HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

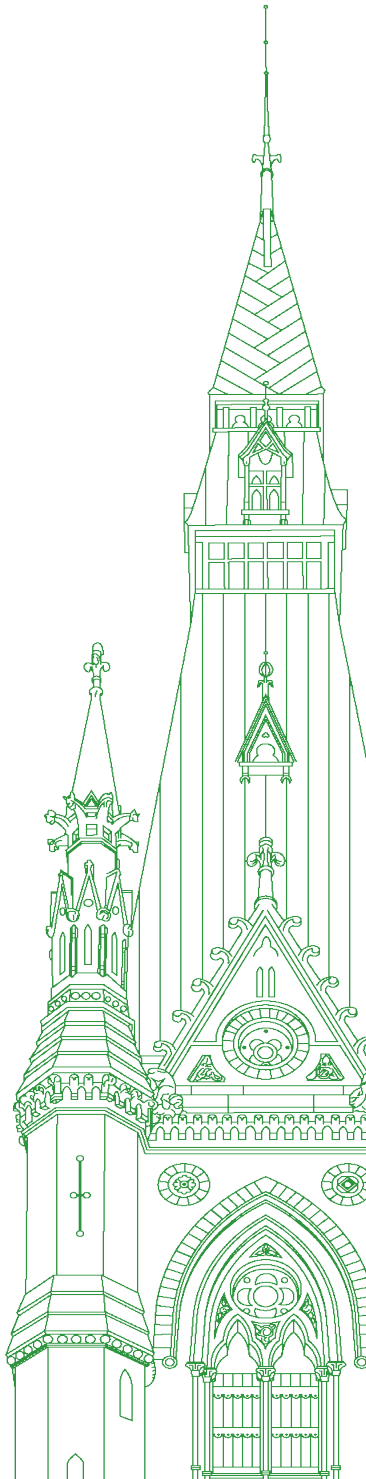
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 094

Monday, February 12, 2024



Chair: Mr. Heath MacDonald

Standing Committee on Public Safety and National Security

Monday, February 12, 2024

● (1600)

[*English*]

The Chair (Mr. Heath MacDonald (Malpeque, Lib.)): I call this meeting to order.

Welcome to meeting number 94 of the House of Commons Standing Committee on Public Safety and National Security.

Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and remotely using the Zoom application.

I would like to make a few comments for the benefit of witnesses and members.

Please wait until I recognize you by name before speaking. To prevent disruptive audio feedback incidents during our meeting, we kindly ask that all participants keep their earpieces away from any microphone. Audio feedback incidents can seriously injure interpreters and disrupt our proceedings.

Pursuant to the order of reference of Monday, March 27, 2023, the committee resumes its study of Bill C-26, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts.

Today we have two panels of witnesses. I would now like to welcome our witnesses for the first panel.

In person, from the Office of the Privacy Commissioner of Canada, we have Mr. Philippe Dufresne, Privacy Commissioner of Canada. By video conference, from the Office of the Superintendent of Financial Institutions, we have Mr. Tolga Yalkin, assistant superintendent, regulatory response sector. From The Citizen Lab, we have Ms. Kate Robertson, senior research associate at the Munk School of Global Affairs and Public Policy, University of Toronto.

Welcome to all.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions.

I now invite Mr. Dufresne to make an opening statement.

Go ahead, please.

[*Translation*]

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair.

Members of the committee, I am pleased to be here to assist the committee in its study of Bill C-26, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts.

Cybersecurity is an area of significant importance, in Canada and globally. Digital services that are delivered through cyber-systems and telecommunications networks are central to the ways that we live, work and interact, and impact large volumes of personal information and data. That is why it is critical to protect Canada's cyber-infrastructure from potential threats.

[*English*]

At the same time, we must ensure that efforts to secure these systems and networks also protect and respect Canadians' fundamental right to privacy. This is not a zero-sum game. Privacy and the public interest are not only compatible; they build on and strengthen each other. I strongly support the objectives of Bill C-26 and believe that it's imperative that we as a society have the necessary tools and the ability to address this important public interest goal.

In my testimony today, I will share ways in which the bill could be strengthened in order to further protect the fundamental right to privacy and address potential privacy implications while achieving its important objectives.

Under Bill C-26, specified persons or entities would be able to collect and analyze a wide range of information, including sensitive personal information that is held by banks, telecommunications operators and energy services providers. The bill would also allow for the sharing of that information with organizations such as intelligence agencies, provincial and foreign governments and organizations established by foreign states.

● (1605)

[*Translation*]

As drafted, these powers are broad. In order to ensure that personal information is protected and that privacy is treated as a fundamental right, I would recommend that the committee consider making the thresholds for exercising these powers more stringent, and placing stricter limits on the use of those powers. One way of doing so would be to require that any collection, use or disclosure of personal information be both necessary and proportionate. This is a core principle for the handling of personal information that is recognized internationally.

[*English*]

Requiring government institutions to conduct privacy impact assessments, or PIAs, and to consult my office on new programs or initiatives created under the authorities in Bill C-26 would also strengthen privacy protections while supporting the public interest and generating trust. PIAs, which are currently a policy requirement under the Treasury Board Secretariat's directive on PIAs but not a legally binding requirement under privacy legislation, are an important tool for identifying, analyzing, addressing or mitigating privacy issues before initiatives are put in place. They can help reduce inadvertent harms to privacy as initiatives roll out. This is why I've recommended that the preparation of PIAs should be made a legal obligation for the government under the Privacy Act.

Bill C-26 would also allow the Minister of Innovation, Science and Industry to prohibit public disclosures of certain orders and directions made under the proposed act. It's important that any such confidentiality provisions that have the effect of reducing public scrutiny regarding the bill's implementation, including the collection, use and disclosure of personal information, be accompanied by appropriate transparency measures. These could include requiring the government to report to Parliament and/or to my office regularly on the number, nature and purpose of such orders and directions, especially when they involve sensitive personal information. This would reassure Canadians that their privacy is protected at all times.

[*Translation*]

I would also recommend that the bill be amended to include stronger accountability measures to ensure the protection of personal information that is shared outside Canada. These could include additional oversight mechanisms and established criteria that must be included in information-sharing agreements with foreign jurisdictions, such as restrictions on any onward transfers of the personal information, establishing safeguards that must be applied, and penalties for non-compliance.

Finally, should Bill C-26 be adopted, it will be important that my office have the necessary flexibility to coordinate, as appropriate, with other regulatory and oversight bodies that are involved in responses to cybersecurity incidents in cases that may involve a breach of personal information.

