. We must look at the whole situation.

Mr. Matthew Dubé: Perfect.

Thank you.

[English]

Mr. Matthew Dubé: Professor Wark, you mentioned the no-fly list. A lot of the problems that arise there seem to often come from using the Americans' list and some of the incongruities that exist. When we're talking about information sharing, some of that also has to do with our allies as well, not just within departments in Canada.

Could you perhaps comment further on some of the problems you see there and how they can be resolved?

Mr. Wesley Wark: Certainly.

First of all, I think that probably all Canadians would agree that if we can in Canada, we want to avoid the problems the Americans have had with their own multiplicity of no-fly lists, border lists, watch-lists, and so on, which is a machine which is truly out of control. It impacts on Canada, to the extent that Canadians can be caught up in various American lists.

We share information with the United States and other allies. One of the problems I think around the way in which Bill C-51 deals with enhancements to the passenger protect program, which I think were necessary but I think can be fine-tuned in revised legislation, is that the whole regime for information sharing with allies, in terms of what we will share and under what circumstances, is not clearly spelled out in a way that it needs to be spelled out.

As I say, I think it would be an important exercise in public reassurance and transparency for the minister in charge, the Minister of Public Safety, to actually publish an annual report simply indicating the number of individuals on the passenger protect list. It's not naming names, but just indicating the number, so that Canadians don't feel that this list is out of control, too large, or that they don't have another kind of suspicion, that it's too small and the government is not doing their work.

I think that would be an important measure, and it's also an important measure of control and accountability. That's one of the things I would like to see. I think there are other ways in which the passenger protect provisions of Bill C-51 can be improved, including the responsibilities that the minister has to respond to appeals to be taken off the list. That is a very awkward piece of drafting at the moment in Bill C-51.

• (1720)

[Translation]

Mr. Matthew Dubé: Thank you.

[English]

The Chair: Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): For my questions, I'd like to take you away for a bit from the role of government and the legal framework, and focus a bit on Canadian society and Canadian culture as it relates to national security.

Monsieur Therrien, maybe to take you up on your last sentence in your submission, you state that it would be important to discuss how monitoring of the Internet to prevent radicalization should not create a climate such that ordinary Canadians feel they cannot enjoy fundamental freedoms—individual freedoms, presumably. I would like to also add that probably it should not be steps that threaten the fabric of our society.

I want to ask each of you what your perceptions are—not your own perceptions of our national security framework, but your perception of Canadian perceptions—on national security. How does Canadian society, Canadian culture, think about national security in the decade and a half since September 11?

Give us as fine-grained a view as you can for the understanding of the committee and Canadians at large. Where I'm going with this is to sort of probe with you the resilience, potentially, of Canadian society toward radicalization, or keeping what we have, what we cherish, against what is described as an increasing and potentially unknowable external threat.

Mr. Wesley Wark: It's an excellent question, sir, and I think it would be difficult for perhaps either of us to give you a truly fine-grained, evidence-based answer to your question. I have views on this, and they're views of long standing that have evolved since 9/11.

I think the first thing that has to be said is that what I call Canadian literacy on national security issues is low. This is not the fault of Canadians themselves. I place the fault squarely at the feet of governments for failing to educate and inform Canadians adequately about national security threats and the kind of response capacity we have to them. I'm hoping that the new Liberal government will change that pattern of past behaviour, and perhaps the green paper is one sign that they truly intend to do so. But I think it has to be systematically done.

I've often responded to media questions whenever there's a terrorist incident or a prevented terrorist plot in Canada. The question is often about how Canadians have responded. My anecdotal feeling about that—and that's all it is—is that Canadian society has shown remarkable degrees of resilience. We haven't faced, fortunately, too many real or prevented terrorist plots since 9/11. But in the instances where we have faced such attacks, as in the Parliament Hill attack, or in Quebec, or things like the Aaron Driver affair, and other conspiracies that have been prevented by law enforcement and intelligence work, I don't see signs of Canadian overreaction or Canadian panic or Canadian misunderstanding of the circumstances. Nor do I see the opposite, which is what is often asked particularly by outside observers of Canada, which is whether Canada is too complacent a country about these kinds of issues.

I think we have, and are capable of having, a mature conversation on national security threats. The challenge for us in having that conversation is that while terrorist and other threats are real, we're not at the epicentre of these threats. We can be impacted by them any minute of the day, but we're not at the epicentre. We're not a European country directly facing the degree of threat that a country like France, for example, or Germany or Italy might. We're not the United States. But we are a country that can be affected by these threats. It's a bit more difficult to judge the reality.

Going forward—and I'll end on this point—I think it's vital that we begin to have a larger conversation about national security. We have been, for the past decade, focused on terrorism as a threat and, from time to time, that's a good focus, but I think it's insufficiently broad for the kind of conversation we have to have going forward. We face other kinds of very significant national security threats that we have to have a national conversation about, including cyber-threats, including the security implications of climate change now and in the future, which are going to impact us and global society. So, the sooner we start having a conversation that is about more than just terrorism, the better off we'll be. I'm sure that Canadian society is capable of having that conversation.

• (1725)

Mr. Sven Spengemann: Thanks very much for that.

Monsieur Therrien, perhaps I could get your views as well.

Mr. Daniel Therrien: I agree that the level of literacy is low. I'll just take a minute to talk about the importance of more transparency on the part of government in this regard.

The green paper, for instance, with respect to the new investigative capabilities, apparently asks Canadians how do they perceive the sensitivity of metadata, because the paper implies that with the answer given by Canadians to how sensitive they perceive metadata, that might influence the kind of legal framework that would follow. That might be a good question to ask, but not before you explain to ordinary Canadians, whose views are sought, what is behind metadata, because people do not have a clue as to what is behind metadata.

