HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 039 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, December 6, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, December 6, 2016

● (1125)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Colleagues, could I get your attention, please? Thank you for your patience this morning.

Pursuant to Standing Order 108(3)(h)(vi), the study of the Security of Canada Information Sharing Act, otherwise known as SCISA, is continuing. We are pleased to have with us as witnesses, from the Canadian Muslim Lawyers Association, Ziyaad Mia, member of the legal advocacy committee, who I believe has been before the committee before, and Anil Kapoor, from Kapoor Barristers, who is here to offer his insights as well.

Gentlemen, neither of you is a stranger to committees. We have in our routine proceedings, our routine motions, that we hear from our witnesses for up to 10 minutes, and then we will proceed to our rounds of questions.

I will simply go in the order in which you appear on the agenda, as prepared for me by our clerk. Mr. Mia, if you would like to start us off, you have 10 minutes, sir.

Mr. Ziyaad Mia (Member, Legal Advocacy Committee, Canadian Muslim Lawyers Association): Thank you.

Good morning, everyone, and thanks for the invitation to be here today. It's a pleasure.

We're studying the Security of Canada Information Sharing Act, which, as you all know, was introduced as part of Bill C-51, Anti-terrorism Act, 2015, and it is now law.

My general concern with the Security of Canada Information Sharing Act, or SCISA, and the Anti-terrorism Act 2015 is that it was essentially it was broad and unnecessary legislation in essence. The entire piece of legislation, including SCISA, was unnecessary, and the justification for it was not there.

Our national security sector is in need of significant change and reform, and we do need to share information. Those things need to happen in Canada, but Bill C-51 and SCISA were not the correct responses to address those very real concerns that have been festering away. Mr. Kapoor can talk about some of the commissions of inquiry. We can talk about that, but some of our commissions of inquiry have made excellent recommendations identifying the problems in our national security sector, and for various reasons those recommendations have gathered dust now for 10 or more years, even the O'Connor inquiry.

That's the context in which I put my comments forward.

The other piece is that the Anti-terrorism Act, 2015, which, as you see, is called the “anti-terrorism” act, was styled as an anti-terrorism law and sold as an anti-terrorism law, and that's not what it was. It was and is a broad national security bill, and it's quite far-ranging. We can talk about some of that today in this piece of legislation, and I'm happy to talk about the other elements as well, if you like.

Again, it was not necessary, because what we needed to do was reform a number of things in national security. There were specific and focused items that we needed to deal with, and we still have not dealt with those. The Anti-terrorism Act, 2015 does not address those concerns. In some cases, it actually makes those problems worse and actually diminishes the capacity of our national security services to find threats and neutralize them.

In general, I think Bill C-51 and SCISA fail on three essential elements that I like to talk about: legality, accountability, and effectiveness. These are the cornerstone principles that I look at when I'm assessing law.

In terms of legality, that would be a sense of the rule of law, that law and policy need to be compliant with the rule of law and the charter, need to be necessary, and need to be proportional. There needs to be a public justification and an explanation of why we need law, because we don't just make laws that are not required, and we need to be compliant with our international human rights obligations as well. I think ATA 2015 and SCISA fail on legality.

Let's talk about accountability. You're all parliamentarians. All of us went to school here, I assume, and learned about responsible government. To me, that's the nub of accountability: that we have a government that's responsible. Public justification comes into it, so that citizens know why we are doing things. You as legislators explain that and are transparent in that.

Bill C-51 lacks that. Public justification is not sound. It doesn't introduce transparency into the national security sector or into the law itself. The public justification in that process itself was a little broken. Again, in terms of a culture of accountability across government and in the notion of responsible government, that culture of accountability also needs to be in the national security sector. That is clearly lacking in Canada.

What we ought to have is an evergreen process of accountability in Canada, in national security but in government generally. I think that would make our national security system work better, be more accountable, and have public confidence, and at the end of the day, I think we'd be safer.

The last piece in my principles assessment, the lens I look at things through in terms of law and policy, is effectiveness. Is it effective? Does it work? I actually think ATA 2015 and SCISA are not effective in getting to what we want. We want a national security system that identifies threats, keeps Canadians safe, and complies with the rule of law and the charter, and so on. They actually don't make things better. They make things worse.

We spend a lot of money on national security. I put it to you that some of that money is not money well spent, because when we talk about SCISA, we'll talk about how we may be chasing red herrings, collecting too much information, and missing the point. That might make people feel safer, but I don't think it actually makes us safer.

We do need to share information and national security—don't get me wrong—and we do need to investigate threats and get at them, but we need to do it in the right way.

Bill C-51 and SCISA are not the right way to do this. Again, part of effectiveness is necessity. Did you need this law? I'm still scratching my head as to why Bill C-51 was needed. Purportedly, it was in response to the acts committed, one of which was in Ottawa —the killing of Corporal Cirillo—and the other of which pertained to a gentleman in Quebec. Those were terrorist attacks, criminal attacks, but although Bill C-51 was sold in that context, there's really no link to how it addresses those issues.

Those are operational problems. We can talk about that, and those need to be fixed, but Bill C-51 does not address those incidents of 2014.

Again, I come back to evergreen accountability. When it comes to national security, the first thing we need to do is prevent. The second thing we need to do is investigate. You prevent as much as you can, and that's front-end work. Not a lot of people know that. That's either community relations or working to move people off the road to violence.

If that doesn't work—in some cases, obviously some actors are committed—you want to investigate and interdict. That's where police come in. I have some serious concerns about the CSIS disruption powers, but the police need to be involved in interdiction and prosecution. Then we need to review—that's an important part—and reform, to improve the system.

That loop is the evergreen process that I'm talking about. We do not have that working well in Canada, and that's what we need to think about.

I have three minutes, so let me talk a little about SCISA itself.

As I said, information sharing is needed in Canada. We need to do that in policing and in national security, but it needs to be done right.

Mr. Kapoor is here and Mr. Cavalluzzo was supposed to be here. Mr. Kapoor was involved in the Air India inquiry and Mr. Cavalluzzo in the Arar inquiry. Those are two ends of the spectrum.

As a Canadian of Indian extraction, I can tell you first of all that it was not acknowledged for a long time that Air India was a Canadian tragedy. There was a failure of information sharing and institutional egos. That's one part of the problem.

The flip side is Arar, where reckless information sharing led to disasters.

What we need to do is learn from those lessons and get to the middle. Again, I'm not against information sharing, but it needs to be done right. SCISA is the wrong way to do this. It's overly broad, unbounded information sharing.

I usually use the analogy that if we're trying to catch terrorists, it's like finding a needle in a haystack. SCISA is adding a couple of trailer loads of hay to that pile. God forbid there's a disaster, a terrorist attack or something to that effect, and we find out that we had too much information and that what we needed to look at snuck through. What we really need to be focusing on are the real threats.

I have about a minute and a half left, and I know you're going to keep me to the 10 minutes. I'm happy to talk about the details and I'm sure we will, but I'll close with the broader context.

What we really need to do is reform national security, as I said. One piece of that, as you've heard from others, is review, proper review. I know some of our agencies don't have any reviews. Some do. They're siloed. You've heard all of that.

You've heard Kent Roach, Craig Forcese, and others echo those concerns. I really am an advocate. I believe you have my submissions from Bill C-51 previously. I'm an advocate of a unified, independent, national security review agency, the Canada national security review agency.

If there's integration in national security intelligence and operations, you need that counterweight. We can talk in detail about that, but that's one piece that needs to happen, and there are other pieces.

I'll be idealistic and tell you, “Let's repeal the ATA 2015. Let's start again and find those fixed pieces.” If you're willing to do that, I'm happy to work with you on that. If you're not willing to do that, then SCISA really needs significant reform, as do other pieces of Bill C-51. The biggest piece for me is the CSIS disruption power. CSIS should not have those powers, full stop. Those powers should be repealed.

● (1130)

I'll stop there. I'm happy to talk about the rest of it. Thank you for the opportunity.

The Chair: Thank you very much, Mr. Mia. His name was Warrant Officer Patrice Vincent.

Go ahead, Mr. Kapoor.

Mr. Anil Kapoor (Barrister, Kapoor Barristers): Thank you.

First of all, thank you very much for the invitation. It's a pleasure to be before you.

I've had the opportunity to read the testimony from your previous witnesses and I hope not to repeat what others have said.

