HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 041 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, December 13, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, December 13, 2016

● (1100)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I call the meeting to order.

Good morning, colleagues. This is the last meeting we'll have, I think, before the impending adjournment of the House of Commons for the Christmas break. We are continuing our study of the Security of Canada Information Sharing Act.

Colleagues, I don't want to get into the discussion right now; I just want to let you know that after today we will have heard from about 25 witnesses on this matter. According to my discussions with the clerk, we have about 70 witnesses who are scheduled or who have been suggested for the committee to hear from. This puts us at about the one-third point if we are going to hear from all of the witnesses. We'll need to make a decision—if not today, as soon as we get back—in regard to how much longer we wish to continue and when the committee feels that it has heard sufficient evidence on this matter.

I'm leaving that out there. It's not for discussion at this particular time, but just as a thought that you ought to have, because we'll need to make some decisions when we return about where we would like to go.

At any rate, we are pleased to have with us today, from the British Columbia Civil Liberties Association, Micheal Vonn, who is joining us by video, and, from the Centre for Law and Democracy, Michael Karanicolas, who has been here recently. An individual who is here before us and actually in the room is Lisa Austin, who is an associate professor from the University of Toronto's faculty of law and the David Asper Centre for Constitutional Rights. We thank each of you for taking the time to be with us here at this committee this morning.

I'm sure that all of you are familiar with our process here. You have up to 10 minutes for a presentation. I'd like you to stay as close as possible to that. I'll give you a little bit of leeway, but if you start stretching it out near 15 minutes, you might see me intervene.

We'll start with the British Columbia Civil Liberties Association, please, for up to 10 minutes.

Ms. Micheal Vonn (Policy Director, British Columbia Civil Liberties Association): Thank you very much, Mr. Chair, to you and to the committee.

My name is Micheal Vonn, and I'm the policy director of the B.C. CLA.

I gather that there has been a great deal of general agreement among privacy and civil liberties organizations on SCISA, as I'm going to refer to it. My association is certainly among those that have called for the complete repeal of the act, but rather than repeat concerns that you may be very familiar with at this stage, 25 witnesses in, I'm going to try to address some matters that I believe have not had as much discussion and that I hope will assist you in your deliberations.

The two matters I'm hoping to address are, first, the seriousness of the disruption caused by SCISA's blurring of the mandate of critically important federal institutions, and second, the evidence that rebuts the hope that other legislation will act as a moderating effect on SCISA.

On the first topic, which is the question of mandate, FINTRAC provides a ready example. The Office of the Privacy Commissioner of Canada does an intermittent audit of FINTRAC, and these audits have consistently found troubling overcollection and retention of personal data. Obviously, there are some discrete remedies that are available to address some of these issues, as indicated by the recommendations in the OPC's report, but in the main, because the standard of suspicion is very low and the prejudice to individuals is very high, FINTRAC itself has long maintained that one of its primary safeguards for privacy is its independence from law enforcement. Now, with the almost unfettered access to information sharing authorized by SCISA, the independence of FINTRAC in this regard is essentially fictional.

The kind of screening mechanism that is the basis for a regime like FINTRAC's is founded on a necessary balancing. The entire enterprise, of course, is one that can only be justified under very compelling need. FINTRAC has extraordinary powers of data gathering. Personal information that clearly commands a reasonable expectation of privacy is nevertheless compelled by the law in such a way that vast over-reporting is a given. Indeed, only the tiniest fraction of reported individuals and entities are ever found to be conducting themselves in any problematic way. To balance this state of extreme prejudice to innocent parties, we require sufficient counterbalancing protections. The basis for that balancing in the FINTRAC regime is now decidedly unsettled by SCISA, even to the point where its constitutionality may be at issue.

The effect on the mandate of federal agencies covered by SCISA may indeed be difficult to assess in the short term, but indications are already very troubling. Because I happen to work in a very broad sphere of rights advocacy, I am in a position to tell you, for example, that health policy advocates are now having to reconsider policy positions and proposals in light of the fact that there is very little confidence in the privacy protections afforded to patient information held by Health Canada, because of the sweeping nature of the access that is granted through SCISA.

Even more so, Veterans Affairs is likely to have grave difficulty convincing Canadian veterans that their extremely sensitive and highly prejudicial personal information, such as physical and mental health information, is appropriately protected. We may of course recall that it was just a few short years ago that Canada saw what I would argue was its single most appalling medical privacy scandal in relation to veterans' medical information. Sean Bruyea, a veteran's advocate, had his confidential medical files passed around by federal bureaucrats in an apparent effort to discredit him and his advocacy on behalf of veterans. This, you will recall, was an extremely high-profile national scandal, in which this veteran's medical information found its way even into ministerial briefing notes.

● (1105)

The unprecedented all-of-government information-sharing capacity afforded by SCISA can only be seen to undermine whatever trust has been rebuilt between veterans and the federal government since the Bruyea scandal. It obviously has a negative impact on the very mandate of Veterans Affairs.

Moving now to my second point, I would like to highlight not only that SCISA has no requirement for individualized grounds for data collection and can facilitate the sharing of entire databases but that it also seems likely that it was enacted precisely for the purpose of bulk data acquisition. It does not seem likely that the model of information sharing that is in SCISA is meant to address merely the possible need for clarification of the disclosures that were permissible under the Privacy Act. I note that during the Vancouver Olympics, when the police were discovered to have purchased a military-grade sonic weapon, they said they were only planning to use it as a giant megaphone, yet they did not buy a giant megaphone: they bought a sonic cannon. Similarly, we did not get an amendment to the Privacy Act: we got SCISA.

This fall we have seen a litany of incidents in which CSIS in particular has been seen to be unmoored from lawfulness in important aspects of its primary activities. It must be noted that the alarm and concern that has been sounded so strongly, not least by the Federal Court, pertains mainly to the collection, use, and retention of bulk data. Sadly, we have learned that section 12 of the CSIS Act, which is the standard for strict necessity, has proved to be very little barrier to CSIS accessing bulk data. As we know from the only SIRC audit ever done, released this fall, SIRC found no evidence to indicate that CSIS had appropriately considered the threshold as required in the CSIS Act in the collection of their bulk data. As a result, it is possible at this juncture that the vast majority, or even everything, in the CSIS bulk data holdings constitutes illegal spying on Canadians.

It has been argued that the troublingly low thresholds for sharing information in SCISA are tempered by the Privacy Act and other governing legislation, including the CSIS Act. Certainly recent events give us no reason to be confident that they are operating as meaningful protections. Not only have some of the recently discovered violations of the CSIS Act been going on for over a decade, but none of them appears to have been remedied. Indeed, there is widespread concern that they will not be remedied and will be condoned with after-the-fact legislation, which will further corrode public trust.

At this juncture, we simply have too much evidence to the contrary to accept that SCISA has checks and balances that will mitigate the unprecedented scale of information disclosure that it allows. The reality is that these other legislated potential checks have been failing utterly to meaningfully constrain bulk data acquisitions. It is untenable to claim at this juncture that finding out about a decade's worth of illegal spying is the system working; it is clearly the system not working.

The notion that we have an effective limitation to SCISA in other legislation has thus far not proved true. It is nevertheless not the model that should be applied. It is SCISA itself, which was never justified and which actually undermines the very mandates of some of its included agencies, that must be repealed. Amendments, in our position, and clarifications on disclosure powers, if they are needed, should be part of the Privacy Act.

Those are my prepared comments. Thank you very much.

● (1110)

The Chair: Thank you very much.

We now move to the Centre for Law and Democracy.

Please go ahead, Mr. Karanicolas.

Mr. Michael Karanicolas (Senior Legal Officer, Centre for Law and Democracy): Thanks very much to the committee for their kind invitation. I'm sorry I can't be there in person this time.

My name is Michael Karanicolas, and I am employed as the senior legal officer for the Centre for Law and Democracy, an NGO based in Halifax. We work to promote foundational rights for democracy, with a particular emphasis on freedom of expression and increasingly on privacy, given that many of the biggest threats to freedom of expression currently present in overly intrusive surveillance systems. Indeed, the nexus between bulk data collection and inhibitions on speech has been widely noted, including by the UN special rapporteur on freedom of opinion and expression.

It is also recognized under international human rights law that states need to put in place effective systems to address terrorism and other threats to security. Among other things, this is necessary to uphold democracy and the whole system of respect for human rights, including freedom of expression. At the same time, international law establishes the clear necessity for balancing security against other fundamental human rights, including privacy.

I do want to mention at the outset that I was greatly troubled by the overall tone of the “Our Security, Our Rights” green paper. It presented readers with a series of ticking-bomb scenarios, seemingly designed to bolster support for expanding powers by painting a picture that focused on the limits of Canada's police and security agencies and the ways in which terrorists are apparently outwitting them. Although the green paper gives a perfunctory nod to civil rights concerns, the green paper could have been improved, or at least balanced, by including scenarios in which these powers are and have been misused.

The green paper also muddies the waters regarding the limits of information sharing by noting, on page 27, that it helps law enforcement by facilitating information sharing without worries about whether the actions violate the Privacy Act. However, just two pages later, the paper's decision-making chart states, as its final step, that information may not be shared if the disclosure runs contrary to another law. We believe this should be resolved by clarifying that the Privacy Act does indeed apply to the Security of Canada Information Sharing Act.