I would be happy to take your questions.

[*English*]

The Chair: Thank you, Mr. Dufresne.

Mr. Yalkin, you may go next.

Mr. Tolga Yalkin (Assistant Superintendent, Regulatory Response Sector, Office of the Superintendent of Financial Institutions): Thank you so much.

[*Translation*]

Good afternoon, Mr. Chair, and ladies and gentlemen of the committee.

The mandate of the Office of the Superintendent of Financial Institutions, or OSFI, contributes to public confidence in the Canadian financial system by regulating and supervising approximately 400 federally regulated financial institutions. In this role, we ensure that these institutions maintain sound financial conditions, continually assess risks and industry trends, and safeguard against threats to their integrity and security, including cyber-threats.

There’s no question that financial institutions are vulnerable to cyber-attacks. In fact, OSFI has highlighted cyber-risk as a key risk to Canada’s financial stability in our annual risk outlook, which is available online.

[*English*]

Given this, it won't surprise you that we have been, for some time, active as a regulator in expecting our financial institutions to adopt appropriate risk management practices in the face of cyber risks. More specifically, we've taken pains to clarify in our guidelines our expectations for how financial institutions should manage technology and cyber risks to prevent things like outages and data breaches and to improve overall technology and cyber resilience.

This also includes an expectation that financial institutions respond to tech and cybersecurity incidents quickly and effectively and, more importantly, notify us whenever an incident happens. That reporting really helps us to identify areas where individual institutions—or the industry more broadly—need to take steps to prevent issues from arising.

We also provide tools to financial institutions. A good example of this would be our cybersecurity self-assessment, which helps them evaluate their current level of cyber-preparedness and develop effective cybersecurity practices. There is also our I-CRT—that stands for intelligence-led cyber resilience testing—framework, which provides instructions to financial institutions on how to implement a sophisticated approach to what is known as red teaming.

These efforts, and others, are critical, in my opinion, as there's little question that cyber-attacks will continue to increase in frequency and sophistication. Moreover, this is a risk environment that, in our experience, changes rapidly, and failure to protect against it can have serious consequences. A successful cyber-attack could impact the confidentiality, integrity, and availability of data and systems, which in turn could result in loss of public trust, reputational damage and financial loss.

● (1610)

[*Translation*]

That's why OSFI is so focused on promoting the sound management of cyber-risks and technology risks generally at all federally regulated financial institutions.

As an identified regulator within a critical sector, OSFI is standing by and ready to support committee members in their reflection around Bill C-26. We want to help to improve the resiliency of Canada's financial system.

I would be pleased to answer the committee members' questions.

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you.

I now invite Ms. Robertson to deliver her opening remarks.

Ms. Kate Robertson (Senior Research Associate, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you, Mr. Chair and members of the committee. As you know, I attended this committee last week in relation to this bill.

I'm a senior researcher at the Citizen Lab, which is based at the Munk School of Global Affairs and Public Policy at U of T. I have submitted a written brief to this committee along with a colleague, Lina Li of McGill Law, which builds upon the research and analysis of my former colleague at the Citizen Lab, Dr. Christopher Parsons.

Today I will readopt my comments from last week and supplement them as follows.

First, several concerns have been raised throughout these hearings focusing on malicious targeting by, for example, ransomware of aspects of the economy that are outside federal responsibility, such as hospitals. The need for protection in other areas is important, but this committee can also be mindful of the proper scope of its responsibility in its work on Bill C-26.

I also appreciate other committee witnesses raising threats facing Canadian society today. However, it is never a good idea to legislate out of fear. This is an important issue that requires careful due diligence and reflection as to what goes into any amendments. I would suggest the committee carefully look at what it is doing. Making the right decision now could improve the security, safety, privacy and charter rights of all people in Canada for decades going forward. It's incredibly important that lawmakers are thoughtful, nuanced and reflective of the kinds of amendments they propose for the legislation.

Second, our brief sets out recommendation 12—including recommendations 12A through 12C—pertaining to judicial review proceedings under Bill C-26. This includes the recommended appointment of special advocates in judicial review proceedings, and the need to align Bill C-26 with analogous provisions under the Canada Evidence Act applicable to secret evidence. These amendments are not only important but also fair, simple and commonsense enhancements.

Lastly, I also wish to address our recommendation that government entities empowered with new information collection and sharing powers be required to limit the use of that information to cybersecurity and information assurance.

The collection or use of information by national security intelligence agencies like the CSE about Canadians or persons in Canada is a core matter of public and constitutional concern. The concern that the CSE may repurpose information it receives through Bill C-26 into its other intelligence activities is not a speculative one. Recent reporting from the National Security and Intelligence Review Agency, or NSIRA, documents that, at this time, the CSE does not consider itself prohibited under its home statute from repurposing information about Canadians across its mandates.

However, only a few years ago, in Bill C-59, an important equilibrium was struck by Parliament concerning the need for important limits, given the prohibition against intelligence agencies directing their activities towards people in Canada. Bill C-26 could destabilize this important equilibrium. It currently contemplates broad and even secretive government collection and sharing powers about information concerning people in Canada. While the Department of Justice's charter statement on this bill referred to the government's potential use of only technical information and not sensitive personal information, there are no caveats or safeguards to stipulate this in the legislation. Clarity is needed.

Telecommunications providers, for example, are quite literally conveyors of the most private information known to our legal system. I agree with witnesses from CIRA and OpenMedia that this is a core matter of public trust. The public should not have to be asking itself whether the government's cybersecurity bill is actually a spy bill under a different name.

As noted by Mr. Hatfield last week, NSIRA has reported a chronic problem in reviewing the lawfulness of the CSE's activities since its inception. Lawmakers here should be very cautious when considering whether extending additional new powers is appropriate or necessary under Bill C-26, and what corresponding judicial oversight mechanisms are necessary and fit for purpose to protect the privacy of all people in Canada.

Thank you. I'm happy to answer any questions you may have.

● (1615)

The Chair: Thank you, Ms. Robertson.

We're going to open the floor now and move right on to questions.

We'll be starting with Mr. Shipley for six minutes.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair.

Thank you to the witnesses for being here today.

Bill C-26 is a very important issue. I'm going to ask for a little time on this. I have no intention of infringing on anybody else's time today, Chair, but I would like to quickly move a motion that's on notice, and hopefully get back to Bill C-26 quickly. It's a short motion.