I want to contextualize my remarks and my evidence before you in the following way. Information is the lifeblood of all intelligence agencies. Without information, there's no intelligence. I'll repeat that: without information, there's no intelligence. In order to effectively have a proper security intelligence apparatus, you must have information.

In these times, you all know that we're swamped with information. Everywhere you go, there is information. The government collects an astounding amount of information on every one of you; on every aspect of each of your lives, the government has information. The ability to maintain all these bits and bytes of our lives poses a huge challenge for our society in the private sector and certainly for government in the public sector.

I can tell you that as commission counsel on the Air India public inquiry, I had a front-row seat to a failure of information sharing that had catastrophic consequences. When I led the evidence of the victims' family members in part 1 of our inquiry, as counsel—I do a lot of trial work and a lot of appeal work—it was amongst the most challenging evidence I've ever had to lead. The impact on those folks was real and remains so today. It remains tangible today.

Similarly, although not as commission counsel, I acted in one of the closed proceedings in the Arar matter. I was involved with some of the folks who did that. I can tell you that the failure to have a proper, regulated flow of information has had similarly catastrophic consequences for that person, but not only for Mr. Arar: it also has had catastrophic consequences for the agencies involved, and if the agencies come before you and say it didn't, I'm here to tell you that it did. No agency wants to be complicit in such a thing.

It becomes even more important now when we have a change in administration in the United States. The CIA is a vast organization that collects a tremendous amount of information and floods the intelligence community with information. If that agency begins to be more aggressive, what are our agencies going to do when the information floats into our data set? How are we going to vet it? How are we going to protect against it?

What I'm most interested in is trying to orient this committee, if I can, to take an approach to this legislation that is, for lack of a better phrase, a grown-up approach. This legislation is immature in a number of ways, and I want to underscore particularly this point. None of us wants the agencies that are charged with protecting us to be starved of important, necessary information. None of us wants that, but we all must also want a refined approach to information sharing that, in my respectful submission to you, more properly balances privacy with necessary information sharing. This legislation doesn't. You've heard from my colleagues, Professor Roach and Professor Forcese, and you've heard from the Privacy Commissioner. The evidence of all three of those folks I agree with entirely.

I want to underscore something about one of the problems with this piece of legislation. It is about a lack of accountability. I mean particularly this. As I said at the outset, lots of information is gathered on each and every one of you. Under this legislation, one of the problems is whether or not the phrase “activity that undermines the security of Canada” is constitutionally compliant. In other words, is it so vague that it would be a violation of section 7 of the Constitution?

● (1135)

Leaving aside esoteric notions of legal theory, the practical concern is that vagueness in that legislation is a gateway for bureaucrats to pass information. Also, it's deployed almost entirely by representatives of the executive branch, without any serious prospect that anyone outside the executive would know what's happening or how it's being applied.

For example, not one of you will know that information about you is passed from one of the 17 agencies to CSIS. You just won't know. You'll have no recourse. Even assuming that you had some information somehow, there is no place for you to go with it. There's no specialized review body. There's no court process. There's no way for you to hold the government to account.

I know we have limited time, but I want to conclude my opening remarks with this notion that I urge upon you with as much force as I can: fundamental to any democracy is the ability to hold government to account for its actions. That can mean in court, at the ballot box, at an administrative tribunal, or in a review or oversight body.

However, blind faith and trust in government is not a virtue. Blind faith in CSIS, the RCMP, and all of these other agencies is not a virtue.

Instead, each one of you must have at your disposal the ability to call government to account for its excesses. Given the ubiquitous nature of information and the extent to which it reveals our tastes, preferences, and inner thoughts and beliefs, any regime that authorizes the sharing of information must be refined to regulate sharing that is necessary to protect national security. All of this requires—in my respectful submission to you—more conservative definitions and a more conservative approach to protecting information and ensuring that information that's necessary is delivered to the agencies so that they can discharge their duties.

In closing, then, the relationship between the citizen, his or her information, and the various government agencies is something that needs to be recalibrated in this piece of legislation.

There are a number of different ways it can be done. You have heard from some witnesses who have indicated changes in definitions. Those are all useful. I appreciate, though, that it may be beyond the remit of this committee. The notion of an independent reviewer is necessary, as well, as part of the framework of oversight and review in the national security environment. A committee of parliamentarians also may be able to do some work in this area, depending on how that committee is structured and staffed.

Really, in this moment when we have such upheaval around the globe, when various intelligence agencies are forwarding information to our intelligence agency, and when information is being domestically being harvested, we cannot not take this opportunity to apply a rigorous standard. If we don't, sadly, what might happen are events like the two horrific events that have happened already: Arar for the agencies and for Mr. Arar, and Air India for all of those folks.

Those are the comments I wish to open with.

Again, I thank you very much for the opportunity to address you.

● (1140)

The Chair: Thank you very much, Mr. Kapoor. That was interesting testimony, and I'm sure we're going to have a very engaging discussion.

We're going to start with the seven-minute round.

Mr. Long, you're up first.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for coming today. It is a very interesting topic.

Mr. Mia, I want to start, I think, in a wide-ranging way.

I've done some reading of some of your articles in the paper and some other things. In one article I read, you felt or you suggested that Bill C-51 is so flawed that it should be scrapped. Personally, I question whether something like that should be scrapped, so I just want an initial comment. Do you feel that we should just throw that out and start again, or do you feel that we are able to tweak it and make adjustments?

Mr. Ziyaad Mia: Thank you for the question.

I think the bill itself—or rather, the law now—was so fundamentally flawed that whatever redeeming qualities it might have had were outweighed by the flaws. I usually use this example. If I bought a house that had a crumbling foundation, I wouldn't throw a few coats of paint on and say, “Let's keep this.” I'd say, “Let's start again.”

Let's go through some of the essential elements of Bill C-51.

The CSIS provisions give CSIS secret disruption powers to essentially disrupt people's lives and take actions that could result in disasters, as Mr. Kapoor said. They are a non-starter in a democracy. Things could happen to people, and they would never have legal recourse. They happen in secret. They would never see the light of day.

In a criminal context, police get warrants and they do have secret wiretaps, but ultimately it sees the light of day. You have a day in court. That's essentially our system. When the state acts against you, you have the right to defend yourself. When CSIS acts against you under these disruption warrants, you will never know and you will never have the right to defend yourself. Whether you're guilty or innocent, you won't have a shot to defend yourself.

Let's talk about promoting and advocating terrorism. First of all, the definitions in there are loose to begin with. The Criminal Code already has always had counselling offences, so when you're involved in criminal activity and encouraging it, you can be caught.

The Anti-terrorism Act, 2001 introduced criminalized actions that were removed from action, such as facilitating terrorism or encouraging someone to start committing a terrorist act. I had critiques about that, but it was still close enough to the act. In criminal law, what you want is to criminalize the act. Terrorism is essentially violent acts. They want to kill someone, so let's say it's killing someone. If I facilitate you to do that by encouraging you, giving you money, talking to you, I can be caught there. As a democratic society, we want to capture the act or something close to the act. If we get far from the act, we're starting to stray from our criminal law and democratic principles and we're starting to criminalize speech. What I learned in law school is that you don't pass redundant laws.

In the Anti-terrorism Act, 2015 we already had facilitating, which is close to the act. Then this must be something further removed from that, so now we're getting very close to criminalizing speech. I'm not saying I support people who say things that encourage terrorism. Of course, we all condemn that, but we live in a society where we tolerate some of that offensive speech.

The Immigration and Refugee Protection Act amendments in Bill C-51 essentially rolled it back, and Mr. Kapoor can speak to this in more detail because he is a special advocate. The Charkaoui decision said that in the security certificate process, secret proceedings where a judge sat alone with a CSIS lawyer were essentially unconstitutional. They introduced special advocates to represent the interests of the named party on the security certificate. Bill C-51 essentially rolls that back. IRPA was amended to say that the special advocates don't have access to all the information. It kind of undoes what the Supreme Court has told us.

Those are three pieces of it.

Let's talk about the no-fly list. We can debate till the cows come home whether no-fly lists—

● (1145)

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): I have a point of order.

The Chair: We have Mr. Jeneroux on a point of order. Just make sure it's a point of order.

Mr. Matt Jeneroux: Yes. I just want to make sure that we're sticking to the information-sharing aspect of it. We're going down a long list of Bill C-51. I would like to think that we could focus on just the scope of what the committee's looking at right now.

The Chair: Your point is taken, Mr. Jeneroux.