The Privacy Commissioner has also recommended that rather than the current standard, which dictates that certain federal government institutions may share information among themselves so long as it is relevant to the identification of national security threats, a standard of being necessary should be put in place. We support this recommendation, and add the note that if we're talking about security, data minimization, whereby organizations seek to limit material stored to what is strictly necessary, is a cardinal principle of digital security. We can look south of the border for lessons on this, as over-storage was one of the reasons last year's hack of the U.S. Office of Personnel Management was so catastrophic.

I think we can also look south of the border for a fairly striking lesson on why it's so important to craft this legislation carefully, with as little scope for potential abuse as possible. It's easy to look at people who one might broadly trust to exercise their powers responsibly and to forget that one of the consequences of democracy is that the nature and state of the people in charge can change very quickly, potentially bringing into power people whose definitions of phrases like “activities that undermine the security of Canada” may be dangerously expansive. Flexibility, as the green paper seemingly welcomes, is very much a double-edged sword.

In that vein, we support the recommendations of Professors Roach and Forcese that the language of “undermine the security of Canada” should be narrowed so that the application of the act is limited to “threats to the security of Canada”, as established in the CSIS Act, and that the act should mirror the language found in item 83.01(1)(b)(ii)(E) of the Criminal Code on the exceptions, whereby “advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C)”—i.e., endangering life, health, or security—should not be subject to the act.

We also broadly support the Privacy Commissioner's recommendation that in addition to parliamentary review, institutions permitted to receive information for national security purposes should be subject to expert or administrative independent review. We noted with alarm that 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. As well, of the 17 entities authorized to collect information under the SCISA, only two had indicated that privacy impact assessments, a fundamental step, were necessary and were under development. There are several models of independent oversight to look to here, including the United Kingdom and Australia, both of which have a dedicated independent monitoring system in place.

● (1115)

I'm going to be brief here because I think that a lot of our recommendations will echo what you've heard from others.

To wrap up, although the online world certainly presents novel challenges to law enforcement, it is worth noting that the tool kit available to our security agencies today is vastly more powerful when compared to their investigative capabilities 20 or 30 years ago. That's true both in relative terms and in absolute terms. This requires carefully crafted limits to protect and safeguard fundamental human rights.

Thank you.

The Chair: Thank you very much.

Our last presenter today is Lisa Austin, from the University of Toronto. Lisa, the floor is yours.

Professor Lisa Austin (Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual): Thank you.

Thank you for inviting me, and I congratulate you on the report you released yesterday on the Privacy Act. I was looking at it quickly on the plane this morning and I look forward to reading it more carefully later; it looks excellent.

Today the focus of my remarks is that I want to outline why I believe that the Security of Canada Information Sharing Act, or SCISA, as I'll call it, is constitutionally deficient and should be repealed. I agree with the commentators who have argued for that. Even if it's the view of this committee that it should not be repealed, I hope that if you think about ways to make it less problematic, you will do so with a strong emphasis on charter rights in thinking that through. That's what I'm going to focus on here.

Canada's constitutional jurisprudence is very clear that information-sharing practices within the government and with foreign states can attract charter scrutiny. Just because the state has collected information for one purpose does not mean there is no remaining reasonable expectation of privacy in that information. This is the crucial point. It's absolutely clear from the Supreme Court of Canada's jurisprudence on section 8.

Generally there can be a reasonable expectation of privacy in information the government already has for some purpose, and where there's a reasonable expectation of privacy, the starting point for constitutional analysis under section 8 is that the state should not get access to this information unless there is prior authorization on a standard of reasonable and probable grounds. Departures from these protections can be authorized by law, but those laws must be reasonable. In other words, such departures require constitutional justification. It's also difficult to establish such a justification in the absence of reasonable safeguards for this information, and again jurisprudence is speaking a lot about the need for safeguards in doing this kind of reasonableness analysis. That comes out strongly in the Wakeling decision.

The question, then, is.... SCISA allows information sharing on a standard of relevance. There is no prior authorization, and as I'll outline, almost no safeguards are mandated in the act. This is a clear departure from that starting point, and the question is, can you justify this constitutionally? I think one of the main problems with this whole justification question is the basic problem that I think the Privacy Commissioner of Canada and all his provincial and territorial counterparts have laid out in their submission on the government's national security green paper, in which they state "... we have yet to hear a clear explanation, with practical examples, of how the previous law prevented the sharing of information needed for national security purposes."

You have clear questions from very serious commentators in Canada saying you haven't met the threshold for public justification for this act at all, and given that there are these departures from what I'm arguing are clear constitutional standards, there's a real dilemma here.

What we do have in Canada are two sets of very careful recommendations regarding information sharing that come out of the Air India inquiry and the Arar commission. Many of these recommendations are narrower in scope than what SCISA provides. For example, the Air India inquiry's information-sharing recommendations concern very specific types of targeted sharing among a small number of institutions, rather than the broad sharing contemplated by SCISA, and some of the recommendations in the Air India inquiry are actually stronger than what SCISA provides. For example, they recommended that CSIS be required to share information with the RCMP, and you don't see this reflected in the act.

With the Arar commission, many recommendations also touch on information sharing, but notably when the Arar commission discusses the Privacy Act, it speaks favourably of the existing exemptions. It says exceptions for consistent use in law enforcement in the public interest are all fine. It does not say that a new authorization is required that would engage paragraph 8(2)(b) of the Privacy Act. That's the provision that says you can share information "for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure". That's the provision in SCISA that many people interpret as opening the door to this broad sharing. The Arar commission did not ask for that. It said the existing exemptions and the way they were being used was perfectly fine, and it also indicated that the proper scope of the consistent use exemption should be informed by charter jurisprudence.

The Arar commission does not talk about the need for new information-sharing powers, but it does talk a lot about the need for written agreements, the requirement of caveats when sharing with foreign states, issues of accuracy and reliability of information, and the need to protect human rights.

● (1120)

None of these latter considerations are strongly reflected in SCISA. We have instead a list of guiding principles that are not requirements. It gives very weak support for caveats. It talks about information-sharing arrangements, but not written agreements, which were very key to the Arar commission report. There's nothing about accuracy and reliability. There's nothing about sharing with foreign states and the potential human rights implications of doing so. There is weak language that they may make regulations about disclosures and record-keeping.

The Supreme Court of Canada jurisprudence suggests that the absence of appropriate safeguards for the sharing of data can undermine claims that the law is reasonable. We don't see any of that here, yet we have these strong reports in the Canadian public sphere that ask for all of these things.

I think that raises a serious question. We don't have the public justification for broad information sharing. What we do have is strong justification for a much narrower set of information sharing in SCISA, and in some cases stronger practices than we see in SCISA. It would be very difficult to justify, I think, the breadth of this act constitutionally.

There are other aspects. I think the sheer breadth of language like "activities that undermine the security of Canada" in this act is overbroad and also is going to raise those problems with respect to justification. You've heard that from other witnesses, so I won't belabour that point.

There have been a number of suggestions that you can change the "relevance" standard to one of necessity. I think that would be an improvement for sure, so in those terms I would support it. I think you should also think through how that might still remain problematic from a constitutional perspective. For example, the Privacy Commissioner of Canada makes this recommendation on the basis that necessity is the standard that CSIS must follow in relation to its investigative powers, as stated in section 12 of the CSIS Act. However, CSIS actually has to seek a warrant where its investigations intrude upon a reasonable expectation of privacy. The warrant provisions of the CSIS Act are a different part of the act, and they require prior judicial authorization. They require that such authorization meet a higher standard than necessity, that there are reasonable and probable grounds that such an intrusion is required, and that there is evidence that other investigative methods have failed or are likely to fail.

The reasonable and probable grounds standard is not simply a test of necessity. When many people talk about the necessity test, what they like to provide as an example from the constitutional context is the section 1 test. The section 1 test is dominated by ideas of minimal impairment. A minimal impairment analysis would be something like, "Do you need this information in order to reach your goal, and, in doing so, do you intrude upon privacy as little as possible?", but reasonable and probable grounds contemplates that sometimes you do not get to pursue your goal, even if this pursuit is minimally impairing. Reasonable and probable grounds includes the idea of the likely effectiveness of reaching that investigatory goal, so even if you're not going to build in some kind of prior authorization threshold—although I still think that's a good idea—there's a need for efficacy review here. Are the powers effective? Are you actually meeting your goal? I don't see that anywhere in SCISA at all. At most, paragraph 4(d) gives you the guiding principle that

> the provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing;

"Feedback" in a guiding principle is not what's needed. There has to be some burden of proof that information sharing is effective—if not beforehand, then at least after the fact.

In conclusion, I want to echo some of the comments that Micheal Vonn was discussing with respect to the issues of bulk access. Much of the discussion of SCISA that the government provides in its green paper proceeds as if the government institutions will decide to share information about specific individuals at discrete points in time rather than share institutionally held datasets for the purpose of more sophisticated analytics, including automated data processing. However, many believe that the latter is precisely what SCISA at least enables, even if it's not being done now—I don't know—and this raises additional privacy concerns.