I move:

> That the committee acknowledge that auto theft is a pressing issue facing Canadians and pursuant to the motion agreed upon regarding auto thefts on October 23, 2023, the committee commence this study on Monday, February 26, 2024 and dedicate the following six Monday meetings to this study, while reserving the committee's Thursday meetings for the study of Bill C-26. Additionally, pursuant to the motion agreed upon regarding the Rights of Victims of Crime, Reclassification, and Transfer of Federal Offenders on Monday, October 23, 2023, that the committee extend its meeting on Thursday, February 15, 2024 for an additional hour and the Minister be invited to appear for the full three hours in order to discuss all matters related to his mandate.

Chair, I feel this is a reasonable approach and motion to prioritize a serious issue. I think all of us around this table agree that auto theft is a serious issue.

The reason we added trying to get a little extra time with the minister is that we have not had a minister report to this committee since May 30, 2023. The last time a minister came for estimates was May 19, 2022. We all passed a motion on October 23, 2023, "that the committee invite immediately the Minister of Public Safety and department officials to appear for two hours to discuss his mandate." I was hoping to consolidate some of those meetings together and make our time work a little better. Perhaps the minister, if he can fit it in his schedule, could find the time to talk to us about many pressing issues that are going on here right now.

With that, I will cede the floor, Chair.

● (1620)

The Chair: Thank you.

Are there any comments?

Ms. Michaud.

[*Translation*]

Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Thank you, Mr. Chair.

I'd like to comment on the motion, if I may.

It's been a while since we've had a chance to discuss a motion. I just want to say that it is true that the minister still hasn't been here to talk about his mandate generally, even though that should happen at the very beginning of the year—and even in the middle of 2023, after he was appointed. I therefore agree with that part of the motion.

Since I proposed the auto theft study, I'm certainly not opposed to moving it up. I do want to say, however, that my intention is not to hold up the study on Bill C-26 either. I think it would be reasonable to do both at the same time.

I'm not sure whether the plan was to vote on this motion today, but I would support the motion.

[*English*]

The Chair: Thank you.

Mr. Julian.

[*Translation*]

Mr. Peter Julian (New Westminster—Burnaby, NDP): Thank you, Mr. Chair.

I want to welcome the students from Saint-Hyacinthe high school and thank them for joining us today.

The motion covers a number of elements, and my preference in those cases is always to have the steering committee discuss the matter. I'm all for inviting the minister, but I think it's unlikely that he'll be able to make time in his schedule on Thursday.

While I think it's important to get started on Ms. Michaud's study, which we all support, as soon as possible, doing so would delay our study of Bill C-26. For the past month, we've had a number of challenges in holding discussions and meeting with witnesses. I think we need to improve Bill C-26 right away. Then, we could move on to the auto theft study, which I think is important.

For that reason, I will be voting against the motion, but I will raise it with the steering committee. I think the committee should meet as soon as possible.

That said, I think we need to work out a schedule and invite the minister again. Mr. Shipley rightly pointed out that the minister has hardly been here, and that needs to change. We can discuss the auto theft issue as soon as we wrap up the study on Bill C-26.

[*English*]

The Chair: Thank you, Mr. Julian.

Ms. O'Connell, please.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Chair.

I would just like to point out that if it weren't for Conservative filibusters, we would have been finished with Bill C-26 and we would be on auto theft right now.

If this were such a serious issue, they wouldn't have brought up Emergencies Act motions—at least six of the same thing, just changing how many meetings—and they would have gotten to the point. I believe that, just at the last meeting, it was the first time a Conservative member actually asked witnesses a question on Bill C-26. If it were such a concern, we would have already been studying auto theft—which was Ms. Michaud's motion to begin with, which we all agreed with.

I think it's crucially important that we finish Bill C-26 and move forward with auto theft, and we can do that. We still have to submit amendments and things like that and then get to clause-by-clause, but we can go to auto theft in the meantime.

I will just confirm that the ministers, both Minister LeBlanc and Minister Champagne, are scheduled on Bill C-26 for February 15, and Minister LeBlanc is also confirmed for his appearance for the week when we're sitting in March. He's there on his mandate, and that's been confirmed to the clerk. Those are both scheduled.

I would like to point out that the minister was available sooner, but we were in a different study, and it was decided to invite other witnesses to come before that. I recognize the frustration in terms of scheduling the minister. I have been taking that back, but if it weren't for all of the continuous filibusters, we would have been in a very different place as a committee.

We need to finish Bill C-26. We have only two meetings left after this. We have the ministers and then one more, I believe, and then we can move forward, but if we continue to get filibustering motions from the Conservatives and they're not serious about talking about Bill C-26, then we're not going to be able to get to auto theft. It's a shame that they've done that, since it's really important.

I would very much hope that we can finish this study and move to auto theft, which was always the plan. Again, we would have been there if it weren't for Conservatives wasting committee time and taxpayer money talking about motions that they actually never even wanted to vote on.

● (1625)

The Chair: Thank you.

Yes, the minister is scheduled for Thursday, March 21. We all know that our schedule in March is broken. We'll expect him here on the 21st.

There's a motion on the floor. Do we want a show of hands to vote?

Mr. Doug Shipley: We want a recorded vote, Chair.

The Chair: Okay.

(Motion negatived: nays 6; yeas 5)

The Chair: We're going to move on.

Mr. Gaheer, you're up next for questions.

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair.

Thank you to the witnesses for making time for this committee.

My question is for the Privacy Commissioner, Mr. Dufresne.

When is it normal for the Privacy Commissioner to weigh in on the legislation? Is it when the legislation is in committee or when it's going through the regulations process?

Mr. Philippe Dufresne: Well, we do so at any appropriate time. Ideally, we would hope to be consulted prior to the bill being tabled, but the regular way is for my office and me to be called to committee to give a recommendation on a bill. We can also do the same for regulations and consultations with the government.

Mr. Iqwinder Gaheer: Just to confirm, your office will be involved in consultation on the regulations when that process goes on.

Mr. Philippe Dufresne: I hope so. We're certainly prepared for that. We expect that and we would call on the government to involve us in that.

Mr. Iqwinder Gaheer: We know that during the course of the committee's study on Bill C-26 so far we've heard a lot of stakeholder reaction around privacy rights and information sharing. You touched a bit on this in your opening testimony as well. Do you have any suggestions for how these concerns can be mitigated through regulations, especially when the data is crossing national boundaries?