I do allow members of the committee to ask broad-ranging questions, but, Mr. Mia, please try to stay focused on what the committee's mandate is in this particular study, which is the review of SCISA.

Mr. Ziyaad Mia: I'm happy to do that. I understood that Mr. Long asked me about scrapping Bill C-51, but I can stick to SCISA.

In SCISA, as I said, information sharing needs to happen. We see the extremes. We see Air India and Arar. We see both sides of it not working.

It needs to work, but as Mr. Kapoor said, it speaks of activities that undermine the security of Canada, and then it lists a number of things in the act, which I'm sure you've all seen, and that is not the list. It is an open-ended list, given content by bureaucrats across government. Those are just suggestions about what undermines the security of Canada; it could include other things.

Essentially, the definition is the heart of the bill. You start with a fundamentally flawed definition and then you start to share information. There are no controls on how that information is shared. The door is open for sharing with foreigners, and that could include Saudi Arabia, and now, with the Trump administration talking about torture, it could be there.

Then I'll point out to you section 9. Section 9 says that when someone shares information and it harms a Canadian or some person —but let's say a Canadian, as in the Arar case—they're immune from paying out compensation or being sued for it.

It's essentially a busted bill. What we need to do is say that information needs to be shared, that it needs to be reliable, that it needs to be in compliance with the charter and the rule of law, and we need to make sure that CSIS actually works with the RCMP to move intelligence into evidence and get real terrorists off the street. The CSIS amendments actually are counterproductive to that.

● (1150)

Mr. Wayne Long: Okay, I'll just jump in. Thanks for that. I know that question was wide-ranging, but I was trying to focus in.

Obviously we're trying to find the balance between government's right to know and people's privacy. We grapple with that.

There are some out there who believe that the Privacy Act should take precedence over SCISA. Do you believe it should?

Mr. Ziyaad Mia: My reading of it is convoluted. I believe you've heard Kent Roach, and I concur with Kent and Craig Forcese in their testimony that it's a bit of a dog's breakfast. Nobody is entirely clear, because the act uses very general terms—"will comply with" laws unnamed.

Then you read the green paper. I don't want to quote it right now because I don't want to delay us, but essentially it says we can share information subject to any prohibitions in law without naming those laws.

The suggestion is that the Privacy Act is there to protect people's privacy. You read the green paper and find that it says the Privacy Act has a number of exceptions, and rightly so. One is lawful authority: the police can come.... Then the green paper says that SCISA is considered to be a lawful authority.

Essentially, the Privacy Act is nullified by that reading. If that's the legal interpretation that government lawyers and staff have of SCISA, then I'd say the Privacy Act protections are not there.

The Chair: Thank you, Mr. Long. We're well past seven minutes.

Thank you, Mr. Mia, for bringing this back on track. It's much appreciated.

Mr. Jeneroux, you have up to seven minutes, please.

Mr. Matt Jeneroux: Perfect. Thank you, guys, very much for being here today. It's important. We have limited time, so I want to make sure we're staying on the topic. We can then make this part of our report for SCISA. I appreciate your doing that.

I'd also remind my colleagues on the other side of the room that in fact Bill C-51 was supported by the Liberals at the time. Granted, I don't think any of you were there at the time, but it was certainly supported on your side.

The Chair: I'm the only one on the committee who was there.

Mr. Matt Jeneroux: Yes.

Anyway, getting back on topic, I want to talk to you a bit about the Five Eyes and our allies across the world.

Given that we're a member of this group, and in looking at the threats towards national security, do you believe that these types of allied relationships are important to better protect Canadians?

Mr. Ziyaad Mia: Is that to one of us or both?

Mr. Matt Jeneroux: It's to both.

Mr. Ziyaad Mia: Obviously we live in a globalized world on all sorts of levels, including intelligence and security, and the threats that are out there are obviously globalized threats. It is important that we have relationships, but I believe it is also important to keep in mind our values in how we interact with the Five Eyes allies.

Saudi Arabia is not a Five Eyes partner, but I've used Saudi Arabia or states like this as an example. SCISA says that activities that undermine the security of another state hit the radar here. Does that include Saudi Arabia? If we are talking about Raif Badawi or about trying to change the government in Saudi Arabia, does that get people here on the radar? That's problematic, but I'll leave it for a minute and go back to the Five Eyes.

We need to share with those allies. One real problem now is that Mr. Trump says that waterboarding is just the start, and that he will kill the families of people who are suspected terrorists. Essentially, he is negating U.S. obligations under domestic and international law. The U.S. is our biggest partner in terms of information sharing on national security. I would be worried about how we protect our values, which are to share but to comply with the charter, the Convention against Torture, and the rule of law, essentially. Canadians need to interact with the world, but we still need to be Canadian. We need to take our values with us. Those are important relationships, but we need to be careful about how we engage and what we share.

I'll give you Arar as a classic example where we were sloppy in our sharing, and that led to a problem.

That's my answer—we need to do it, but we also need to be very conscious of injecting our values, protocols, and protections into that interaction.

● (1155)

Mr. Anil Kapoor: We have to be a robust part of the Five Eyes. Culturally, we are all connected. Broadly speaking, we have the same sort of democratic structures and geopolitical positioning. I think the Five Eyes is a crucial alliance—if I can call it that—and we have to be a player in it.

Mr. Matt Jeneroux: Great.

Mr. Anil Kapoor: I think you asked whether it was a good thing. I think it's a good thing.

Mr. Matt Jeneroux: It's safe to say that you both think it's important that our Canadian national security organizations...that we have the same tools as our allies, essentially. Can I sum it up like that?

Mr. Anil Kapoor: I would say that it's important to participate and to be involved in it.

Some of these countries have threat levels that are radically different from ours. For example, the threat level in the U.K. is much higher than the threat level here. Their tolerance for incursions on the ECHR, or what we would call charter rights, is calibrated differently as a result of the threat environment.

If a state has, let's say, indefinite detention for 14 days, that doesn't necessarily mean that we ought to deploy that tool, even if they are Five Eyes. When it comes to information sharing with our Five Eyes partners, I think that's crucial, but the tools that we deploy are tools that are made in Canada and relevant to the Canadian threat environment.

Mr. Matt Jeneroux: Can you comment on some of the other countries within the Five Eyes and some of their information-sharing agreements that you either see as crucial that we adopt here in Canada that we should stay away from?

Mr. Anil Kapoor: In the case of the U.K., not a lot is known about the internal ministry arrangements. Much of it gets done at the ministerial level. There is some control of information by various administrative bodies, and certainly the independent reviewer in the U.K. reviews the extent of information-sharing.

In Australia and New Zealand they have information-sharing arrangements between, for example, federal and state police and ASIO in the Australian environment. Information does, then, get to be shared.

From a comparative law perspective, whether their particular tests for sharing information comply with ours or not, I couldn't tell you offhand. I can find out, as could one of your clerks, I suppose, but my view would be that the test of relevancy is too low in our statute. The test should be that it be necessary, as Daniel Therrien mentioned in his evidence.

I want to round out by responding to something that some of the service witnesses said on this question, and that I think Scott Doran from the RCMP said as well: that there's the sense that no one is going to know in some other agency what CSIS's mandate is, so how do I know whether it's "necessary" for CSIS? How am I going to divine that?

If you look at their testimony, you will also see that they talked about these agencies' having sectors or groups within the agency for whom there's going to be training on how to comply with the statute. Well, if there's going to be training on how to comply with the statute, you can train them to understand what "necessary" means for CSIS. It's not rocket science. CSIS does it; they deploy it. Somebody sitting in Health Canada, then, or one of the other agencies—CRA, let's say—can learn what the mandate is and can apply it. It's not as if it's mysterious; it's just a matter of training.

The Chair: Thank you.

Mr. Anil Kapoor: I'm sorry; I think I took too long.

The Chair: No, not it's fine. It's a great conversation.

We now move to Mr. Blaikie for seven minutes.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much for being here today.

When we talk about trying to strike the right balance between the need to share information for security purposes and the need to protect Canadians, I think it's often easier for folks to understand the risk of not sharing enough. You can understand the idea quite readily and in an abstract way that there's a threat and that if the left hand doesn't talk to the right hand and they don't get the information on time, then that threat is allowed to get through.

You've referred to the Arar case, and I'm sure most of us are familiar with the broad strokes of that case. Could you guys help us by explaining a little more concretely some of the details of that case? It might be helpful even to speak more generally about what the risks are. In what ways can unrestricted information sharing end up posing a threat to Canadians?