● (1125)

Many of these types of analytic techniques rely upon access to the personal information of individuals who are themselves under no suspicion at all. There are a number of privacy considerations there, but the considerations that touch upon charter issues are broader than that. There are a lot of freedom-of-association concerns that come with some techniques, especially when the data involved is either social media information or metadata information, whereby people's social networks can be mapped. There are freedom of expression issues at stake, as we've already heard from the Centre for Law and Democracy.

There are also equality concerns. How are these techniques being used? Are biases being built in, either in relation to the datasets that are being used or the types of algorithms that come out in respect to processing this information? There's emerging literature regarding algorithmic responsibility, and a lot of concern about how information is being processed and whether that leads to problematic biases and inaccuracies.

None of those concerns are possibly met by SCISA as it is drafted right now. As Micheal Vonn from the B.C. Civil Liberties Association indicated, there's a sense that if we overhaul the Privacy Act, that might temper some of the problems with SCISA. Sure, it will temper them, but I think that SCISA itself raises a lot of really specific charter questions, some of them about privacy and some of them about these related sets of issues in the national security context that on their own require justification and that the legislation as it stands is seriously deficient on.

Thank you.

● (1130)

The Chair: Thank you very much.

We'll now move to our rounds of questions, starting with our seven-minute round.

We'll start with Mr. Erskine-Smith, please.

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

I want to start with the definition: "...undermines the security of Canada".

Mr. Karanicolas, you mentioned that you'd prefer and you support the recommendation of Professors Roach and Forcese, which is to stick to the definition in section 2 of the CSIS Act.

Ms. Austin and Ms. Vonn, are you in agreement with that?

Prof. Lisa Austin: I am, yes.

Ms. Micheal Vonn: Certainly I agree. We don't actually even know what "undermining the security of Canada" means. It's unprecedented in Canadian law. It's *terra incognita*. Certainly it would be an improvement to go to the definitions that we are familiar with.

Mr. Nathaniel Erskine-Smith: With respect to relevance and necessity, Ms. Austin, we had John Davies from Public Safety before us, and he referenced an Auditor General report from 2009 that found that departments and agencies were not sharing intelligence information because of concerns related to privacy. He pointed to that as one example of why SCISA was put in place. He suggested, and the department officials made the case, that SCISA changes the disclosure rules but not the collection rules, so the standard of relevancy is only on the disclosure side.

When we talk about relevance and necessity and warrants, if we put in black and white clarity that the mandates of the recipient institutions have not changed, that they're subject to a necessity collection requirement and subject to warrants if their operating rules require them to obtain warrants to obtain information, does that satisfy the concern, or should we go further?

Prof. Lisa Austin: I don't know the report, so I don't want to talk about that specific report.

When you depart from a warrant...because you're not going to be dealing with that when you're dealing with use and disclosure, but when the government already has information, and the constitutional jurisprudence says there's still a reasonable expectation of privacy—not necessarily on all of it, but it can still attract a reasonable expectation of privacy—there's a constitutional question when there's further sharing of it or some subsequent use that's not the use that it was collected for, so the constitution is in play there.

Does that mean you need a warrant? No, the courts have allowed departures from warrant requirements in all sorts of contexts, but you still have to think through the charter question about whether this is reasonable or not.

I don't think this information should be shared without some review happening, at least after the fact. Part of what the reasonable and probable grounds says is that you have this threshold that gets you to the question of whether you are likely to get evidence, but what about after-the-fact efficacy review, so that if it turns out you're not actually meeting any intelligence goal or national security goal, you shut down whatever that information-sharing practice was?

In the absence of that, is the law reasonable? I don't think so, in the absence of some of the other sorts of safeguards, such as written agreements. The act talks about arrangements; they're in the guiding principles. The act doesn't require that there be rules around data retention and other sorts of protections.

Mr. Nathaniel Erskine-Smith: Assume for the sake of argument, then, that we recommend putting in a requirement for written agreements and we suggest to institutions that they have safeguards put in place for the reliability of information. Imagine that an individual works for Immigration Canada. They see a document that, in their view, has national security implications, but they are unclear on its full implications. They then would send it to CSIS, and they wouldn't be worried about doing so, because they're disclosing on the relevance standard, but CSIS, to actually collect that information and to use that information, is still subject to the "strictly necessary" test and any warrant requirements, as I understand it.

I understand that there's been confusion about the law, but if we put it in black and white that this is the case, what is the concern, then?

● (1135)

Prof. Lisa Austin: I still don't understand why you want the relevance threshold when already under SCISA no one is going to get into trouble for good-faith sharing. If you have a necessity standard and that person is saying "I don't know" but in good faith says that they think this meets the necessity threshold, where's the concern?

Mr. Nathaniel Erskine-Smith: I see. Your point would be that it should be necessity all the way down, both on the disclosure side and on the collection side.

Prof. Lisa Austin: Yes, because there's already a protection for the good-faith use of the act, so I don't know why you need an extra protection for the people sharing.

Mr. Nathaniel Erskine-Smith: Right.

With respect to review, we've had some witnesses come before us and talk about a super-SIRC type of body. There are 14 recipient agencies under SCISA that don't have expert review right now. Would it be a reasonable solution to have the Privacy Commissioner review all information sharing on an annual basis and issue a report to Parliament?

Prof. Lisa Austin: I'm not an expert on the question of review. I do generally agree with my colleague Kent Roach. I know that Kent Roach and Craig Forcese have made recommendations on this.

My hesitation in leaving it all up to the Privacy Commissioner is that there are very specific considerations that come up in a national security context that some of these other bodies might have more contextual information on and that would be very useful in reviewing this. My second hesitation would be that the Privacy Commissioner's office has not had a strong mandate with respect to charter issues, and a lot of the concerns I have here have to do with the charter and how it applies to information sharing, so I'm not sure.

Mr. Nathaniel Erskine-Smith: Really quickly, then, I would like to have the other two witnesses answer that question with respect to review.

If the Privacy Commissioner is tasked with reviewing information sharing, at least for the 14 agencies that don't have expert review, and works with the other expert review bodies in reviewing that information sharing and issues a report on an annual basis, would that satisfy some of your concerns? Is that sufficient?

Ms. Micheal Vonn: No. It's not sufficient from my perspective.

Again, what we've just learned about what's happened about SIRC reviewing CSIS and its bulk data holdings should give us no confidence that we are going to be able to get the kinds of privacy protections that Canadians expect for the information for which they have a reasonable expectation of privacy. Ten years running, we have seen bulk data collection that is illegal, although SIRC had the obligation not to collect it unless it was strictly necessary.

Again, we cannot say that we have a system of oversight that is effectively dealing with, in this case, the illegal—let alone problematic—information sharing that's going on in this sphere.

Mr. Michael Karanicolas: I would echo that there needs to be an independent civilian oversight rather than bundling this into the Privacy Commissioner.

I'll start by saying what I should have said at the outset as well, which is that I want to also congratulate you on the reforms to the Privacy Act, which look great. There's a lot of good stuff in there.

Generally speaking, we've talked about how this is a privacy concern, but it also touches on freedom of expression and freedom of association. There's a broad and specialized basket of issues that come up, and I think they should be dealt with by a dedicated oversight body.

The Chair: Thank you very much.

That uses up your time, Mr. Erskine-Smith.

To our witnesses, you have no idea how it warms the hearts of those around the table that you were looking at the report we tabled yesterday in Parliament.

We now move on to Mr. Jeneroux, please, for seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair.

I'm sure it's a popular read amongst the Canadian population right now. We appreciate hearing that.

I do want to talk to you briefly, Mr. Karanicolas. When you appeared before the committee during our Privacy Act review, you mentioned that “expanding the commissioner's ability to share information with counterparts domestically and internationally is also a good idea”.

I think everyone on the committee here agrees that when multiple organizations are working towards the same purpose, it's important for them to share valuable information with one another. Although I understand that the kind of information the Privacy Commissioner would share would be different from what the national security organizations would share, the overall principle that information sharing is important would still apply.

With that, would you agree that our national security organizations need to have the tools to share information so they can effectively protect Canadians?

● (1140)

Mr. Michael Karanicolas: That's a very broad statement, so it's tough to fully endorse it. I do think that information sharing by itself is not necessarily a bad thing. As you point out, obviously agencies need to be able to work together, and if you have two agencies with a different mandate, and one of them has information that is of relevance to the other's duty, certainly information sharing is not necessarily negative. It just needs to be done, first of all, with respect to the principle of data minimization. You need to look very carefully at the organization's mandate to see what kind of information it is keeping, what kind of information it is sharing, and what kind of warehouse it is building, and be sure that is done in a way that's going to keep this information secure and protect the privacy of Canadians. Then beyond that, I would say there's a strong need for clear rules to be put in place.

I don't think we're hostile to sharing information. I think our broad point is that it needs to be done according to clear and carefully constructed rules to ensure that the system operates and that the system can't be pushed in abusive directions.

Mr. Matt Jeneroux: Okay.

Then notwithstanding your concerns with regard to the privacy safeguards on the information-sharing tools in SCISA , do you think this legislation helps our national security organizations do their job more effectively?

Mr. Michael Karanicolas: It's difficult, because I'm not viewing things through their lens. It's a little bit difficult to express that.

I do want to echo the remarks of my colleague when she said that there hasn't necessarily been a proper case made for the necessity of new legislation. We've taken a position for improving the legislation rather than repealing it largely because, as a matter of advocacy, we generally look toward how to make systems better rather than toward repealing legislation entirely, because there's always a risk that the legislation is going to reappear.