Mr. Philippe Dufresne: Certainly in terms of data crossing national boundaries and being shared with other institutions, my recommendation is to make sure we have specific requirements for these information-sharing agreements so that the purpose, the retention and the safeguards regarding that information by our international partners—all of these—are set out and are strict, and there's a dispute resolution mechanism just so we bring in more rigour and guardrails to those exchanges of information. The concepts of necessity and proportionality should also be included when it is being determined whether to share the information in the first place.

● (1630)

Mr. Iqwinder Gaheer: What role does your office currently play or how would your office's role change based on how the legislation is worded so far?

Mr. Philippe Dufresne: The legislation currently doesn't provide a role for my office. The role would be specified under the Privacy Act. We have jurisdiction over the government's handling of information and we have jurisdiction over the private sector's handling of information.

One of our recommendations is to have more transparency mechanisms so that we can know what is happening and so that we can know what type of information is being collected, disclosed and used so that we can exercise our powers in that regard.

With regard to those reports, there's a provision in the bill for an annual report by the minister overall. We're recommending that this be more specific and that there be more details about what is happening.

We would also potentially have a role in working with the regulators in cases of cyber-breaches and cyber-incidents. One of my recommendations is that we be given the ability to collaborate with those regulators and, as needed, exchange information and work collaboratively when cyber-incidents involve personal information. We know that's a big area of concern for Canadians.

Mr. Iqwinder Gaheer: I think in your opening testimony you touched on this. I just want to go over it one more time. I think you wish that more came under your purview based on what this legislation is bringing in. Is there anything else you'd like to have oversight on?

Mr. Philippe Dufresne: I'm not suggesting that we would have oversight under this legislation. I'm suggesting that we be given the necessary information so that we can fulfill our mandate under privacy legislation with respect to public sector and private sector privacy information.

One of the recommendations I've made is that privacy impact assessments be mandatory and that I be consulted on those so that we can provide insight and advice to departments, because when that happens at the front end, these issues can be corrected and addressed before they become issues that can impact Canadians' trust.

It's not so much the fact that my office would be the regulator; in many instances we wouldn't be.

I'll give the example of former Bill C-11, which falls under the CRTC. The CRTC has jurisdiction, but we can provide input, and the bill recognizes privacy as a consideration.

Mr. Iqwinder Gaheer: Thank you.

It's always great to have you at committee.

The Chair: Thank you, Mr. Gaheer.

We'll have Ms. Michaud next.

Go ahead, please, for six minutes.

[*Translation*]

Ms. Kristina Michaud: Thank you, Mr. Chair.

Thank you to the witnesses for being with us.

In your opening remarks, Mr. Dufresne, you raised your concerns with respect to privacy. Most of the witnesses we've heard from actually share your concerns.

What you're recommending—that your office be consulted—differs from what most of the other witnesses have proposed. The mandate of the Office of the Privacy Commissioner is to oversee "compliance with the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act".

You are recommending that, should Bill C-26 be passed, the Department of Public Safety or the minister responsible consult your office.

In the case of other bills, do departments or ministers consult your office on privacy considerations? If so, can you provide an example? It would give us a sense of how things would work.

Mr. Philippe Dufresne: All right.

What we examine are activities that impact privacy. Our mandate does not extend to security issues that do not relate to privacy. We aren't looking to broaden our mandate.

According to Treasury Board policy, departments are supposed to consult our office when activities or projects could impact the privacy of Canadians. That doesn't always happen. It's a policy, not a legal requirement. We are recommending that the requirement be set out in the Privacy Act.

In some cases, we've worked with the National Security and Intelligence Review Agency to examine departments' practices and the transfer of information as it relates to privacy. In that situation, security and privacy did overlap.

In co-operation with our colleagues at Competition Bureau Canada and the Canadian Radio-television and Telecommunications Commission, we established the Canadian Digital Regulators Forum. We realized that there was some overlap, or a grey area, in many sectors. Some activities bring together competition, privacy and broadcasting considerations. The idea is to coordinate our efforts to avoid contradictory approaches.

If the activity could potentially impact privacy, we recommend that our office be informed. Not only would that be beneficial, but it would also give Canadians some reassurance.

● (1635)

Ms. Kristina Michaud: That part about reassuring people is extremely beneficial.

I gather that, if it's just a recommendation, the department or minister wouldn't necessarily have to consult your office. However, if the bill is amended to incorporate the requirement in the legislation, the minister or department would have to consult your office.

Do I have that right?

Mr. Philippe Dufresne: That's exactly right. If it's in the legislation, it becomes a legal requirement, and departments have no choice.

Ms. Kristina Michaud: You also mentioned additional oversight mechanisms. It's a fairly important idea that comes up often. Some have raised concerns over giving the minister the power to make orders, because we don't have a clue what that could look like.

It's fine to give the minister powers, but clearly, the House and parliamentarians don't necessarily have control over the whole regulation-making process. The government is really the one in control.

What is a better way to control this and ensure that privacy is protected?

Mr. Philippe Dufresne: One way would be to build in the test stipulating that the activity be necessary and proportionate. The second one is missing. The necessity component is covered in the act. For example, certain provisions stipulate that, if the minister is of the view that it is necessary to do something, the minister has the power to do so. Other provisions refer to relevance.

The principle of proportionality is important. The necessity test is important and helps to meet the objective. Ensuring proportionality, however, means really checking whether the method is the least privacy-invasive. It's similar to the assessment carried out under the charter, in terms of achieving that balance.

This would cover the principles of necessity and proportionality, which are central to the protection of privacy. That's the case in the international community and in countries such as Australia, the U.S. and Great Britain. They have clearer rules around taking privacy into account and examining other options.

The idea isn't to prevent the minister from doing their job—absolutely not. As I said, I strongly support the objectives of the bill, but it's important to build in that requirement, especially when people's privacy is at stake.

Ms. Kristina Michaud: Thank you.

Are there other recommendations you want to share with the committee? I'm talking about protecting privacy and reassuring the public or businesses and organizations that would have to comply with the legislation if enacted.

Some are concerned that the legislation will mean more work for them, more red tape. The sharing of information is another cause for concern.

Mr. Philippe Dufresne: I think all the recommendations I covered in my opening remarks help to reassure Canadians, as well as small and medium-sized businesses. The institutions are there to help them. The responsibility is not being put wholly on individuals or small and medium-sized businesses.

Take privacy impact assessments. If the process is mandatory and my office is consulted, it would give people reassurance. They would realize that there is some oversight, that the commissioner is aware, that the commissioner can make recommendations and, if necessary, that the commissioner can file complaints or make recommendations.

It's about transparency, in other words—

[*English*]

The Chair: Thank you, Ms. Michaud. Your time is up.