I think many people think that if you don't have anything to hide and you're not up to anything, then it shouldn't matter how much information they're sharing about you, because what possible harm could come of innocuous information? If that's not the case, maybe you could just help....

● (1200)

Mr. Anil Kapoor: Very briefly, then, and I'll let my colleague pick it up, the concern here is that you have two ends. You have the relevancy test for passing information over, and it's information relevant to activities that undermine the security of Canada, meaning the sovereignty, security, or territorial integrity of Canada. I sense that it's an incredibly broad definition, and the examples that are given are simply illustrative; they're not closed sets. Even if they were closed sets, even within them they're pretty broad, so you have broadness on both ends of this equation.

The concern I have with robust information sharing along these lines is that there's no real control for false positives. I appreciate that when it gets to the service—let's take the service as an example—they will apply their analytics and will ask whether this person is really engaged in something that undermines the sovereignty of Canada, whatever that means, and whether they'll take any national security action against the person.

However, it's rather like this: once they're on you, they're on you, and they just don't let go. It sits in the database, and there are no real retention issues spoken about here in this legislation. There are, at the service; they have their own retention standards, but what I'm concerned about is that the agency that sends information on, the transmitting agency, doesn't really turn itself to false positives. The "necessary" test would impose some rigour that at least has the prospect of doing so more efficiently than a relevancy test would.

Part of the training for those folks who are in the transmitting agencies is to really have some understanding of national security and to appreciate the ease with which there can be false positives. If you're alive to that possibility, then you'll be vetting for it, and the risk is diminished on the false positive side.

That's what my concern is.

Mr. Daniel Blaikie: Am I right to hear, then, that you're suggesting that a necessity test is as important as a screen for false positives?

Mr. Anil Kapoor: Yes.

Mr. Daniel Blaikie: Do you think it matters whether that happens at the transmission end or if there's a duty on the part of CSIS to only receive into their databases certain kinds of information? Do you think that would be just as good, from the point of view of screening for false positives?

Mr. Anil Kapoor: I think it ought to happen at the transmitting agency side, and it will happen anyway at the surface.

Mr. Daniel Blaikie: Right.

Mr. Anil Kapoor: They will vet and employ analytics in any case, but in order to maintain protection for privacy rights, it ought to happen at the transmitting agency as well.

Mr. Daniel Blaikie: Mr. Mia, do you have some examples of how, concretely speaking, information sharing can impact Canadians?

Mr. Ziyaad Mia: I concur with my colleague's comments. How do we find reliable information? That's what ought to be shared. That reduces the hay pile, for one, so we can get at the needles. The other piece is that then we avoid mistakes.

I'll give you some hypotheticals. Let's look at the definition, as Anil's pointed out. The real risk is that we've cast the net so wide when it was styled as "terrorism". Terrorism is item (d) here. That's not even a Criminal Code offence, so that's something that needs fixing. Let's assume that's one piece, and we can agree with that. Nuclear proliferation and all of those are fine. Those are national security issues. However, then it's so broad that it's open-ended. Who hits the national security radar? If you see my submission, that little chart shows whole-of-government information sharing, so all these disparate decision points across government are making a low-threshold test to put information into this bucket. Someone may say, "Well, I have nothing to hide", but in today's world, with data management....

Let's use my Saudi example. You're involved in trying to get Raif Badawi out of that hellhole in Saudi Arabia and you go to protests. The Saudis' intelligence says, "Some of these people are causing trouble for us." Obviously they have a very low threshold of what's undermining their state security.

These countries usually see everyone as a terrorist. You or I are going to a protest, starting a petition against Saudi Arabia, boycotting Saudi oil or something, and we get picked up on their radar, so now we're in this bucket of data. It isn't just that piece of information, but it's the data crunching now as well, because it's whole of government. Now somebody might say, "Well, you know what? I've flagged someone of some suspicion at that low threshold, so let's see what else. Let's see what FINTRAC has on this person." Those points are then put together and may create a false positive suspicion, so it's not clear, but there's a lot of data mining and data crunching going on through analytics.

Then we may share. This is the Arar-type situation. We may then say, “Here's the Saudi threat profile of protesters in Canada, and let's share it with the United States or with Saudi Arabia.” Then, after the fact, we may say, “Well, this was a mistake.” In our case, the agency may say, “Well, Ziyaad's cleared; expunge him from our CSIS database.” First of all, you're now in a bunch of other Canadian databases, so who's controlling that? The rules on retention and expunging are not clear. They're not even not clear; they're not there.

Then the other piece is, who's reeling back the information? In today's world, you see what a tweet does. You can't reel back a tweet, and this is much worse than a tweet. The worst thing would be if your name shows up and you're flagged and you go somewhere. Arar showed up in the U.S., and he was sent to Syria. Many Muslim Canadians travel to Saudi Arabia for a religious ritual, but if you now show up and land in Saudi, everything's integrated. Your passport's scanned and you're red-flagged there, and there's a real risk you won't just be sent back: you're going to be kept there, and that's worse than being sent back.

Those are the types of risks with data mining and harvesting all sorts of information under this very broad definition. What does “undermining the financial stability of Canada” mean? We make the debate about people who are involved in activities that criticize Canada's policies or whatever, and that's fine. We should have that debate. My worry is that this definition is going to put all sorts of innocent Canadians onto the national security radar when they should not be.

● (1205)

The Chair: Thank you. We're going to have to move on. We're well past the eight minutes.

Go ahead, Mr. Saini, for the last of the seven-minute rounds.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you, gentlemen, for being here. I want to pick up on a point that both of you have emphasized throughout your testimony, and that is the amount of information.

I understand, Mr. Mia, that you sent in a brief from the Canadian Muslim Lawyers Association.

Mr. Ziyaad Mia: Yes.

Mr. Raj Saini: In it, you talked about a term that struck me: “a multiplicity of decision points”. Let's say, for example, that there are 17 government agencies and 111 departments, and foreign actors are also involved. Let's say, then, that the information was necessary. We clean that up, and it's not relevant anymore. It's necessary, so it goes to three, four, and maybe five government departments. Each department is going to retain that information and pass it on.

My question to you is—and you mentioned it a bit earlier—what do you recommend as a disposal mechanism to make sure...? When you talked about “expunging”, you said there was a problem if four or five different agencies or four or five different departments have that information. What could you suggest to have that information expunged or disposed of so that we don't get that multi-layering that you spoke about earlier?

Mr. Ziyaad Mia: That's a tough nut to crack, because I'm not an IT guy. I'm an Indian guy, but I'm not an IT guy; I'm probably one of the only Indian guys who doesn't know anything about computers.

Voices: Oh, oh!

Mr. Ziyaad Mia: I think the one of the solutions is to have a sort of centralized control over it. I recommended in the submission that there needs to be some centralized control of information sharing. The departments could do their piece, but somewhere in government —maybe in Public Safety—there would be someone overseeing all of this. The Privacy Commissioner and SIRC and everybody will do their audits, and we're calling for a national security review agency. Those will be the watchdogs, but someone in government needs to be shepherding the whole thing by asking what's being shared, what are the thresholds that are the same across government, and then asking, “Are we doing this and is it consistent?” Then if there's a false positive or something, that person or that entity within government would be able to issue instructions across government to say, “Search your databases for this record and this person and remove that information.”

It's not a fail-safe method, because government is so huge and people forget and whatnot, but it still leaves us with the real problem back in the world, because if it has left here and has gone to the Five Eyes or to Saudi Arabia, we'll never get it back. We have no control over how they deal with that information. We don't even have control anymore to tell them that they have to use that information “relevant to these issues”. They could use it for some other purpose completely.

I think there's a possible fix, but in today's big-data world where there is so much information, it's very hard to clean that up. I think one attempt would be a centralized review, and then a way to issue instructions across government.

Take, for example, the no-fly secure air travel passenger protect program. I don't even know what's happening, because it's shrouded in secrecy. We can debate about whether it works, but let's say you get the passenger manifest and you check for the names. If none of the names are on the flight and the flight lands safely, why should that information be kept?

I remember Bill C-17 years ago, when they introduced the regulatory framework for the no-fly list. That information could be shared around and kept indefinitely. I do not want the travel data of all Canadians flying on Canadian airlines kept in government databases to then be mined for travel patterns. We know that CSIS and CSE have played funny with metadata and and have crossed the line.