Generally speaking, I don't necessarily know if the case has fully been made, but it's a little bit difficult to assess that because, again, I don't have access to the information on how this stuff works that others might.

Mr. Matt Jeneroux: Okay.

How do you believe we can balance helping our national security organizations more effectively to do their job while protecting the privacy rights of Canadians?

Mr. Michael Karanicolas: I think the recommendations that have been spelled out, first by the Privacy Commissioner and then by Roach and Forcese, are a good start. I think that expanding the role of the Privacy Commissioner, as it appears is being done—particularly the move to order-making power, which I was ambivalent about—is a good step in this regard. I was ambivalent about it regarding the private sector; applying it to the public sector I think is quite good.

It's a big question to answer. Generally speaking, it's just about putting proper safeguards in place. That's kind of a vague answer, but I can unpack it more carefully with respect to specific aspects of it if you want.

Mr. Matt Jeneroux: I think how we find that balance is probably the biggest question before the committee in a lot of ways.

If there's anything else you want to add, to unpack a little bit, we'd be happy to hear it. I think it would help us as we continue our deliberations.

Mr. Michael Karanicolas: Proper oversight is key. I just mentioned how I don't necessarily have the full picture. It's important to have an oversight body that has access and can view the full picture. There can be a danger in terms of stovepipe oversight, whereby oftentimes the overall harm of a particular system is greater than the segmented harm of each individual component of it, so it's important to allow an oversight body to get the full picture and to have access to classified information that would let them fully see if the measures that are being taken are appropriate to the needs of the security agencies.

I want to echo what we heard previously about the need to make the case not only internally in that regard but also to Canadians, and to show why we necessarily need to expand our powers more than they've already been done.

I think that we've seen that the tool kit, the level of powers of investigation, of data processing, of law enforcement and security agencies have all expanded exponentially over the past few decades, and I don't necessarily think that there's been a concomitant understanding about the implications of this to privacy rights of Canadians. I think there needs to be a consideration of the significant expansion of information sharing and surveillance that has taken place in the historical context, but also I think context is important in terms of the threats that we face today. Terrorism has been around for a long time, and I think we need to ask ourselves if we are necessarily facing unprecedented threats. Are we facing threats that are greater than they were during the FLQ crisis, greater than the U. K. faced in the 1980s from the IRA?

These are challenges that we've dealt with previously, and we've been able to establish safeguards in place that properly respect Canadians' privacy rights. I'm not sure if the case has been made that there's a new challenge that justifies additional legislation.

● (1145)

The Chair: I think we're at the end of your time, Mr. Jeneroux. We'll now move on to Mr. Blaikie, please.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thanks very much.

When we're engaged in this debate about privacy and striking the right balance, I think it's easier for people to understand what it means if intelligence services fail and someone is successful in perpetrating a terrorist attack, for instance. I wonder if any of the witnesses would like to help give us an appreciation of what it means for individuals when information sharing takes place on the level that SCISA allows and what the potential harm to real people is if you don't have proper information-sharing practices in place.

The Chair: Why don't we start with Micheal Vonn?

Ms. Micheal Vonn: Sure. Thank you very much for the question. It's part of why I wanted to bring up the issue of the mandate of the various agencies.

As I'm pointing out, the real-life effects of this are right now. People who are talking about such issues as how we are going to make an effective national pharmacare system in Canada meaningful for people's health are saying, “Oh, dear; what about SCISA and the fact that Health Canada is impacted by this detrimental impact on patients' information rights?” That is affecting people in their ability to essentially govern ourselves, benefit our health, etc. On a very real level, these discussions right now are impeding our ability to effectively govern ourselves.

On an individual level, it has mass implications. As I say, I am of the opinion—and I share it with various of my colleagues—that if you were going to do one thing to reduce the abuse power of SCISA, make it so that you could not have bulk data transfers as part of it.

If there was confusion about what individual suspicion standards of information sharing should have happened in the past, again, we could have clarified those in the Privacy Act. Instead, we enacted an act in which it was very clear that bulk data transfers were facilitated. The kinds of profiling that bulk data is used for have a devastating impact not only on some individuals, which they have brought to our attention that they do not deserve—they may find themselves on the no-fly list, the slow fly list, or other various aspects, on the basis of profiling without any individualized suspicion—but entire communities are impacted by being under the threat of racial and religious profiling.

I could go on about this subject for quite a while, but I'm going to keep it narrowed to those examples because I think they speak to both the front-end chill and the ultimate impact of where we do have very reasonable grounds for suspecting SCISA was essentially enacted, which is about the bulk data holdings.

Mr. Daniel Blaikie: Thank you.

The Chair: Go ahead, Ms. Austin.

Prof. Lisa Austin: I would just add that I agree with those comments. I think there's a real and serious issue about trust in government when you have an act that contemplates the sharing of the entire government with these recipient institutions. I think there would be a lot more support if it was information sharing within the recipient institutions and understanding that they share certain kinds of national security interests, but when it's the entire government, then you undermine the trust of Canadians, who often have no choice but to share information for all sorts of government purposes. I think that is really an important aspect that is not taken into account here with the sheer breadth of the sharing that's contemplated here.

● (1150)

The Chair: Go ahead, Mr. Karanicolas.

Mr. Michael Karanicolas: I'll add to what my colleague said. I think it might be useful just to flesh out a little an example of why when datasets are combined they can be way more privacy intrusive than the sets considered in isolation. I can give you an example from the private sector that helps to make this point.

There is an app that was published and was called “Girls Around Me”. Basically, it combined two sets of publicly available information: information from Facebook profiles, which is generally about people's pictures and their likes, dislikes, interests, and what have you, and then information from Foursquare, which allows people to use their iPhones to check into a particular thing, such as “I'm at this restaurant, I'm at this movie theatre, I'm at this bar”, or whatever. Combining those two datasets, which in isolation have their own concerns but are not super-intrusive, basically creates this stalking app that allows people to look at their phone and say that in this restaurant there is a girl, here's what she looks like, here's what her interests are, and here's everything about her.

Again, you take these two datasets in isolation and then put them together, and suddenly you have something that is far more intrusive than the two taken separately. That's an example from the private sector, but I think it does illustrate the harm and the concerns that can come about when these datasets are combined, particularly echoing what my colleague said about the fact that, in dealing with the government, people don't necessarily have a choice when they're sharing this information. When you're dealing with communities that are under risk and already have a good reason to be suspicious of their interactions with government, I think these are very good illustrations of the kinds of concerns that come into play.

Mr. Daniel Blaikie: I think we've heard already from you, Mr. Karanicolas, that your organization is recommending changes to SCISA, and we heard from Professor Austin that her choice would be to have a straight-up repeal of SCISA.

Ms. Vonn, does your organization have a preference? Do you think it would be wise to just repeal the legislation, or do you think that changing it is the way to go?

Ms. Micheal Vonn: Our view is that the repeal of the act is certainly the preferred methodology for bringing accountability to this question.

Mr. Daniel Blaikie: Let's say that did come to pass. Is there anything in SCISA that you think should be preserved in terms of helping intelligence agencies do their jobs better?

Ms. Micheal Vonn: I'm very suspect of “more powers equals greater efficacy”. At the same time that the civil liberties organization is very much of the view that there is more than one good and that national security is a powerful good, we want to ensure that the appropriate tools are in the hands of our intelligence agencies. In order to do that, we need to understand the problem in greater specificity. If the problem was literally that there was some difficulty in understanding what the provisions already allowed for in the exemptions for disclosure in the Privacy Act were, then clarifying those exemptions is clearly the tool that we need to address those.

Again, if that were required in order to get appropriate information sharing on an individual basis, we would be very much in favour and and would roll up our sleeves to help draft that provision.

Mr. Daniel Blaikie: Thank you.

The Chair: We now move on to Mr. Saini, please, for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning. Thank you very much for being here.

I want to pick up on a point, Ms. Austin. You mentioned the Arar inquiry. I want to get an opinion from all of you, but I'll start with you, Ms. Austin.

One of the recommendations that was made in the Arar inquiry was as follows:

> Information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture.

Just generally, what safeguards does Canada have in place to make sure that doesn't happen? Does SCISA have any provisions in and of itself to ensure that this doesn't happen?

● (1155)

Prof. Lisa Austin: I can't speak to general provisions in other legislation. I would defer to some of my colleagues in the national security space with respect to specific agencies and their mandates.

I was surprised that it's not in SCISA, given that it's clear that this also empowers sharing with foreign governments. Why is there not a provision that it must be part of the set of protections, given everything the Arar commission says? Again, that goes to my general point that I think those kinds of safeguards, I would say, are pretty much constitutionally required, not just as a recommendation of the Arar commission. I think it's problematic that they're not there in this act.

Ms. Micheal Vonn: I can jump in.

Thank you very much for your question.

Currently ministerial directions expressly allow for the sharing and importation of information that might contribute to or be derived from torture. One of the things that my association has called for—along with many colleagues, including Amnesty International—is the immediate repeal of those ministerial directions of some years' duration that do allow for or make provision for.... They're supposed to be scrupulously scrutinized in terms of their necessity, but, as I say, it flies in the face of international law and human rights protections to say that this can be effective.