I'm just making that point to say it is crucial that there be more transparency. Obviously, there are limits to transparency when you talk about national security, but there is no doubt in my mind that more can and should be done to inform the public, so that the political, societal debate as to the right balance between security and human rights takes place in an environment where the participating public is as informed as possible.

Mr. Sven Spengemann: Thank you.

Very briefly, once it is more educated, what role do you see for Canadian society in, first of all, establishing better security, but also making sure we don't lose our individual rights and societal values that we've worked so hard to build?

Mr. Daniel Therrien: The kind of process that has been started is an excellent point. If there are more educated Canadians who participate in an exercise like the one initiated by the government and the one that you're undertaking now, I think it would make for better laws, and perhaps more importantly, laws that have a greater consensus in society.

Mr. Sven Spengemann: It was just mentioned by my colleague, do Canadians even know what metadata is? I take it both of you agree that education is paramount in establishing a good framework for national security.

Mr. Daniel Therrien: Absolutely.

Mr. Sven Spengemann: Mr. Chair, I think that's my time.

Thank you very much.

The Chair: You have three seconds.

Mr. Sven Spengemann: Thank you, again.

Merci.

The Chair: It is 5:27. We have Mr. Généreux next. We'll give him five minutes, if everyone is in agreement.

[*Translation*]

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

Thank you as well to the witnesses.

Mr. Wark, you said earlier the Green Paper focused a great deal on terrorism and very little on information technology, which today is a constant feature in the lives of all Canadians. We have it in our hands. We're a threat to ourselves, if we want to look at things that way.

Let's talk a little about what you would have liked to see in the Green Paper with regard to the balance between terrorism and new technologies.

[*English*]

Mr. Wesley Wark: Thank you, sir.

My desire would have been—and perhaps it was a little unrealistic in the political circumstances of the green paper and recognizing the fact that this is an unprecedented experiment—to have seen a broader opening statement about the kinds of national security threats that Canadians face now and are likely to face in the future. In part it would be to provide that sense of scope to Canadians, so that they could provide proper feedback about the instruments they might want to see deployed against this variety of threats.

It's one thing to ask Canadians what they think the best responses to terrorism might be. It gets more complex but perhaps more important to ask them what they think is the best mix of tools to deal with this range of national security threats. It does require education, and it does require people to understand that terrorism is just one of a number of national security threats, and it may not be the most important one that we face.

My concern is that if we focus too much on policy, regulation, and legislative changes, which are simply focused on the terrorism problem, we're going to leave ourselves with capability gaps, legal gaps, and policy gaps that are going to hinder our ability to deal with other kinds of threats.

The green paper was designed in large part to respond to election campaign promises and Bill C-51 issues, but I think it would have been helpful if they'd taken a fresh start on the whole question of what are the threats to Canadians that we need appropriate response tools for, and how do we build that balance that the government is so interested in. It's not just about technology. It's about the implication of other changes in our universe, including climate change. This is on the agenda of many of our allies. It's regarded as the number one national security threat for the United Kingdom in their annual threat assessments. It's high on the list of the director of national intelligence's annual statement on global threats that he presents to Congress. We haven't even started to have a conversation about what is the nature of climate change security impacts for Canada as an actor in the world and for Canada at home. The sooner we do that, and the sooner we broaden that discussion, the better off we'll be.

• (1730)

[*Translation*]

Mr. Bernard Généreux: Unfortunately, we didn't receive the text of the presentation—at least I didn't. I don't know whether it was

distributed. I'd like to receive it, Mr. Chair. I have only the text of Mr. Therrien's presentation.

Should the committee so desire, I would like you to provide a one pager on the balance the committee should take into account between the different elements. We can ask people questions.

As the chair said, we're currently in the early stages. Mr. Therrien, you gave a very good presentation. What you said was very interesting. It helped us determine what important aspects should be taken into account. We must shed as much light as possible on the issue. We'll cast the widest net possible to try to understand all the aspects. If it were possible to give us a document like that, I would appreciate it.

Do I have any time left, Mr. Chair?

The Chair: Yes.

Mr. Bernard Généreux: Mr. Therrien, I really liked your presentation. If I understand correctly, Bill C-51 was adopted, but you have doubts about the balance in terms of freedom of expression, or, in other words, people's fundamental freedoms.

Do you think it constitutes a threat to Canadians, in that case?

Mr. Daniel Therrien: I may answer the previous question on the link between the standards of evidence and the risk for ordinary Canadians.

Take people who travel abroad, for example.

In that case, does all the information on every traveller need to be sent to CSIS so that it can identify threats to national security—this involves a standard of relevance—or should we instead provide only the information required by CSIS to carry out its work?

Is there a threat?

We're currently looking at how Bill C-51 was implemented. We've noted that it was used about 50 times last year. We're continuing our review.

Does that mean it has been overused?

Probably not, but it's too early to say. I think the standards of evidence, which allow for information sharing, create a significant potential risk for innocent people, for ordinary citizens who shouldn't be studied by CSIS.

How can we try to find legal tools that would enable the government to protect the population without compromising the freedoms and privacy of ordinary citizens?

I think that's a very important issue for you.

The Chair: Thank you.

The meeting has ended. Thank you for your presentations. Thank you as well to all the participants. We'll continue our work on Thursday afternoon.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

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

Also available on the Parliament of Canada Web Site at the following address: <http://www.parl.gc.ca>

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

PERMISSION DU PRÉSIDENT

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

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

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

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : <http://www.parl.gc.ca>