You have metadata and travel patterns, and you might be pulled in here now. You can see that all of this is there in government databases, and the preamble to the act says that there is the ability to collate. That, to me, is data mining. That's what it's enabling. Clearly, that's what part of it is. We do need to do some of that, but again, the net is cast so widely.

My starting position is that Canadians' privacy needs to be protected. If the government doesn't need to have information about you to do business with you—to vet your taxes or your health records—they should not have it as a starting point. If they have collected it in this process of security screening, once you're not a suspect or the flight has landed, etc., they should expunge that information. That's how we minimize the databases and avoid errors.

● (1210)

Mr. Raj Saini: Now we have an international issue, because as part of Five Eyes and as part of our international tax treaties and other things that we're doing, we may have an agreement with one country that may have an agreement with a tertiary country or a secondary country that we don't have an agreement with. If we send information to the country we have an agreement with, how do we make sure that they use the information specifically for what it was sent for, and not allow it to be sent to another country? Is there any way to do that?

Mr. Anil Kapoor: Generally speaking, in intelligence matters there is an implicit caveat. When the service passes intelligence—let's say, to MI6 or MI5—there is an implicit caveat that it remains the property of the service and will not be passed on.

Mr. Raj Saini: I ask because you mentioned earlier that whenever we do something, we have charter provisions, but that threshold is different in England because they have a higher threat matrix. In the United States you would have a higher threat matrix also. Maybe the information we sent met our threshold, but it might be a little bit looser or a little bit more exaggerated in other countries where the threat matrix is higher.

Mr. Anil Kapoor: Generally speaking, as I said, intelligence agencies tend to abide by this notion of an implicit caveat. There are also explicit caveats that are placed on intelligence that will say "Not to be used for...", and you fill in the blanks. We rely upon our partners to follow those caveats, as they rely upon us to follow theirs. There is a mutuality to it.

I think that when you step out of the Five Eyes, European intelligence agencies will probably follow the caveats as well, for the most part. When you get further afield, it's much more difficult to ensure, but within the Five Eyes I think caveats are well respected, and everybody gets the protocol.

I want to add something very briefly. I'm going to part company with my colleague here on the question of retention, and I'm going to do it in this way.

To the extent that the service properly receives—and I underscore "properly"—information about national security threat information, I don't think it's wise for the service to destroy it. I don't think it's wise. Today it may not mean much, but 10 years from now or five years from now, when circumstances change and you're continually revising your analytics, you need to have a rich environment to be able to stay on top of the threat environment.

● (1215)

Mr. Raj Saini: Do you think there should be no sunset provision to say that information should be held for a certain period of time? Otherwise—

Mr. Anil Kapoor: I think that with respect to information that's properly in the hands of the service—and I underscore "properly"—they should be able to maintain their files.

Mr. Raj Saini: But didn't you mention earlier that it would not be a virtue to trust a...?

Mr. Anil Kapoor: Well, no. I do accept that, but I'll give an example.

Let's say that you destroy a piece of information, and three years later. something happens. Perhaps a bomb goes off somewhere.

Where was the information? Why did nobody know about it? Well, you've destroyed the information or you weren't able to stay on top of that particular threat circumstance.

I think it would require extraordinary circumstances to destroy information that the service properly has, because they have an ongoing national security mandate.

From my perspective, if the service takes action and they do something and pass it to the RCMP for an investigation, it's going to end up in a court process, but I think it would be wrong to put an arbitrary time frame on how long the service should maintain it.

The Chair: Thank you, Mr. Saini and Mr. Kapoor.

We'll now move back to Mr. Jeneroux, and now we're in the five-minute round.

Mr. Matt Jeneroux: The tone of your voice, Mr. Chair, suggests you're surprised that I would ask a second round of questions.

The Chair: I'm shocked, actually.

Mr. Matt Jeneroux: I'll try not to disappoint.

Thank you to both of you.

Section 4 of the Security of Canada Information Sharing Act sets out a number of principles for information sharing under the act, including the following:

> (c) entry into information-sharing arrangements is appropriate when Government of Canada institutions share information regularly

I want to get to some of the basic elements that you believe should be part of SCISA. Could you help lay those out for us as we debate this further?

Mr. Ziyaad Mia: In terms of the principles in those arrangements, you've heard from others that reliability is a core principle. We've talked about relevancy versus necessity. I'd concur with my colleagues Roach, Forcese, and Anil about necessity being a threshold. I believe Professor Forcese talked about "materiality". I think that gets us more reliable information, so changing that standard would help, as would ensuring in those arrangements that there is rigour in the sharing, that we're looking to those criteria, and that there is necessity as well.

We talked about the life cycle of data. I'd like to see something about that. I don't entirely disagree with Mr. Kapoor. Yes, relevant information needs to be maintained, but a lot of irrelevant information may be pulled in, especially in the case of SCISA. That is what I'm concerned about. Therefore, I think those arrangements should also have an eye to the life cycle. How is data shared? How is it used? What happens to it afterwards? Also, is there some tracking of where it has gone within government agencies?

I come back to my suggestion that there be some kind of stickhandler in government who is overseeing this and setting standards in creating these arrangements, maybe with a model agreement or an arrangement that comes from the centre and has gone out to agencies.

Mr. Anil Kapoor: On this issue about necessity and the nature of the information-sharing agreements, I don't necessarily agree that materiality is a workable test. I am saying that because I think necessity is much easier to manage.

Materiality brings into relief not only what you know at the transmitting agency but also what the recipient agency or the requesting agency knows, because under this legislation the service could request from any one of the other 17 agencies. It's unworkable to say that the transmitting agency should know the service file. We have one intelligence agency, CSIS, so if CSIS thinks.... Pick somebody else, such as the CRA or the Department of Health. Let's say that for some reason CSIS thinks the Department of Health has important information for their case. The people at the Department of Health aren't going to know the entire CSIS brief, nor is it practical for them to know it, but they would need to know that to execute on materiality.

Necessity, by contrast, I think is more modest. The service can warrant why it's important to them, and Health Canada can then do its own due diligence on its own side. Materiality is just a very broad concept that brings it into a whole mosaic that I think is just not practical for all the various agencies to transact in parallel.

● (1220)

Mr. Matt Jeneroux: Okay.

I want to jump into one of the questions that has been prepared by the Library of Parliament. I'm curious, Mr. Kapoor, to have it answered here. It's about the concerns addressed by the commission of inquiry into the Air India flight and how CSIS failed to share information with the RCMP about facts related to the investigation. Does SCISA respond to the commission's related concerns on that?

Mr. Anil Kapoor: It certainly allows for sharing of information, but this problem that existed in terms of Air India was really the result of a very immature approach by the RCMP and CSIS to their respective mandates. Of course, keep in mind that CSIS was a baby at that time. It had just been created.

The infrastructure problems and the lack of coordination that we saw in Air India have to a large extent been ameliorated by changes in the way in which the RCMP and the service deal with each other on a regular basis. That problem is working itself out, and the agencies are much closer and have a much more mature relationship today than they did then. This statute doesn't really affect that. It's going to happen anyway; it happened before this statute. The statute doesn't really enable that. It's just kind of more stuff, more information, but the real rigour happens in the ways in which those two agencies have decided to change how they coordinate with each other.

The Chair: Thank you very much.

We will now move to Mr. Lightbound.

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you very much. This is very interesting testimony.

I only have five minutes, so I'll ask you to try to keep your answers as short as possible.

My first question is in regard to the institutions that can send or receive information. In terms of your interest in Bill C-51, in regard to having so many institutions that can send information—from the Yukon Surface Rights Board to the federal Consumer Agency of Canada, which I didn't even know existed—has the case ever been made that they actually have information that is somewhat relevant to national security? Has there ever been a case made for the 17 agencies that are listed in schedule 3 that they have anything to do with it?

For instance, we have the Department of Finance, which deals with national security. It's on the recipient end. Has there ever been a case made for them to be on the recipient end of SCISA?

Mr. Ziyaad Mia: I'll take a quick shot at it, and then I'll let Mr. Kapoor handle the rest.

On the all-of-government sharing, clearly some government agencies may have information that would be useful in national security investigations. In terms of casting the net that wide, I don't know if a case has been made that it's just every conceivable government agency. That would be the troubling thing—that it would be cast so wide—but I wouldn't say that no other agency, other than national security agencies, would have information. Clearly there may be information in other agencies that may be useful in a national security investigation.

Mr. Anil Kapoor: To answer the question, there's a bit of irrationality going on here. The primary actors for national security are the service, the RCMP, the CSE, and then National Defence and the CBSA. Let's call them the main actors.