We know that very little actionable intelligence is derived from torture, and security agencies will confirm this. Not only is torture a grave human rights violation, but it produces no actionable intelligence. You are very, very likely to get faulty intelligence from information derived from torture, and yet we continue to have in Canada an allowance for such information. Torture-tainted information is, I would suggest, a deep human rights scandal in this country and one that, as I say, we voiced in terms of the national security consultation.

Mr. Raj Saini: One of the reasons I bring this up is that there have been some comments from president-elect Trump that he may authorize torture in some very specific circumstances.

As part of the Five Eyes and also because we share continental security within North America, it would be very difficult for us not to share information with the United States. Is there something we can put in our own domestic legislation that can protect us from that?

Ms. Micheal Vonn: Certainly, as I say, repealing those ministerial directives would be stage one, and then expressly prohibiting such torture-tainted information would be very, very welcome.

Mr. Raj Saini: Do you have any comments?

Mr. Michael Karanicolas: Just to disagree with you slightly, I don't think the incoming administration's view is that torture should be used in a highly limited and specific way; in the statements I've heard, he seemed to be endorsing it extremely broadly. Certainly I agree with everything that my colleague said in terms of repealing those ministerial directives.

I also want to add more broadly that I think that now is potentially a time when Canada can and should be exercising strong moral leadership on this issue when questions of international human rights law are being threatened in this kind of way. I think that Canada should take a very strong stand on that.

I'm glad you brought up the recent election with regard to this issue, because I think we can talk about the Arar commission and people being transferred to Syria, but when our closest intelligence partner is taking a stance like this, I think it does force some very significant questions on Canadians about what our moral duty is in terms of the way we conduct ourselves.

Mr. Raj Saini: Do I have any time remaining, Mr. Chair?

The Chair: You have several minutes.

Mr. Raj Saini: Just to close up on this question, the one thing I want to ask about is that within SCISA there is no civil liability requirement. Do you think there should be some judicial recourse for those people who are unfairly or improperly targeted or under scrutiny, who may have had some harm caused to them?

Ms. Micheal Vonn: May I say that when I did education on what was actually in Bill C-51, there were often audible gasps in the audience when people found out that those who might be rendered to torture, Canadians, would have no civil recourse under SCISA because of the liability waiver that is part of it—and this is, of course, something that has happened.

Citizens of Canada who know this about this portion of the act are appalled.

● (1200)

Prof. Lisa Austin: I would agree with that. I would just go back to my general point that when you create a law for information sharing around national security, you need to maintain the trust of Canadians. A provision that there is no recourse for those who are abused undermines the trust of Canadians.

I think it also connects not just with privacy concerns but with equality concerns, because who is going to feel most targeted potentially by that? I think it causes a lot of ill will unnecessarily. Is there really such a risk of abuse? I hope it's not the position of the government that it would require that provision.

Mr. Raj Saini: Mr. Karanicolas, do you have a comment?

Mr. Michael Karanicolas: I would generally support those kinds of provisions as well. I do think there needs to be accountability, and while we've seen certain provisions in there for good faith, those don't necessarily apply to this kind of a case, so I would concur with my colleagues.

Mr. Raj Saini: That's fine.

The Chair: We'll now move to our five-minute round, colleagues, starting with Mr. Kelly.

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

Now that I have the floor, I would like at this moment to move the motion that was put on notice last Friday.

> That the Committee invite the Minister of Democratic Institutions to testify before the Committee, at the earliest opportunity, regarding what steps she and her ministry have taken to ensure that the privacy of Canadians is protected, according to the provisions of the Privacy Act, when they enter demographic information into the survey at my democracy.ca.

The Chair: Your motion is in order, Mr. Kelly.

Do you wish to speak to it at this time?

Mr. Pat Kelly: Yes, I would.

I believe we need to hear from this minister regarding the MyDemocracy.ca program that she has. Changing or retaining Canada's electoral system has been an important topic over the past year. A special committee was formed to study the issue, and it reported earlier this month. I myself travelled with the committee during part of its tour through the western provinces and territories.

However, the minister was somewhat dismissive of the committee's report. She conducted her own parallel consultations on the topic and has now has launched a third party survey on democratic values, ostensibly to consult Canadians indirectly instead of through a referendum, as recommended by the special committee.

We've heard much about the survey at MyDemocracy.ca of late. It asks a series of oddly drafted questions with many conditionals or what-if statements. It doesn't actually ask what system a responder would prefer and does not give the option to call for a referendum. It allows responses from out-of-country IP addresses, which is interesting too, if a responder provides a Canadian postal code.

Most interestingly for this committee, it asks for significant demographic information, which may be used to identify individuals. This last point has attracted the attention of the Privacy Commissioner, who is now investigating the survey due to his concerns about Canadians' privacy.

While he's conducting the investigation, we can't call the commissioner. We certainly can't question the commissioner while an investigation is in process. We will wait until he has completed his investigation before we can hear from him.

In the meantime, I think we should provide the Minister of Democratic Institutions a chance to tell the committee more about this survey. The survey has been met with widespread and, I would say perhaps, universal ridicule, which discredits the process itself. The fact that the process is under investigation by the Privacy Commissioner also means that perhaps the most important thing we can ask this Parliament about is what our democracy will look like in the future.

She stated in question period last week that the survey protects respondents' privacy pursuant to the act. That's what she said. Time certainly did not allow for her to discuss specifics. In contrast, by appearing before the committee, she would have the time for a detailed discussion of an important concern for privacy in light of an important national discussion.

There are many questions we could ask her, and there's substantial expertise now around this table on privacy matters from the numerous witnesses we've heard from and the study we have completed. Many of these questions have in fact been asked in the House and have not really been answered. For instance, what will the government do with all of this information that it is collecting as part of the study? Will the information be destroyed at the conclusion of the study? If not, what further use would be made of people's demographic information, together with their answers to these value questions about opinions on democratic reform?

This is a timely issue. It's an important one for Canadians. I think this is the place where it should happen.

In terms of scheduling, we won't be meeting again until late January. There should be ample time for the clerk to find an agreeable time for the minister.

I would move that we have the Minister of Democratic Institutions appear before the committee.

● (1205)

The Chair: I have a speaking list, colleagues.

I'll just let our witnesses know that we should be through this little bit of business shortly. Please just bear with us.

Go ahead, Mr. Blaikie.

Mr. Daniel Blaikie: Thank you very much. I just wanted to take a moment to speak in favour of the motion.

One of the things we've been discussing even in the context of our study of SCISA has been a necessity test. It was very interesting to hear that as part of the government's survey, Canadians have to submit information having to do with their level of income, for instance, and a bunch of other things that I don't think are obviously necessary to the government getting their opinion on what kind of voting system we would like to have.

I think there are some interesting questions that bear even on issues that we're discussing in the context of our study. It might be helpful to get the point of view of the minister to better understand why she believes this information is necessary.

Also, it would be good to get a better idea of what they are going to do with that information. When the minister has been asked questions about why the government would want that kind of demographic information on respondents, her answers, frankly, have been quite evasive in the House. She says, you know, it's not a requirement that you provide that information in order to complete the survey. Presumably Canadians are filling out that survey not because they care to know whether Vox Pop Labs thinks they are an innovator or a guardian but because they want their preference to be registered. Although she has refused to say, it does say on the website that if you don't provide that information, then your preferences and the information that's actually germane to democratic reform—if anything really is out of that survey—isn't counted.

I think having her come here with more time might allow us to get a better answer from her as to whether or not it serves any purpose at all, other than to get that opinion on whether you fit into whatever categories the company that designed the survey came up with. I think filling out that survey if you're not prepared to provide that information would be very useful.

In our last study that has been referred to today on the Privacy Act, we talked about government exploring ways to see the Privacy Act apply to minister's offices. I think this MyDemocracy.ca survey is a great example of why Canadians might want the Privacy Act to apply to ministers' offices, because one wonders really what the point of collecting that information is, if it isn't ultimately for some kind of profiling or outreach. I don't see that profiling people is useful to government with respect to their preferences about democratic reform. I can imagine how it would be useful to the Liberal Party of Canada. Therefore, I think getting some more precise answers from the Minister of Democratic Institutions as to why it's important to government to have that information would be very good.

For all those reasons, Mr. Chair, I do support this motion.

The Chair: Thank you, Mr. Blaikie.

Go ahead, Mr. Jeneroux.

Mr. Matt Jeneroux: I would also like to speak in support of this motion. As Mr. Kelly indicates, it's incredibly timely, owing to a variety of concerns that our side of the House has with the survey, particularly the demographic information. We're asking Canadians to fill out this information in good faith without accurately telling them exactly where it's going.

If I were on the other side of the table, I would think this is a tremendous opportunity to have the minister come before us here and explain in more detail what exactly is happening with this information. Is it going to the Liberal Party of Canada? Is it going to the minister's database? These are questions that we would like her to clarify. She would have the opportunity, if she comes here before us, to take that time to clarify. In particular as it pertains to privacy, the Privacy Commissioner would also be someone pertinent, if he has an ongoing investigation on this. He might have some thoughts on this as well.

I think we should have the minister here before us to clarify what exactly it means when Canadians are being told that they are guardians. Where is that information going, and how exactly can we ensure that information is being protected? I would hate to think it was going to the Liberal Party of Canada for perhaps another fundraiser of some sort.