Mr. Julian, go ahead, please.

[*Translation*]

Mr. Peter Julian: Thank you, Mr. Chair.

Thank you, Mr. Dufresne, for your service as law clerk and parliamentary counsel of the House of Commons, as well as your work in your current role as the Privacy Commissioner of Canada.

Thank you to all the witnesses for the information they have shared with the committee.

Commissioner, I have two questions for you.

You mentioned the importance of having Bill C-26 require government organizations to conduct privacy impact assessments.

First, have government or non-government organizations ever consulted your office? The bill was introduced in June 2022, so certainly, there will be an impact.

Second, has an organization consulted your office to learn how to conduct the assessments? What impact will Bill C-26 have?

● (1640)

Mr. Philippe Dufresne: As it stands, Bill C-26 does not include a requirement to conduct privacy impact assessments. The Treasury Board does, however, have a policy with such a requirement. We consult with departments regularly. We have a government advisory directorate, and we provide advice to departments.

In some cases, the assessments are done after the fact, once the tool has already been used. In fact, I recently appeared before the Standing Committee on Access to Information, Privacy and Ethics on the subject.

It undermines trust when Canadians find out that the government is using a tool or developing a program without conducting a privacy impact assessment first. That's why privacy impact assessments should be conducted at the outset.

In addition, people should know that our office has been consulted. That way, when the information becomes public, they know that we were consulted, that discussions were held and that advice was given.

That is what I'd like to see in Bill C-26, given the potential impact of those powers.

Mr. Peter Julian: Thank you.

I have one last question.

Can you give us some best practices other countries follow to prevent personal information from being shared outside the country?

Mr. Philippe Dufresne: It is actually permitted to share information outside the country, provided that it's done in accordance with lawful agreements and specific conditions. Under the European model, for example, laws and mechanisms have to be equivalent to what exists in Europe. In Canada, the law requires that it be equivalent to what exists here, where the sharing of information may potentially be contract-based.

That's why we recommend that the legislation include a requirement to specify retention practices and safeguards, as well as apply the necessity and proportionality test, before data are shared with organizations in other countries. The goal is to prevent the data from being vulnerable to a cyber-attack.

Mr. Peter Julian: Thank you.

[*English*]

I'd like to go to you, Mr. Yalkin.

You raised some important issues through OSFI. I have two questions for you.

First off, have you been consulted at all on Bill C-26? Was the banking sector consulted before the legislation was tabled, or afterwards?

Second, how many cyber-attack incidents have we had in the financial institutions covered by OSFI's mandate? How many cyber-attacks were there in 2023? Is that number increasing, decreasing or staying stable?

Mr. Tolga Yalkin: Mr. Chair, we were engaged by Public Safety on the bill itself. In terms of consultations with other stakeholders, I'd defer to them to respond to those questions.

Should the bill come to pass, we would obviously look forward to engaging with Public Safety in the development of the regulations. We expect, as part of this process, that the banking sector would have an opportunity to engage.

In terms of the frequency and severity of cyber-incidents, I can share a bit of information on that because we have a reporting protocol that financial institutions are expected to comply with. They alert us within 24 hours if a technology incident or cyber-incident occurs.

We have seen an increase when it comes to cybersecurity incidents. In 2022, I believe we had 10 of what we call priority one incidents, but we saw a significant increase in these in 2023. I think the number almost tripled to about 28 in 2023. Basically, moving from 2022 to 2023, we had a number of more impactful incidents. This represents a significant growth from our perspective as a prudential regulator.

Mr. Peter Julian: I'm going to move on to Ms. Robertson, but can you share with us how priority one is defined for a cyber-attack or a cyber-incident? If you could let the committee know, that would be very helpful. One of my colleagues may follow up on this.

Ms. Robertson, you identified in your paper the importance of having a special advocate. Could you speak a little bit more about the importance of that in the legislation?

● (1645)

Ms. Kate Robertson: Yes, of course.

Special advocates are intended to enhance the fairness of a closed hearing process concerning secret evidence without compromising Canada's ability to safeguard security information. They protect fairness for the party that is excluded from the closed hearing, as well as the public's right to free expression, by ensuring that any secrecy in the court proceedings is necessarily justified.

You can have special advocates either challenging the amount of secrecy that the government is seeking with respect to the evidence, or testing with due diligence and adversarial submissions the sufficiency, weight and appropriateness of the evidence that the government seeks to rely on. There's a very long history in the courts of using special advocates to protect the openness of the courts as well as the fairness of those proceedings.

The Chair: Thank you, Ms. Robertson.

Thank you, Mr. Julian.

Now we're moving on to the second round.

Mr. Lloyd, you have five minutes, please.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

I'll go straight into the questions, and I'll start with Ms. Robertson.

We're talking about Canadians' private information and about information sharing. It can all seem a bit abstract. I am wondering if you can provide some examples of what you can imagine. What kind of information are we talking about that we're concerned about being inappropriately shared between agencies?

Ms. Kate Robertson: The breadth of the collection and sharing powers means that the list of hypotheticals with respect to critical infrastructure providers, as well as telecommunications providers, could be quite long.

I'll provide one hypothetical example: There is the potential that the minister could compel telecommunications providers to furnish subscriber information with respect to individuals using telecommunications networks anonymously in circumstances that have been the subject of the Supreme Court of Canada's guidance around the importance of protecting the privacy interests of that type of information. In terms of this legislation, there would be no apparent restriction in preventing that information from being shared with other government agencies identified in the bill and from potentially repurposing that information for other aspects of their mandate, such as providing assistance with federal law enforcement.

Mr. Dane Lloyd: Now, I was reading that under this act and the legislative review the minister doesn't even have to make these orders known. They can be confidential. Usually they have to be posted in the Canada Gazette, where everyone can access them and see them. However, the minister can make orders that the information be withheld from the Canada Gazette.

Are you saying that there's a situation where Canadian citizens could have a telecommunications order to provide their private information? The subjects of that might not even know that it's happening and would have no recourse to know that it's happening to them.

Ms. Kate Robertson: Yes, that's a function of the absence of publicity requirements with respect to the orders themselves, as well as the absence of any notice obligation set out under Bill C-26.

We've recommended in our brief that the constraints on secrecy must be defined and strictly curtailed to what is absolutely necessary. Language exists in the bill to support that amendment, as well as the need for notice obligations, which is an essential function for review mechanisms that would be necessary for this level of collection and sharing power, of course.