When you drill away from that and look at the Department of Transport, they may have a national security remit, but it would be sort of a knock-on remit, if I can put it that way. Let's say CSIS has intelligence about some weakness to some rail system somewhere, or somebody's going to blow up something at a rail system. They would then want to activate the Department of Transport for assistance, and our provincial partners as well.

It seems to me that it should be about information getting to the main actors in national security, because that's what this is about. It's not just simply the service giving information to the CRA to help them collect your taxes.

● (1225)

Mr. Joël Lightbound: Would it be worth our while examining schedule 3 to perhaps make it narrow, which I don't think was done previously?

Mr. Mia, you mentioned section 9 and immunity. When Ann Sheppard, the senior legal counsel at the Department of Justice, testified here, I asked her what that provision actually meant. She said it was designed to encourage "responsible disclosure" and "charter-compliant disclosure". I fail to see how granting immunity achieves that. She also mentioned that this position was meant to shield public servants and was never intended to shield the crown from prosecution.

I just want to know if you agree with that interpretation of section 9.

Mr. Ziyaad Mia: I don't agree with that. The section says "any person". My concern with this....

I would agree with the first statement, that this act purportedly encourages information sharing. You don't need section 9 to do that.

I didn't have a chance to read her testimony, but the other piece is good faith. They may hang their hat on that, saying that these aren't malicious shares, but you can be negligent and act in good faith as well, in my view.

I think it includes the crown. I think it's pretty broadly worded. I think it's disingenuous to suggest that this facilitates sharing or—

Mr. Joël Lightbound: Encourages responsible disclosure.

Mr. Ziyaad Mia: —encourages that. I think civil servants should be acting in good faith all the time, and I think they should act within the law. When they step outside those bounds, the government should be held accountable. That would be my position.

Mr. Anil Kapoor: Really, this is just an indemnification issue. The government has to be responsible for mistakes. Individual persons are on this team and are transmitting information. Just by indemnification, the government can solve this problem so that they're not hung out to dry. From my perspective, we can get rid of this provision and have proper indemnification agreements.

Mr. Joël Lightbound: Okay.

I have a last question for you, Mr. Mia. I think you talked about having a national security agency review. As it pertains to our study of SCISA, if we were to recommend having an agency or perhaps the Privacy Commissioner look at the information sharing that goes on pursuant to SCISA, how would you envision that this could be set up? Do you have any ideas in mind for us as we deliberate on what we want to recommend?

Mr. Ziyaad Mia: The Privacy Commissioner plays an important role because of the privacy protections, but the Privacy Commissioner is not a national security expert. That department does not have that expertise. That would be one of the issues. Would they have the clearances to get at everything and look at everything? That would be a concern, although certainly the expertise of the Privacy Commissioner is welcome.

The recommendation I've also made is that other than the committee of parliamentarians, we need to have one unified, arm's-length, well-resourced review agency—some call it super-SIRC, but I like it call it the Canada national security review agency—to oversee all of national security. That organization could play a role in reviewing information sharing as well. The other piece, which I don't think would be touching as much on information sharing as on the law policy side, is the independent reviewer of national security law and policy.

The last piece I've suggested is that within government itself, probably within Public Safety and reporting to the minister, there should be some sort of information-sharing czar to oversee all of it. When you have all these pieces moving, we could actually have a national security disaster if something weren't caught or we could have a disaster when mistakes were made. Someone in government who's actually a bureaucrat could be overseeing all of this and reporting to the minister.

Those would be all the pieces, I think. There would be one from the public watchdog side but also one in government to make sure all the parts are moving well.

The Chair: Thank you.

Go ahead, Mr. Kelly, for five minutes, please.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you, Mr. Chair.

Mr. Mia, in the briefing material you provided, there was a list of 16 questions that you had about the material. Your briefing was dated March 2015.

Have any of these questions—and if so, which ones—been answered since the time of your briefing?

● (1230)

Mr. Ziyaad Mia: I'll try to be quick without going through the whole list.

I think the amendments were essentially on lawful advocacy. I believe there was one other amendment, and it was to section 6, which says that information can be shared for any purpose. The complaint I had was that this was essentially completely unwarranted, even in this broad act. Once the recipient agency has it, it can then be shared anywhere, including with foreign agencies, for any reason. There was some amendment to that.

I don't think those amendments essentially changed the core of my concerns. I'll just quickly go through them.

The word “lawful” was dropped on the advocacy. That is fine, because the complaint was that people can be unlawful but not violent, just civilly disobedient, and do we want to pull those people into the national security net? I don't think any of us want to do that.

I believe that Professor Roach and Professor Forcese raised the issue of violence. I concur with them that you need to clean that definition up to make it a little tougher. It's a little loose now. It needs to mirror the Criminal Code's lawful exemption, where advocacy, protest, and dissent that are not violent are covered. They could be unlawful but not violent, and we would all probably agree on that.

I don't think the other amendment on section 6 actually changed anything. Some words were changed to say that sharing is neither allowed nor prohibited but must comply with law. The question was, which law? The green paper's legal interpretation of the Privacy Act is that SCISA is a lawful authority to override the Privacy Act. Essentially, section 6 still says that you can share with anyone, and it's not even linked to the purpose of SCISA anymore.

Essentially, those are the two amendments. I don't think they change my concerns with the bill.

Mr. Pat Kelly: They more or less all stand—

Mr. Ziyaad Mia: Yes.

Mr. Pat Kelly: —as prepared in 2015.

I guess I'll let either of you comment further. You've both already had some comment on the issue of effective oversight for abuse of information-sharing power.

I remain concerned about how any government agency's power is used, and I'll let each of you have a word on that.

Mr. Anil Kapoor: I think there are two components to any sort of after-the-fact oversight of it, rather than a real-time review. I've said before other committees that I think real-time review is kind of silly. You can't have an investigator out there trying to do his investigation and at the same time being required to show up before a review committee. That's just not going to work. It has to be after-the-fact oversight, and I think there are two components to it.

There has to be an expert component to it—that is, people who are expert in the area of national security—and there has to be what I would characterize as a parliamentary review, which is the committee of parliamentarians.

The committee of parliamentarians is very important because it has democratic legitimacy. It can bring concerns from constituencies to the agencies and can conduct closed hearings as well. I think there is a democratic legitimacy to the committee of parliamentarians, augmented by expert review, which can be.... Justice O'Connor recommended a sort of “super-SIRC” across all the agencies. To the point my colleague was making, we were certainly of the view on Air India that there ought to be a national security adviser.

The expert review has to be across all the agencies, and there needs to be a panel as part of that, but also an independent reviewer, as they have in the United Kingdom. In the United Kingdom, the independent reviewer is tasked often with particular instances, and I'll give one example for Canada: the tragic events on Parliament Hill. It might be important for the population to understand how this happened, what the intelligence agencies knew, and what they did not know. Was it something that could not have been prevented? An independent reviewer can dig in on an event like that in a way that no one, from a public consumption perspective, is actually doing.

From a public relations perspective, it is very important that the public understand what the agencies do. Frankly, a lot of what they do, they do very well. I think that oversight can deliver that message.

● (1235)

The Chair: We're at five and a half minutes already.

Mr. Pat Kelly: Okay.

That's fine.

The Chair: Mr. Mia, do you have a quick comment?

Mr. Ziyaad Mia: I will echo my colleague here. We've called for it for a long time. A committee of parliamentarians is fine. I think Bill C-22 needs some reform, but it's a step in the right direction to give some political accountability and public accountability linked to all of you who are elected.

The first thing is to have a national security review agency that unifies all the agencies, but it would not be separate agencies working together, which I think is too convoluted. You want one counterweight to the security agencies. It makes security better, makes them work better, and gives public confidence.

Second, we need well-resourced experts in the field who can build relationships with the agencies and have access to all information.

Third is that independent review of national security law and policy as they have in the U.K. That person would, in the case of Bill C-51, come and testify on that and give independent advice on it. That person would be able to have access to secret jurisprudence and legal opinions in government and be able to comment to the public and experts with some feedback on what the national security landscape looks like.

The Chair: Thank you, Mr. Mia.

We will now move to the last five-minute round.

Mr. Erskine-Smith, it's your turn.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

I want to start with the definition at section 2: “activity that undermines the security of Canada means any activity, including any of the following activities, if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada.” Then there is a long list of items, but of course that's a non-exhaustive list based on the definition.