I think this would be a tremendous opportunity for the those on the other side to call the minister here and have her explain to us so that we can answer some of these questions and there's not the type of speculation that Canadians right now are curious about.

Thanks, Mr. Chair.

● (1210)

The Chair: Thank you, Mr. Jeneroux.

Mr. Lightbound is next.

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you, Mr. Chair.

I can appreciate that my colleagues have a lot to say on this important issue, but considering that we have witnesses in different time zones—and I'm thinking of Ms. Austin, who flew in to testify before us—I move that the debate be now adjourned.

The Chair: This is a dilatory motion, and I must call for a vote immediately.

Mr. Matt Jeneroux: Can we record the vote?

The Chair: We can.

Mr. Clerk, will you please call the roll?

(Motion agreed to: yeas 6; nays 3)

The Chair: Thank you to everyone involved. The motion to adjourn the debate on the motion that was before us has been sustained.

We will now resume the agenda that we had previously, and we'll return to Mr. Kelly for his five-minute round of questions.

Mr. Pat Kelly: Thank you, Mr. Chair.

To our witnesses, thank you for your patience.

I know we've heard concerns from many of our witnesses about the necessity versus “undermines the security of Canada”. If I understand the positions correctly from our witnesses, we have two who want to repeal the act completely and start over, or not start over, and Mr. Karanicolas, if I understand you correctly, you want to perhaps not necessarily abolish the act completely, but make numerous changes.

Many Canadians—and I think of the people in my own riding, when I knock on doors and when I meet people—if they thought that an intelligence-gathering agency or a security enforcement agency of some sort, a law enforcement agency, possessed information that undermined the security of Canada, they might feel that it may be appropriate to share information that undermined the security of Canada with a more appropriate agency to exercise its judgment and deal properly with that information.

Perhaps make the case again, or explain it in a way that would resonate with residents who have concerns about those who would undermine the security of Canada.

Perhaps we'll start with Ms. Austin.

● (1215)

Prof. Lisa Austin: Thanks for the question. I think it's a great question.

The one thing that strikes me in examples like this, and the one you're giving too, is that as I said before, there is much broader popular support for information sharing within agencies that have a national security mandate. Where I think the trust issue becomes much more problematic is when you say, “Oh, this isn't about an intelligence-gathering agency or an enforcement agency possessing information and then sharing it with some agency that they think is more appropriate. This is about any government department sharing with these recipient institutions.”

The sheer breadth of the information sharing contemplated here is part of the problem with the basic justification for this. The specific targeted improvements on how information is shared come out of the Arar commission and the Air India inquiry, and there's, I think, great support. It's always a case of the devil's in the details, right? I think specific information sharing within agencies with national security mandates, with appropriate protections and accountability, sounds all right. Broad information sharing that also contemplates bulk access in ways that haven't been disclosed publicly, with potential additional concerns around equality and profiling and association and expression, is part of the problem here.

Justifying this act based on examples around narrow information sharing is part of the issue. I think people accept the narrow information sharing. It's the breadth of what's contemplated here that's the problem.

Mr. Michael Karanicolas: Just to clarify my position and my organization's position, we're not necessarily opposed to repealing the law itself. As I said, I'm not necessarily sure that the case has been made for the law's necessity, but I just generally find that it's better to come to these things with recommendations in hand to improve the law as well, which is why I framed the issue the way I did. However, I don't think my statements should be construed as being broadly supportive of the law.

It's a bit of a straw man to frame the conversation the way you did, because I don't think that anybody around this table is opposed to information sharing in all circumstances. Obviously there are going to be cases where it's essential and important to share information, and we want our intelligence agencies to work together to protect Canadians. As my colleague said, it's important to have proper safeguards around that front and to make sure it's done with respect to our core democratic values. To frame the debate in that way, the security of Canada is also tied into our constitutional and democratic values, including our respect for human rights. That's a core part of who we are. That's what we're meant to be defending.

I think it's important to understand in the debate that nobody's arguing that Canadians should be under threat or face greater threats; it's just important to establish our response in a manner that protects core democratic values that have served this country for quite a long time, have seen it through difficult times before, and should be maintained.

Ms. Micheal Vonn: Just quickly, I'll say that the Canadian citizens I talk to are very concerned about the new terminology. “Threats to the security of Canada” is something we understand. That's embedded in our national security legislation and jurisprudence. As for “undermine the security of Canada”, when people read the list of what that includes, it includes ordinary public life, it includes the administration of justice, it includes the financial stability of the country, it includes undermining the security of other countries. People say, “My word, what does that mean?” We say, “We don't know.” Nobody knows what this means. It's a new definition. It hasn't been tested.

Clearly, the list that's included in the legislation is extremely broad, unprecedentedly broad, in terms of national security legislation. I think that is part of the essence of what concerns Canadians.

● (1220)

The Chair: Thank you very much, colleagues.

The shorter we keep the preamble to our questions, the better the chance of finishing within our allotted time.

We'll now move to Mr. Lightbound, please.

[*Translation*]

Mr. Joël Lightbound: Thank you, Mr. Chair.

Ms. Austin, in a way you answered my question earlier when you said that national security agencies weren't necessarily included in the Security of Canada Information Sharing Act. However, over 140 agencies can share information. Even the Yukon Surface Rights Board can do so. There are 17 agencies that can receive information, including the Public Health Agency of Canada and other agencies whose roles are less clearly linked to national security.

To ensure these agencies actually have a role to play in national security, do you think there's a need to review, and limit, the number of agencies that can share information and the number of agencies that can receive information?

My question is for the three witnesses.

[*English*]

Prof. Lisa Austin: Thank you for that question.

More attention needs to be paid in SCISA to this incredible breadth, as I've been saying about so many agencies involved in potentially sharing information with a small group. As you said, some of them themselves have a tangential relationship with national security.

I would just point back to the Arar commission's report, which suggested that some of the existing exemptions in the Privacy Act—including the public interest exemption that says where there's a public interest that outweighs the privacy interest of the information, information can be disclosed—met all sorts of needs.

Again, my question around the overbreadth of this act is, why not...? Obviously I've said you should repeal it. If that's not the case, why not scale it down to a much narrower set of institutions that are sharing information? If it so happens that there's information that some other unrelated agency has that they think really should be shared, why isn't the public interest exemption perfectly adequate? It's already right there in the act. Again, in terms of justifying the overbreadth, I'm having trouble seeing that broad scope of the act, and a lot of the examples being offered as to why it's needed contemplate a much narrower set of information sharing, which I think you have a much greater chance of getting Canadians on board with.

The Chair: Go ahead, Mr. Karanicolas.

Mr. Michael Karanicolas: I'm still formulating it. Do you want to go first?

The Chair: Go ahead, Ms. Vonn.

Ms. Micheal Vonn: Certainly. Thank you.

I was just going to say that I would only be paraphrasing my co-panellist Professor Austin's remarks. I concur completely.

Mr. Michael Karanicolas: It's a bit of a challenge to define where the information should or shouldn't be, and who should or shouldn't be involved with sharing the information, particularly because, with the advance in big data, there is an enormous expansion in information that could potentially be relevant to security investigations. I suspect that would raise troubling questions for Canadians who think they're providing information to the government for a particular purpose and it ends up being processed in order to investigate crimes.

The things you mentioned in the discussion that just took place—the information entered into the MyDemocracy.ca website—is a good example of that. What if that fed into the RCMP, and people found some correlation between views on democracy and probability to commit a crime, and suddenly it was processed in that way? That's a strange example, but I think it's important to consider very carefully the relationship Canadians have with particular government agencies. If they're giving information that they feel is for a particular purpose, it might be troubling to them to know it's going to be used to investigate them or to process whether they're going to be suspected of any kind of wrongdoing.

Again, we're not necessarily hostile to sharing information, but I do think it's important to consider the relationship Canadians have with these government institutions and the way this principle that anything you say around anybody in government is potentially going to be used as part of an investigation against you will impact the relationship and the way Canadians interact with governments.

● (1225)

[*Translation*]

Mr. Joël Lightbound: My second question concerns the civil immunity provision.

You spoke about it earlier, Mr. Saini. Ann Sheppard, who appeared before our committee as counsel for the Department of Justice, told us this provision was never meant to exempt the Crown from all prosecution.

[*English*]

The Chair: Excuse me, Mr. Lightbound. I'm sorry. I'm not getting any translation here. Is everybody else getting it?

You're all good.

My apologies, Mr. Lightbound.

Mr. Joël Lightbound: I wasn't talking about you, Mr. Chair.

The Chair: I understand that.

[*Translation*]

Thank you.

[*English*]

You can keep going.

I'll need to figure out why my interpretation is not working.

[*Translation*]

Mr. Joël Lightbound: I was saying that Ms. Sheppard told us the goal of this provision was not to protect the Crown, but only to protect the public servants. I want to know whether the witnesses interpret the provision the same way.

Ms. Austin, since you're a law professor, I want to know your view of the legal impact of section 9 of the Security of Canada Information Sharing Act.

My question is also for the other witnesses.

[*English*]

The Chair: Seeing that we have no takers and that we're well past the six-minute mark on your five-minute round, is there somebody who would like to give a quick response?

Ms. Micheal Vonn: I can certainly give a quick response. I thought there was a small glitch in the sound, so forgive my hesitation there.