Mr. Dane Lloyd: Now, even if the subject of this order did learn that this information was being compelled of the telecommunications provider, if they said that they didn't think it was fair and they wanted to take the government to court over it, this legislation allows the government to conduct these court hearings in secret and not have to share the information with the subject of this. Is that correct? Can you give us more of an explanation on how you see that working?

Ms. Kate Robertson: Yes. In the situation where an individual or institution would seek to challenge the collection powers or orders under Bill C-26, there is a judicial review mechanism that's available. There are other complaint proceedings that are available in law outside of the scope of Bill C-26.

In this case, it contemplates secret evidence. In this case, there is some language that is included. Unlike the minister's discretion to keep secret the orders themselves—and that discretion doesn't appear to have any limits—there is some language in the bill at least with respect to the secret evidence proceedings. However, we've recommended that it be tightened and aligned with that which is set out in the Canada Evidence Act, because there's no justification for diluting that requirement or the court's ability to balance the public interest in disclosure in contrast to the government's interest in confidentiality. That's essential, in our view, with respect to the constitutionality of the scheme.

● (1650)

Mr. Dane Lloyd: Thank you for that.

Yes, I think there could be very compelling and extraordinary circumstances whereby the government would have to keep certain information secret, but we don't want to allow legislation to go through that gives overly broad powers that could potentially be abused, however good the intentions of the people passing the bill might be.

To the Privacy Commissioner, in my last 30 seconds, what sort of personal information are you concerned could potentially be inappropriately shared under this legislation?

Mr. Philippe Dufresne: Similarly, I think it's subscriber account information, communication data, website visits, metadata, location data and financial data that may not be what is ultimately requested, but we want to make sure that the bill doesn't allow for it.

What we're recommending is that notion of necessity and proportionality that would bring that rigour to say, "You may need it, but also consider whether there are less privacy-intrusive means to achieve the goal."

The Chair: Thank you.

Thank you, Mr. Lloyd.

We'll go to Mr. Schiefke, please, online. Thank you.

Mr. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Thank you very much, Mr. Chair.

I, too, want to add my thanks to the witnesses for appearing today.

I have some questions for Mr. Yalkin and then Ms. Robertson.

I'll begin with Mr. Yalkin. What new powers and responsibilities will be given to the Office of the Superintendent of Financial Institutions under this act?

Mr. Tolga Yalkin: I think a lot would depend on the regulations, but as the committee will be well aware, there are a number of different expected outcomes associated with the legislation relating to identifying, managing, preventing, detecting and limiting damage associated with cyber-attacks. We're already quite active in a lot of those areas, and we have a lot of levers through our supervisory work to be able to try to encourage financial institutions to respond to those different expectations.

I think the difference here is that if this legislation were to be introduced and regulations were to be introduced, rather than having us rely on our supervisory oversight as a lever to try to encourage good practices, it would be the case that there are different expectations that would have the force of law, which would then be subject to regulatory enforcement.

In terms of the specifics around those different levers, I suspect others would be better placed to speak to them than I.

Mr. Peter Schiefke: Thank you.

You spoke earlier about reports that were shared with you with regard to cyber-attacks. Were those shared with you voluntarily, or was that mandatory?

Mr. Tolga Yalkin: We have an incident-reporting protocol whereby we set out for financial institutions our expectations of when and how they report incidents to us. Now, in a sense, one could say they're voluntary, but I'll give you a bit of background, if you'll permit me.

Mr. Peter Schiefke: Please.

Mr. Tolga Yalkin: As a prudential regulator, we have a general responsibility when it comes to overseeing financial institutions and making sure that they're engaging in sound risk management practices. What we do, then, instead of issuing regulations that have the force of law, is articulate for them our expectations of them, which we then supervise them against.

When we issue, for example, a reporting protocol, which we have in place, more often than not the case is that financial institutions comply with it, because if they don't, we may consider that as part of our ongoing supervisory oversight of them.

Mr. Peter Schiefke: Okay.

This legislation includes mandatory reporting mechanisms. Do you agree with those? Why is mandatory reporting important?

Mr. Tolga Yalkin: This legislation would be a bit different from what we currently have in place for reporting. Under our reporting protocol, banks report to us. If something happens, we have a mechanism for them to indicate to us within 24 hours that an incident has occurred.

Here, with this legislation, the reporting would be to a cybersecurity centre, so there would basically be dual reporting. We'd have to figure out, for example, how we effectively and efficiently facilitate that, because we have a form for reporting and there would undoubtedly be one under this particular regime as well. However, that's something we would be able to tackle with banks to make sure that the reporting expectations were clear to both coordinate parts of government.

Mr. Peter Schiefke: Thank you, Mr. Yalkin.

I'll turn my questions over now to Ms. Robertson. Thanks for being with us today.

I'm very interested in hearing more about some of the oversight mechanisms you would like to see put in place. You mentioned them earlier in the line of questioning. Can you expand on those and perhaps comment a bit on how Bill C-26 intersects with the Privacy Act?

Is there anything in there that you see as problematic? How can that be mitigated here in committee? What can we do?

● (1655)

Ms. Kate Robertson: There are a number of recommendations, including those identified in my comments of the last date as well as in today's proceedings, in addition to those identified by Commissioner Dufresne.

We have set out recommendations relating to the need for proportionality and reasonableness limits as an overarching framework that guides both the minister and the government in the implementation of the bill, but also the oversight mechanisms that should be attendant to the privacy interests and other interests that are at stake in this type of legislation.

We have recommended that there be a formalization through the legislation of the role for independent regulators in the assessment of the proportionality criterion when considering potential orders to be put in place under the act.

In light of the really sweeping nature of the types of privacy interests that are engaged by the institutions at issue, including telecommunication providers, we've recommended, being mindful of the constitutional obligations of the government in legislating, that judicial oversight be applicable to private information, de-identified information that has a reasonable expectation of privacy, which is absent from the legislation at this time.

Mr. Peter Schiefke: Thank you, Chair, and thank you, Ms. Robertson and Mr. Yalkin.

The Chair: Thank you, Ms. Robertson.

We're going to move on to Ms. Michaud for two and a half minutes, and then Mr. Julian will be the last one up for two and a half minutes, with a hard stop. We're getting down on time here.

Ms. Michaud, go ahead, please.

[*Translation*]

Ms. Kristina Michaud: Thank you, Mr. Chair.

Ms. Robertson, welcome to the committee.

The brief that you submitted to the committee contains a number of recommendations, and we appreciate them. It's very useful for us.