Mr. Kapoor, you had noted this as a problem. Would an appropriate amendment be to limit information-sharing to the working definition of “threats” as understood under section 2 of the CSIS Act, or would you have a different proposal?

Mr. Anil Kapoor: No, I think that harmonizes it and rationalizes it to the national security remit.

Mr. Nathaniel Erskine-Smith: Okay.

The second question, just following up on Mr. Lightbound's question, is that it seems we've thrown everything and the kitchen sink into government institutions under section 3 of the Privacy Act. There are 17 recipient institutions, including the Canadian Food Inspection Agency, and there's not necessarily an obvious relation to national security.

In both of your views, in a simple answer, should this committee make a recommendation to narrow the scope of SCISA to institutions and departments that have something to do with national security? Would that be fair to say?

Mr. Anil Kapoor: Yes, on the recipient side I would agree, but on the delivery side, if I can put it that way, I don't have any trouble with who knows what kind of information floats in through any different agencies.

This is about national security, so the hub has to be the lead agencies. They ought to be the main recipients.

Mr. Nathaniel Erskine-Smith: Then you'd narrow the 17 recipient institutions, but you have no particular problem with 140-plus institutions being disclosing institutions.

Mr. Anil Kapoor: I don't, provided that the test is a necessity test.

Mr. Nathaniel Erskine-Smith: Let's pick up on that.

You referred to the testimony of some officials, and Mr. Blaikie got into this to some extent. I understand from their testimony that a 2009 Auditor General's report identified a real concern over government officials being reticent to share some information, and that was a potential problem. The previous government's solution, which appears to be a pretty over-broad solution, was to say that we're going to have the relevance test, and everything can get out the door. You had mentioned that the necessity test is a matter of training, and that isn't appropriate now.

I want to push back a little. If we have 140-plus institutions that are disclosing institutions, there need to be individuals in those 140-plus institutions who are familiar with the necessity test. Do you still stand by those comments that we can train these individuals effectively?

Mr. Anil Kapoor: Yes. I don't see why not. As I said, it's not rocket science. I think it was somebody from the service who testified before you who said we have to educate them on relevancy.

Mr. Nathaniel Erskine-Smith: With respect to oversight and review, we have Bill C-22, which will be in place soon enough. The committee of parliamentarians can be asked by the minister to engage in a particular review, including perhaps a SCISA review.

There was a Liberal amendment in the last session to suggest that all information shared under SCISA should be shared with the Privacy Commissioner and that the Privacy Commissioner should issue an annual report to Parliament on the nature of information sharing and identify any problems.

Perhaps if there were any problems with such information sharing, in the absence of a super-SIRC-type body, which I think both of you have referenced, would that be a palatable solution in the interim?

● (1240)

Mr. Anil Kapoor: Well, at least it's better than none. I suppose the Privacy Commissioner will have a particular sensitivity to the extent to which information is being passed on when it's not in accordance with this statute.

I don't have a visceral objection to it. I'm more interested in the efficacy of the national security information that's being harvested by our agencies. That's what I'm more interested in, and I think that's something that an expert national security panel can deal with on the privacy side. I agree that the Privacy Commissioner is the appropriate one to deal with that.

Mr. Nathaniel Erskine-Smith: My last question is this.

We had Professor Roach and Professor Forcese before us, and they indicated some confusion with the drafting of this bill. I think Mr. Kapoor called it “immature”. It's unclear on a first reading that recipient institutions are still subject to their own mandates. There's a real worry, for example, where we have disclosing institutions subject to a relevance test and all the information gets out the door. Lo and behold, the RCMP and CSIS and other of the 17 recipient institutions now have the information before them.

Should we clarify in this bill that they're subject to existing mandates, that they require a warrant to access this information, that they still have to obtain this warrant before they can review the information and use it in a serious way? Should we explicitly put in this bill that if they do not have proper authorities within their existing mandates, they have to destroy the information immediately?

Mr. Anil Kapoor: On the warrant question, I think both Craig and Kent testified about how this is infirm in relation to section 8, to the extent that it connects to criminal law enforcement. In my other life, I defend and occasionally prosecute on the crime side. I would say that this bill needs to be amended in some way to preserve section 8 rights in the criminal prosecution realm, and there should be a requirement that a warrant be obtained.

What I'm concerned about is a factual situation in which at the national security joint operations centre, they're on somebody. They think there may be some information sitting in one of these 17 agencies or one of the hundred-and-some agencies. They pick up the phone, call down, and say, “Do you know anything about this guy Blogs?”, and the answer is, “Yes, we do.” They say, “Okay, I'm going to make a request.” Then they make a request and they get the information that way, rather than through a warrant.

I don't want it to be misused. I would want the warrant requirement to be preserved here. You can foresee that there will be litigation on that question, so why not just cross it off now?

Mr. Nathaniel Erskine-Smith: Officials did say that they would be subject to the warrant requirement, but we perhaps have to put it in black and white.

Mr. Anil Kapoor: I would say that in a criminal investigation, you can't make a request. You have to....

Mr. Nathaniel Erskine-Smith: You have to get a warrant.

Thanks very much.

The Chair: Thank you.

Go ahead, Mr. Blaikie, for three minutes.

Mr. Daniel Blaikie: Thank you.

We know that information sharing occurred prior to SCISA. If you were to scrap this and start again, what do you think is in SCISA that would be important and should be preserved, and what do you think are some of the things...?

In the opening presentation there were some allusions to the fact that certain kinds of important information-sharing needs aren't addressed by SCISA. What would you keep, and what do you think isn't there that should be there?

Mr. Ziyaad Mia: When we look at Air India, we see that information wasn't shared, so I think we maybe need to look at new legislation—I mean, it's not in here—and some requirement for the agencies to work together.

Mr. Kapoor has indicated they're doing that, but that's the type of thing we need in an information-sharing law. We need to look at encouraging that information sharing where it's necessary and within the bounds of what we're talking about. It's not about harvesting a lot of information, but about keeping it very focused to the information we need that's related to national security issues.

Then I think information-sharing legislation should look at the principles that we talked about related to the thresholds. That should be laid out in law. Possibly the idea of a stickhandler in government should also be looked at. Those roles need to be laid out.

I think there is a role for law in setting up the architecture. You don't want to just have it happening out there, because if it doesn't happen properly, you'll have a problem, or if it happens in the wrong way, you'll have a problem on the other side, as we've seen with the two inquiries. A good role for law on information sharing is to set up that architecture—to set out the rules and the thresholds, and what the mandates of the agencies are.

To follow up on Mr. Erskine-Smith's point, who's overseeing this? I'm worried that interim measures may become permanent measures, and we'll say we have something. If you can recommend pushing towards coherent controls and review, that would be my suggestion.

I don't think there's much in here that I'd keep. I'd say you could use this as a basis to redraft. As I said, there are a lot of fundamental flaws, starting with the definition.

● (1245)

Mr. Anil Kapoor: I think the concept of having regulation of information sharing is a good one. You've heard various criticisms about this particular act, but the idea of identifying agencies that are delivering information and identifying each of the recipient agencies is a good thing.

I would have a slightly different list. We said in Air India that we thought that a national security adviser is important not only for investigations that are both CSIS and RCMP investigations, but a national security adviser could also direct traffic on information. We had a section in there on how that content can be privileged so that it doesn't necessarily end up in a court case. Having a robust national security adviser goes some way of directing the traffic, not only in terms of investigations but also in terms of information sharing. There just doesn't seem to be an appetite for that on the part of the agencies.

The Chair: Thank you very much.

Colleagues, that brings us to the end of the official round of questioning. We have a few minutes left. The conversation is excellent today. Mr. Bratina has indicated, as a parliamentarian who has yet to be able to ask questions, his willingness to do so. If it's okay with committee members, I have several questions I'd like to ask as well, so we'll do that.

Go ahead, Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thank you.

Often structures begin innocuously enough and then grow. I've seen this at other levels of government: somebody is supposed to build a trail, but they end up running the whole waterfront. Is there anything that concerns you in terms of SCISA growing into something more than it is in terms of its operations?

Mr. Ziyaad Mia: This goes to the root of my concern. The target of information that would reach the threshold is so broad that it's not even broad: it's open-ended. It's already set up to become something quite amorphous.

At the lowest level, it could just be that they'll harvest all sorts of information and they won't know what to do with it. The worst-case scenario, as I've pointed out a couple of times, is that either we miss a terrorist or a national security threat because there's so much information there, or else that we make mistakes and share collected information and mined data abroad and create a disaster for individual Canadians.