I certainly read the clause as one in which the crown was waiving its own liability, and not civil servants. If failure to achieve clarity in that clause was evident to us, it will be evident to most Canadians, I would think.

Prof. Lisa Austin: I would add that because the word “person” is there, I would automatically assume it includes the crown. If it's not meant to include the crown, it would be a useful amendment to say that the crown can be liable.

Again, if you move to a necessity standard.... There was the question earlier about what happens with the civil servant who is worried about misjudging that line in terms of sharing information, so it seems useful to keep some provision to say that a good-faith interpretation of this isn't going to get you into trouble, as a way of maintaining a higher threshold, rather than having some kind of dual notion or keeping relevance.

I think this is a serious issue to clarify with respect to whether the government is trying to get out of liability, because then people are just thinking, “Oh, you want to make sure there's not another Arar”, but that's horrible, right? What happens if the same situation arises?

The Chair: Thank you.

We now need to move on to Mr. Jeneroux, please.

Mr. Matt Jeneroux: Thank you, Mr. Chair.

I have one question for all the witnesses, but before that, Mr. Karanicolas, you brought up a great point. We just don't know what we don't know about the MyDemocracy.ca survey. It would be nice to get some of that clarification. I appreciate your putting that on record.

The one question that I have for all witnesses is this: do you believe there are any situations where the need to protect our national security might supersede the right to privacy?

I'll start with Mr. Karanicolas.

Mr. Michael Karanicolas: Just to clarify, that wasn't really an endorsement of the need to...of concerns with it—

Mr. Matt Jeneroux: I heard what I heard, Mr. Karanicolas. I appreciate that again.

Mr. Michael Karanicolas: Okay. Just to clarify, I was using that as an example of information that's fed into the government, because it had just been mentioned.

In terms of balancing security, yes, absolutely, I think a core function of democratic systems is that they balance different interests against one another, and balancing security against privacy or security against freedom of expression is something that all mature democracies have to do.

There are going to be cases where security does trump the privacy of Canadians. We have warrants for investigation that involve exactly that kind of measuring. I think there are certainly going to be instances where that happens. I think no reasonable Canadian would say that people have an absolute right. It's just a question of how to balance rights in a way that fundamentally best protects Canadians, including respect for our traditional values.

● (1230)

Ms. Micheal Vonn: I can jump in after that. It's a very easy answer. The answer is, of course, yes, but our constitutional rights are framed this way: we have a right to be protected against unreasonable search and seizure, and that means that post hoc figuring it out is not the way to do it. The question is not, "Does security ever trump privacy?" Of course it does. The question is, does SCISA provide us with the constitutional protection that we require to be protected against what is unreasonable—not what is justifiable and reasonable, but what is unreasonable? That, I think, is the heart of the SCISA question.

Prof. Lisa Austin: I would add to that. I think section 8 jurisprudence is not about preventing state access to information; it's all about ensuring that when the state gets access to information for law enforcement or national security purposes, it's within a very protective set of accountability mechanisms. The devil is in the details about what those are.

I would also add that there is some support in the jurisprudence, although it's very undeveloped, for protecting privacy under section 7 as well, and then it's balanced against the principles of fundamental justice. There is a lot of balancing that goes on in the charter. That's why the questions about overbreadth, safeguards, protections, and thresholds all become really important in striking that balance fairly, but everyone agrees that of course national security sometimes means that you get access to it—absolutely.

Mr. Matt Jeneroux: Mr. Kelly is next.

The Chair: You have about a minute and a half left, Mr. Kelly.

Mr. Pat Kelly: I have a quick question—well, maybe it's quick, but I don't know—for Mr. Karanicolas. In an earlier answer you gave, you made reference to the long history of terrorism as a threat, and you cited some historical examples.

I completely agree that terrorism has been around for a very long time, but what is different now, really, is the nature of the collection and transmission of information. This is much different from when earlier terror threats were addressed by various countries. In light of that, would you not say that older methods and older attitudes toward data collection and sharing do in fact require more contemporary solutions?

Mr. Michael Karanicolas: Yes, methods should certainly evolve, but I'm not sure that our values necessarily should.

Obviously, nobody is suggesting that law enforcement agencies and security agencies should be existing in the 20th century. They should be using the Internet. They should be monitoring electronic communications as appropriate. Certainly there is a need to have up-to-date investigative techniques, but at the same time, my point in framing the idea that terrorism has been around for quite a while is to counter the idea of the narrative that's come out, which is to almost present this as an unprecedented kind of threat, as if the gravity of what western countries face today is vastly beyond anything we've seen before.

You can look to parallel examples again. You can look to the U.K. in the 1980s and to what Spain faced with the Basque separatists, and you can see that time and again western democracies have faced threats that were far more serious, you could argue, than are being faced today, and have managed to persevere. I think that level of historical context is important in terms of maintaining our values and our respect for privacy, in terms of keeping that balance, as opposed to saying that law enforcement shouldn't adapt and improve their technology to make use of new technologies that are available.

The Chair: We'll now go to Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): I'm going to take you all back to October 22, 2014. I was the mayor of Hamilton. It was a beautiful, sunny morning. As I got to the office shortly before 10, we heard about the shooting on the Hill. Within about half an hour, we learned that it was one of ours, a Hamilton Argyll. Before noon, we understood that Corporal Cirillo had died. Early that afternoon, the police chief and I visited the family. On Friday, I rode in the motorcade—there was an unbelievable turnout of people along the Highway of Heroes—and the subsequent funeral was one of the major military funerals in Canada in recent history.

The events and the response by the people cried out for a response from the government. The government did respond, whether or not the response has been perfect.

Can I to start with you, Ms. Vonn? If you put yourself in that mind frame, at the time how did you see what would become of this, and then, how did you see the way the government subsequently took the matter into its hands?

● (1235)

Ms. Micheal Vonn: I think that certainly, along with many Canadians, we saw the initial polling on what was then Bill C-51 as something with great emotional sympathy for the crisis, the tragedy that had occurred. Overwhelming numbers of people said yes, we must have a response. Then you will recall that very shortly afterward—I can't remember if it was weeks or some very short months—when people had had an opportunity to acquaint themselves with the bill, the majority of people who did so and were polled said that they did not support it and that the point was not that we must do something but that we must do the right thing. It must be proportionate, necessary, and effective, and this was not found to meet the measure.

We certainly understand the need for responsiveness, and we don't slight that in the least. The question is whether, with sober hindsight now, when we apply our rationality to this, we have effected an improvement.

As Professor Austin was indicating, we have no indication of efficacy. As the community of privacy commissioners of Canada has said, we have actually achieved no reasonable justification for these extraordinary powers. Do we know that they are making us any safer? We do not. Instead, as I hope I made clear in my submission, we actually serve to harm some of the federal institutions that are part of the architecture of our government by imposing this information-sharing scheme on them.

We should consider very carefully not whether we have tools but whether they are the right ones.

Mr. Bob Bratina: Mr. Karanicolas, could you comment?

Mr. Michael Karanicolas: I would echo what my colleague said regarding the need to look back in hindsight. A tragedy can give rise to particular kinds of legislation, which can be reactionary or can overstep or can fail to achieve a sober balance. We've seen that time and again.

We saw that in the U.S. after the September 11 attacks. There was a huge increase in the security establishment and in surveillance. People look back on that, and there have been increasing concerns over time.

Certainly I do understand that when we have a highly emotional and tragic event, there can be a drive to push legislation in a particular direction, but reflecting in hindsight is indeed the best thing we can do.

Mr. Bob Bratina: Ms. Austin, why do you suppose the government went in the direction it did in terms of creating the controversial legislation we're now discussing?

Prof. Lisa Austin: I don't have any insight into why the government chose to do as many things as it did within Bill C-51, but I would say there's a very delicate balancing act in which there are legitimate needs, as Mr. Kelly has been pointing out in his questions too, for the national security agencies to have the right powers to do the job we all want them to do. When these tragedies happen, that's the emphasis in the mind of Canadians.

If you go too far in overbreadth of new powers, then you're going to hit the other end, which is undermining trust in government. I think Bill C-51 goes too far in that direction. Specifically, obviously my comments today are on the information-sharing act, and I do think there's a delicate balance, but I think this isn't the right balance.

The Chair: Your time is up, unless you have a quick supplementary to follow up, Mr. Bratina.

Mr. Bob Bratina: No, I have a long one, so go ahead.

The Chair: Well, we'll get back. We'll have time.

Mr. Blaikie will finish us off with the official allocated time for questions.

● (1240)

Mr. Daniel Blaikie: Thank you very much.

Ms. Vonn, I would come back to a similar line of questioning that I had before.

I'm trying to understand the importance of having good privacy protections for public policy. It seems to me that it wasn't that long ago that we had a debate in Canada around whether or not we should have a gun registry. Critics of that policy at that time were very articulate about concerns over government having certain kinds of information and what it would mean if that were shared or if the government changed its policies and had that information on people.

Do you not think that the people who were critics of the gun registry should be the first to stand up for very strict rules around information sharing within government, because they understood so well what the risk to ordinary Canadians might be if government had lots of information and was able to share it without discrimination?

Ms. Micheal Vonn: I'm not sure that I can provide an answer on that.