You recommended a mechanism whereby smaller telecommunications service providers, such as providers that have fewer than 250,000 or 500,000 subscribers or customers and that have historically been conscientious in their security arrangements, can seek at least some temporary relief if they're required to undertake new, modify existing or cease ongoing business or organizational practices as a result of a government demand, order or regulation.

Can you elaborate on this mechanism? On a number of occasions, I asked various stakeholders who met with us whether SMEs had any concerns about complying with these types of requirements under the legislation. This could mean more bureaucracy and an additional workload for these companies.

That said, it's a bit worrying that the government could force them to stop their business practices altogether. This may fall under the order-making powers of the Minister of Innovation, Science and Industry and the ministers covered by the bill.

I'm wondering about the scope of the ministerial powers. I'll ask you the same question that I put to Mr. Dufresne earlier. How can we better regulate these powers?

[*English*]

Ms. Kate Robertson: Thank you for the question. My apologies for responding in English.

Our recommendations here intersect with the public policy implications of the legislation, as well as potential constitutional risks around the equity impacts or potential discrimination impacts of the legislation in the order-making power. In terms of the need for standards for telecommunication providers, to protect the security of individuals in Canada, it's absolutely necessary on a platform-neutral level. However, there are potential impacts for Canadians in certain regions, including in rural or indigenous communities, who may suffer from the adverse impacts of smaller, orbit-size providers being unable to maintain viability in implementing security measures.

We have noted that the CRTC has found recently that there have been successive years of decline in competition in Canada. This was particularly noted in Quebec and Ontario, where the declines have been most significant, so this is where we've identified the need for appropriate balance.

The Chair: Thank you, Ms. Robertson and Ms. Michaud.

Mr. Julian, please proceed, for two and a half minutes.

● (1700)

[*Translation*]

Mr. Peter Julian: Thank you, Mr. Chair.

Mr. Dufresne, I asked a question earlier about intelligence shared outside a country's borders.

Which country could serve as a model for privacy protection?

Mr. Philippe Dufresne: There are a number of models. I would have a hard time identifying one model as the best option.

For example, the European model sets out the key privacy expectations of necessity, proportionality and transparency. It gives a prominent role to privacy organizations. In addition, this model requires other countries to have a proper system in place. These countries are assessed. Canada has recently been granted the status of a country that ensures a proper level of protection. This model makes sure that these criteria are strictly enforced.

Other countries have reached agreements or signed treaties to this end. Quebec adopted Law 25. This legislation requires a privacy impact assessment if data is shared outside Quebec.

These are all examples of discipline and rigour. We must think about privacy from the outset, as soon as we come up with an initiative, as soon as we decide to use a tool.

Mr. Peter Julian: Thank you, Mr. Dufresne.

[*English*]

Mr. Yalkin, you mentioned earlier that in 2022, there were 10 priority one incidents of cyber-attacks. In 2023, that moved to 30. How would you describe a priority one cyber-attack? What is the difference between that level of cyber-attack and others?

Mr. Tolga Yalkin: Priority ones are basically high-impact incidents that cause disruption of service or leakage of data, so any that meet that definition would constitute priority one and be accordingly reported to us.

Mr. Peter Julian: We're basically seeing an incident of that magnitude every two weeks or less at this point. Are you concerned about that number growing? As some witnesses have indicated, if we don't put in place protections, for example with Bill C-26, Canadian financial institutions may increasingly be targets.

Mr. Tolga Yalkin: We are concerned with that number growing. We're tracking it very carefully, and we are eagerly watching to see whether or not the trajectory continues to grow. This is an area of risk for financial institutions. We've outlined it in our annual risk outlook, published on our website, and cyber-risk and cyber-attacks would constitute an element of that.

The Chair: Thank you. If there's information that you feel Mr. Julian would like to have as part of his question, please forward it to him.

I want to thank all the guests for today. We appreciate your valuable time. It's a very important topic.

We going to suspend for about five minutes until we get set up for the next guests.

Thank you.

● (1700)

(Pause)

● (1705)

The Chair: I would like to welcome our second panel of witnesses.

In person, we have Eric Smith, senior vice-president, and Robert Ghiz, president and chief executive officer, Canadian Telecommunications Association. By video conference, we have Angelina Mason, general counsel and senior vice-president, legal and risk, and Charles Docherty, assistant general counsel and vice-president, legal and risk, Canadian Bankers Association. As an individual, we have Andrew Clement, professor emeritus, faculty of information, University of Toronto.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions.

We will start with you, Mr. Ghiz.

Mr. Robert Ghiz (President and Chief Executive Officer, Canadian Telecommunications Association): Thank you, Mr. Chair.

Good evening. As said, my name is Robert Ghiz. I'm the president and CEO of the Canadian Telecommunications Association. I'm joined today by our senior vice-president, Eric Smith.

[*Translation*]

The Canadian Telecommunications Association is dedicated to building a better future for Canadians through connectivity. Our association includes carriers, manufacturers and other companies that invest in Canada's world-class telecommunication networks.

We appreciate the opportunity to speak to you today about our association's views on Bill C-26.

● (1710)

[*English*]

The security of Canada's telecommunications system is of the utmost importance. Our members recognize that their services are critical to the social and economic well-being of Canadians, as well as to their security and safety. Accordingly, our members invest significant resources to safeguard their systems and infrastructure from cyber-attacks and other threats.

Members also actively participate in the Canadian security telecommunications advisory committee, or CSTAC, which facilitates the exchange of information between the private and public sectors, as well as strategic collaboration on current and evolving issues that may affect telecommunications systems, including cybersecurity threats. In addition to providing connectivity services, many of our telecommunications service providers also deliver cybersecurity solutions to businesses across the country, helping them protect their operations against cyber-attacks.

In other words, our industry takes security seriously and is committed to the security of the Canadian telecommunications system. As such, we share the Government of Canada's objective of protecting critical infrastructure from cyber-attacks and other threats.

However, Bill C-26 in its current form raises some concerns. We have outlined our concerns and proposed amendments to the legislation in a written submission to the standing committee. I will mention a few of them, all of which pertain to part 1 of Bill C-26 and the proposed amendments to the Telecommunications Act.

First, the bill gives the minister very broad order-making powers that lack appropriate checks and balances. Given the extremely broad scope and potential impact of these powers, the proposed legislation should be amended to impose conditions on exercising them. Specifically, orders should not only be necessary in the opinion of the minister but also reasonably necessary—in other words, proportionate to the potential harm of the security risk and reasonable in the circumstances. The legislation should also require that orders be made only after the minister has consulted with prescribed experts to ensure they are proportionate to the risk posed, have a limited impact on service availability and are economically and operationally feasible for affected service providers.