If I were rewriting this, I would just start again. It's a short bill, so you just start again. As I answered to Mr. Blaikie, you'd lay out those principles. You'd start with a very tight definition. I believe Mr. Erskine-Smith mentioned the section 2 definition in the CSIS Act; I think that's a good start, because if this is a national security information sharing bill, let's tie it to national threats to the security of Canada. That's the remit of CSIS, and that's a pretty broad definition in itself. That brings us to a nice tight definition, and then of course there's laying out the protocols and safety measures. I think that would do it. That would regularize and give us some coherence in national security information sharing.

As well, though it's not for a bill, a lot of work needs to go into making the agencies work together in a coherent way and into improving that review over time.

Mr. Bob Bratina: In your submission, you stated that Canadian Muslims will be disproportionately affected. Could you just expand on that comment?

Mr. Ziyaad Mia: I believe Commissioner O'Connor mentioned in his report that given the threats out there in the geopolitics of the world, obviously Muslims are implicated. That's not the right word, but you know what I mean. They're possibly seen as threats or whatnot, and because Muslims are on the radar, that can lead to problems. Though the national security bills are drafted neutrally and nowhere say “Muslim” or “Arab”, that's the fight we have right now in the world with terrorism. In that context, likely a lot of national security resources are going to be focused on that. We can debate whether that's right or wrong, but that's what's going to happen, and inevitably, because the security agencies are going to be looking at those communities, there's a risk that the mistakes will impact those communities disproportionately.

● (1250)

Mr. Bob Bratina: Thank you.

The Chair: Thank you, Mr. Bratina.

This is one of my favourite days at this committee so far. This has been an excellent conversation.

Mr. Kapoor, I have a question for you. Mr. Mia, feel free to join in at any point.

As somebody whose background is in IT, I make an important distinction in my mind between data and information. We seem to have used the words “data” and “information” interchangeably at this particular committee, so I would like to get a distinction from either of you on the difference between data and information.

Mr. Anil Kapoor: Data, as you know, can be very significant, particularly metadata, which is a lot of what our service harvests these days, and a lot of agencies are trading in it. There's a big debate right now about its usefulness and its probativeness in criminal trials, for example, and whether it can be obtained without warrant. There's a whole big debate on this question, as you know.

From my perspective, it's all about content that's important for national security, so if you're sitting on a data point and you've satisfied yourself that it's necessary for the service to have it for their remit, then I think the act is engaged and the content can be passed.

From my perspective, it's about national security content, if I can put it that way, which would cover both data and information.

Mr. Ziyaad Mia: I concur with that. I agree that data per se, or data points—metadata and those sorts of things—can appear innocuous in some ways, but again it's the data mining. Because of the—

The Chair: I understand. You have to have data to run analytics on in order to synthesize information.

Mr. Ziyaad Mia: Exactly, and we certainly need to do that. I'm not suggesting in any way that our security agencies should not be doing that, because that's a useful way to identify threats and see patterns of criminality, but it's how we do it and how much information we're pulling.

You're an IT person. Humans still are the programmers, so whatever algorithms we design and run are not perfect, because humans are running that AI. We should be cognizant of the fact that those computer programs can make mistakes, and that's where I see the data.

The Chair: That's interesting. Computers never make mistakes. They will calculate the same answer every single time in exactly same way. The only errors that are ever made are human errors in the programming of that computer.

The reason I'm asking this is that when it comes to the analysis of data and as we look at the review of this legislation, I would suggest that actually it's more than information. It's not information that's being passed, but data, so I don't know if the act is actually properly named. That's a moot point.

However, if I were an analyst working on a large set of data—we can call it metadata or we can call it whatever we want—it will come in all shapes and forms. It will be shared in different varieties and different formats and different platforms, depending on the agency that shares that information, depending on whether it's domestically sourced or whether it's internationally sourced, and I would want as much data as I possibly could to run analytics on. Do you believe that we should be limiting ourselves to the amount of data that we actually have? There's a good discussion here at the table.

I'll give you an analogy. I'm a fisherman as well. Why would you want to limit me to fishing in a certain corner of the lake? Wouldn't you rather just change the nature of the hook that I use and allow me to fish everywhere?

Mr. Anil Kapoor: I guess what you're asking is whether or not the standard should be more forgiving of sharing information—I'm using “information” to include data—or less forgiving of sharing. Again, it comes back to a question of balance.

From my perspective, if this is a national security piece of legislation, which I gather it is, we ought to marry up the definitions for the national security agency. They ought to be harmonized and rationalized to the service mandate. As for whether it should be based on necessity or relevancy, the service should only share it if it's necessary and should only use it if it's necessary. The service should have a necessity requirement built in. So too should the agencies that are sending information.

● (1255)

The Chair: That's the hook that I would argue for, and we should be able to cast the widest net we possibly can.

Mr. Anil Kapoor: Right, but I think "necessary" is pretty wide.

The Chair: I agree. I think it should be. That's my personal opinion.

Mr. Anil Kapoor: Yes.

The Chair: There's been a bit of a discussion too, and a disagreement between the two of you, insofar as the retention of data is concerned.

Mr. Kapoor, I would agree more with your particular perspective.

Mr. Mia, my question is more for you in relation to the examples that you brought up about Mr. Arar. Perhaps there may be others, and I'm going to defer to your expertise on this point.

We've already had the conversation about analytics and the results of human error when it comes to programming that might result in sloppiness and we've talked about the vastness of information that led to a false positive. If we didn't keep the data on which the poorly programmed analytics were run, how would we exonerate a person if the data were no longer there to run the correct analytics on?

Mr. Ziyaad Mia: Fair point. It's probably different in degree rather than in kind. Mr. Kapoor, you can jump in.

I don't want to use the word "relevant", because we're debating that, but it was information that was properly within the remit of those agencies. I have no problem with agencies keeping information properly relevant to the investigations and their work.

In the case of large-scale harvesting of information, such as checking passenger manifests from every flight against no-fly lists, presumably that does not need to be kept. We don't need the travel patterns of every Canadian. Arguably somebody could make a case that three years down the road we will see Joe Smith on our radar, and we'll want to check all of his travel patterns in the past. What I'm really concerned about is that we're getting into a pre-crime society. Now we're keeping data on everything that someone does against the possibility that Mr. Bratina may do something in the future, so we can check if in the past he's crossed the line.

I'm just using you as an example. You're the first person I saw.

Mr. Bob Bratina: I don't know what you're talking about.

Some hon. members: Oh, oh!

Mr. Ziyaad Mia: I'm sorry.

The Chair: We all know what you're talking about.

Mr. Ziyaad Mia: That's my main concern there.

In today's world, it's going to be tough, especially with a lot of data, but I think we need to be very nuanced in how we strike that balance while respecting the law.

The key is going to be those thresholds. If we start to get the inputs right, then likely the information in the databases will be necessary to be held. If the net is so wide that we're pulling in anti-Saudi protestors, or whatever they are, or just anyone who is flying, and then later they show up on the radar possibly, and then all of that is pulled in to create a profile of them with metadata and travel patterns, that to me is worrying, because fundamentally in a democracy we don't do that. When Commissioner Paulson was talking about keeping email content on servers, one of the U of T researchers said, "Why don't we just have a camera in all of our homes because it could be useful someday?" I think that really hit the nail on the head.

The Chair: Mr. Lightbound, did you have something?

Mr. Joël Lightbound: If I may, based on the testimony we've heard today, would it be possible for the clerk to ask the 17 agencies —maybe not the ones who are clearly dealing with national security —to provide this committee with a written—

The Chair: I have no problem with that. Does anybody here at the committee have a problem with that?

Mr. Joël Lightbound: —explanation of how the information they receive pertains to national security and what their mandate has to do with national security.

The Chair: I want to thank the witnesses.

I'll leave you with one note: I don't know what I don't know. I put trust in the people who do these things on my behalf to keep me safe. My only hope is that information or analytics that were either missed or could have been harvested that could have prevented the deaths of Nathan Cirillo and Patrice Vincent would have been used. We can't bring them back from the dead, but we can always make reparations with Mr. Arar for some of the misdeeds that have happened to him. I think we need to be very cognizant of the consequences of what we're doing.

I thank the witnesses very much for their testimony. It was absolutely fantastic today. Thank you very much.

The meeting is adjourned