I certainly know that for many people there are a patchwork of sensitivities where they are concerned about privacy and where they believe other people shouldn't be concerned about privacy because they themselves aren't. I think we need to take the most broadly democratic view and identify where we have concerns that actually reflect on the health of our democracy, and this would be one sphere in which we do.

Again, let me give you another very concrete personal example. People in British Columbia who work for environmental agencies will tell you that when they go door to door asking people if they would like to sign this petition, if they would like to make their democratic voice heard as a citizen of a democratic country, people will say, “Will this get me on a list?”

There is a grave concern about the dragnet of bulk information gathering and how it will prejudice people in the ordinary course of their participating in democratic governance.

When you look at a harm that is that profound, you have to say that information sharing on the scale envisioned in SCISA is having some fundamentally detrimental effects.

Mr. Daniel Blaikie: Thank you very much for that answer.

Thank you to all our witnesses for participating here today.

As we are now pretty much at the end of the official round of questioning, I would like to move that we resume debate on my motion from meeting 36, and therefore the subsequent amendment by Mr. Kelly.

The Chair: As it's a dilatory motion, we proceed directly to a vote.

All in favour of resuming debate on the previously adjourned debate on the motion previously tabled, please so indicate.

Mr. Daniel Blaikie: Will this be a recorded vote as well?

The Chair: It can be, as soon as we're all clear on what we're voting on.

We're voting on returning to the debate of the motion brought forward by Mr. Blaikie, subsequently amended by Mr. Kelly, on which the previous debate was adjourned at a previous meeting.

This is a dilatory motion. I've been asked for a recorded vote to return to that debate at this particular point in time.

(Motion negatived: nays 6; yeas 3 [See *Minutes of Proceedings*])

The Chair: The motion to return to a previous debate has been defeated.

Mr. Kelly, do you have something to say?

Mr. Pat Kelly: I have a question of clarification, if you may give me the floor just to ask you, Mr. Chair.

How do we get this motion back on to the floor? Is it necessary to move, as we just did, and immediately go to a recorded vote? Is that the only way to get this motion back on to the floor for debate?

The Chair: In my opinion, this is the only way to return to the debate of the motion that was previously adjourned.

However, there is nothing stopping a member of this committee from introducing another motion of the same content, as long as it's within the rules and the provisions that we govern ourselves by. The mover of the motion would present that motion after 48 hours' notice, much like your motion today, and then the individual who moved the motion would obviously be allowed to immediately speak to their motion.

Mr. Pat Kelly: Thank you for clarifying that.

Mr. Daniel Blaikie: Would it be possible to make time in our agenda for unfinished business when we come back? Can we have a meeting dedicated to discussing those items?

● (1245)

The Chair: I appreciate your question, Mr. Blaikie. I somehow feel as if I have failed this committee. We have these two motions at loggerheads because apparently we do have other business that committee members would like to bring before the committee, and if that's the case, then the chair will always entertain if somebody wants to have 15 minutes of the committee's time at some particular point to discuss committee business. I would be more than happy to entertain that in that vein.

I'm trying to guide this committee as smoothly as possible. I also think it's particularly unhelpful to continue to adjourn debate on motions, thereby leaving the motions hanging before the committee. We now have two, and at any particular point any member of this committee can move a motion to resume debate on them. This takes time. We would eventually find ourselves in a situation with four, six, eight, 10, 20 of these motions before the committee, which anybody can move at any particular time.

My advice to you as your chair is that we should probably resolve these motions at some point. If any of you wish to discuss with me how we can do that in a manner that suits all parties, I will have some recommendations for you.

Mr. Nathaniel Erskine-Smith: Perhaps it could be when witnesses aren't here before us.

The Chair: I will enforce the rules. Every member of Parliament has the ability to do that, and I will safeguard those protections and privileges. Everybody at this table was duly elected and has these privileges. Whether and how they choose to exercise them is their prerogative, but I will uphold those protections for members of Parliament, as I am one.

Colleagues, we have a few minutes left. We have dealt with the motions that are before us. Mr. Long, I understand you had some questions, so if you would like to talk to our witnesses, we have about 10 minutes of the committee's time left.

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

Thank you to our witnesses, and I'm sorry for the delays today. My apologies.

Ms. Vonn, you're quoted as saying, “There is a crisis of public confidence in national security agencies that appear to break the law with no consequences.”

Two surveys were done, and I want you to talk to them if you can. A CFE survey said "Slightly more than 70% of respondents agreed that most Canadians are unconcerned or unaware about government surveillance.”

A CBC poll also said 77% supported police forcing someone to surrender encryption keys or a pass code as part of a criminal investigation.

I respect your positions and I know exactly where you're coming from, but I read these two polls last night, and I'm wondering if you could help square those for me.

Ms. Micheal Vonn: Sure. Some aspects of the polls asked to describe.... In the ones that came out in the *Toronto Star* and the CBC, I believe, in the series they did and I participated in, rightly and unsurprisingly the kinds of things that Canadians say are exactly the sort of things we say, that there's more than one good. Sometimes, yes, we have to clearly accede to police or law enforcement having access to information, but the kinds of things they also said that I think were surprising to many people were that they understand what basic subscriber information is, as in the Spencer case in the Supreme Court of Canada , and they think you should get specific and meaningful pre-authorization for that.

These kinds of things again indicate that Canadians do appreciate that there's a balance, and they want the pre-stage protections to make sure that you have justification and authorization, and then by all means give law enforcement the tools they need to do their job. I don't think there's a conflict there when you look at specific aspects of what those tools would be. People have different opinions as to when the threshold will be met, but that there is a balancing is very clearly the view of the Canadian public.

Mr. Wayne Long: Thank you.

There was one more comment you made in an article I read. You stated:

> Instead, a discovery that national security agencies are breaking the law leads quickly to changes so that what was once illegal becomes legal — rewarding the violation, not punishing the violator. And this pattern of encouraging impunity has had a corrosive effect on public confidence.

Can you give me your comment on that?

● (1250)

Ms. Micheal Vonn: Certainly.

We're very concerned when we hear the statement by Mr. Justice Noël, for example, in the Federal Court case that found 10 years of breach of the duty of candour by CSIS in relation to the illegal collection of metadata in their bulk data holdings. You will find in that 137-page judgment—very thoughtful, very considered—a kind of statement that you almost never see from a judge of the Federal Court, traditionally very deferential to national security needs.

He asks what it will take. Do we need to prosecute for contempt of court in order to get these findings of failure of the duty of candour before the court to be taken seriously?

That kind of statement from a Federal Court judge should alert us to what I am indeed calling—you are citing those correctly—a crisis of confidence that we have national security agencies, specifically in this case CSIS, operating within the law.

Mr. Wayne Long: Thank you.

Thank you, Chair.

The Chair: Mr. Bratina, I seem to recall that you had some supplementary questions.

Mr. Bob Bratina: Yes. Thank you.

Ms. Austin, what would your recommendation be with regard to this committee's recommendations on any usefulness of SCISA? Let me put it this way: what problems would be created if it were our recommendation to eliminate it, to just go back to the previous security protocols? What would you say to that?

Prof. Lisa Austin: I would be open to the argument that this wouldn't be sufficient, but you would have to take a look at the evidence. The government hasn't implemented the Arar commission's recommendations. It hasn't implemented the Air India recommendations. Some of those were very strong on information sharing, saying that CSIS and the RCMP "must" share information, right? There's no "must" share here.

With regard to my comments that this measure should be repealed, it doesn't mean there aren't information-sharing issues that need to be addressed through the law. I would go back to those and ask two things: why isn't that sufficient, and where is the evidence that you need more than what those two very careful inquiries asked for? If the case can be made that, well, actually there's this other situation, then have a very carefully tailored amendment to whatever law you need for that.

It's just the sheer overbreadth of SCISA that's very shocking and, I think, unjustified. I think you could justify specific information-sharing practices and amendments in light of things like Arar and Air India.

Mr. Bob Bratina: Okay.

Mr. Karanicolas, I'll give you the opposition question period question: "Yes or no?" What would your recommendation be to this committee with regard to SCISA?

Mr. Michael Karanicolas: Regarding whether to repeal it or to amend it?

Mr. Bob Bratina: Yes.

Mr. Michael Karanicolas: We avoided taking a firm position on this for a reason, but generally speaking, I would probably be in favour of reforming it rather than revising it entirely. Now that we're having the debate, it might be useful to try to arrive at a proper solution so that this can hopefully be settled and doesn't recur in terms of new problematic legislation down the road.

That's probably the position I would take.

Mr. Bob Bratina: Would you comment, Ms. Vonn?

Ms. Micheal Vonn: We favour repeal. To echo Professor Austin, if there are any needs for which the justification can be demonstrated, certainly those should be put in the Privacy Act, in our view.

Mr. Bob Bratina: Right.

Thanks, Mr. Chair.

The Chair: Thank you, colleagues.

The committee business that we could have done at the end of the committee meeting has already been dealt with, so I will take this opportunity to wish each and every one of you a very merry Christmas and happy holidays. I would like to extend that to the clerk, our analysts, and all of the folks who support us here so capably in the House of Commons. I wish you all a very safe holiday time with friends, family, and loved ones, and eagerly look forward to our return in January.

I'd like to thank the witnesses for their insightful comments today. They will be very helpful as we deliberate what to do with the review of the SCISA legislation.

Thank you, and I wish you all a very safe holiday.

The meeting is adjourned.