Second, while orders made under the bill are subject to judicial review, the legislation provides that a judge can base his or her decision on evidence the applicant is not allowed to see and therefore cannot challenge. This process makes no effort to provide for alternative means of testing the government's evidence, including the appointment of a special advocate with the appropriate level of security clearance.

Third, Bill C-26 does not include a due diligence defence for alleged violations of orders made pursuant to the proposed new sections of the Telecommunications Act, even though a defence of due diligence is available for other violations of the act, as well as for violations of orders by others under the rest of Bill C-26. The absence of a due diligence defence is even more striking given that the legislation seeks to introduce significant monetary penalties. Telecommunications providers should have the right, as afforded to others under Bill C-26, to avail themselves of a due diligence defence in appropriate circumstances by demonstrating they took all reasonable care in the circumstances to avoid the alleged violation.

Lastly, part 1 of Bill C-26 should be amended to make clear that compensation may, at the discretion of the government, be awarded for any financial expenditures, losses and costs resulting from complying with an order.

[*Translation*]

Thank you for giving us the opportunity to share our views on this key issue. We look forward to answering your questions.

[*English*]

The Chair: Thank you, Mr. Ghiz.

I now invite Ms. Mason for her opening statement.

Ms. Angelina Mason (General Counsel and Senior Vice-President, Legal and Risk, Canadian Bankers Association): Thank you.

Good evening.

I would like to thank the committee for inviting us here today to provide our views on part 2 of Bill C-26, an act to enact the critical cyber systems protection act.

My name is Angelina Mason, and I am general counsel and SVP of legal and risk at the Canadian Bankers Association. I am joined by my colleague, Charles Docherty, assistant general counsel and vice-president, legal and risk.

The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

Banks in Canada are leaders in cybersecurity and have invested heavily to protect the financial system and the personal information of their customers from cyber-threats. We are also a highly regulated industry and comply with robust requirements from the Office of the Superintendent of Financial Institutions in respect of cybersecurity risk, supply chain and third party risk management, and incident reporting.

The security of Canada's critical infrastructure sectors is essential to protect the safety, security and economic well-being of Canadians. The banking industry counts on other critical infrastructure sectors, such as telecommunications and energy, to deliver financial services for Canadians. We have encouraged the government to leverage and promote common industry cybersecurity standards that would apply to those within the critical infrastructure sectors, and we support the government's efforts to achieve this under the act. We recognize that critical infrastructure, such as energy, crosses jurisdictional boundaries. We have also recommended that the federal government work with provinces and territories to define a cybersecurity framework across all critical infrastructure sectors.

Having consistent, well-defined cybersecurity standards will provide for greater oversight and assurance that these systems are effective and protected. Protecting against state-sponsored and other threat actors requires a coordinated approach between the government and the private sector. The government can play a pivotal role in bringing together critical infrastructure partners and other stakeholders and building upon existing efforts to respond to cyber-threats.

While recognizing the importance of the act, we need to get this right. Some of the proposed provisions need to be better tailored to address operational and other risk concerns, including being able to leverage existing robust requirements of specific sectors, like banks, to mitigate duplicative or inconsistent requirements, providing greater safeguards for the protection of confidential information, and improving the threshold and timing for cybersecurity incident reporting.

In addition, there should be appropriate guardrails for the invocation of the government's very broad powers under the act. Consistent with other legislation, the act should also include safe harbour provisions that provide designated operators immunity from civil and criminal proceedings for good-faith compliance with the act's reporting requirements and cybersecurity directives.

Looking beyond mandatory incident reporting, the act should also support broader voluntary sharing of incidents, cyber-threat information and expertise about cyber-protection with the Communications Security Establishment and among classes of designated operators, while also including safe harbour provisions to enable this sharing without creating additional risk. Effective sharing of this type of information is a critical component to cyber-resiliency and should be fostered through the act.

Finally, we believe it is necessary to allow the CSE and CSIS to share relevant intelligence and information with designated operators of critical cybersecurity infrastructure in Canada to help them effectively prevent and mitigate cybersecurity incidents.

We will be following up to provide the committee with additional written details on these recommendations. We want to work collaboratively with the government and with other sectors to ensure that Canada remains a safe, strong and secure country.

We look forward to your questions.

● (1715)

The Chair: Thank you, Ms. Mason.

Now we'll move on to Professor Clement for his opening remarks.

Professor Andrew Clement (Professor Emeritus, Faculty of Information, University of Toronto, As an Individual): Thank you, Mr. Chair and committee members.

I am Andrew Clement, a computer scientist and professor emeritus in the faculty of information at the University of Toronto. I cofounded the interdisciplinary Identity, Privacy and Security Institute there.

For the past decade, I have focused on the privacy, security and surveillance aspects of Internet communications. Currently, I colead a project with the Canadian Internet Registration Authority on Internet measurement aimed at advancing Canadian cybersecurity, resiliency and sovereignty. The project is funded through Public Safety Canada's cybersecurity co-operation program. Beyond an annual $1,500 honorarium, I receive no funds from either CIRA or Public Safety. While I endorse CIRA's submission to your committee, I am speaking here in a personal capacity.

I strongly endorse the recommendations in the submission by the Citizen Lab and the joint submission by several civil society organizations. Both of these submissions draw heavily on the fine report by Dr. Chris Parsons, “Cybersecurity Will Not Thrive in Darkness”.

There is no debate over whether Canada needs a stronger regime for securing our critical cyber infrastructure. Bill C-26 contributes to establishing a worthy cybersecurity regime. However, it needs substantial amendment to ensure that the sweeping and secretive powers it grants the government do not override other equally vital values, such as privacy, freedom of expression, judicial transparency and government accountability.

For better and worse, the government's leading agency for ensuring cybersecurity is the Communications Security Establishment. It faces a vital and remarkably difficult task. Fortunately, it appears to be staffed by dedicated experts. However, unsurprisingly, given its origins in wartime signals intelligence, CSE operates with an extraordinary degree of secrecy and boundless appetite for data collection. This is quite justified in some areas of its mandate, but as its capabilities have grown to include extensive surveillance of domestic communications, CSE needs to be much more open and publicly accountable.

In 2013, Snowden documents—notably, about CSE's “CASCADE: Joint Cyber Sensor Architecture”—indicated that the agency was embedding extensive interception capabilities within the Internet infrastructure able to capture a very large portion of Canadians' Internet communication.

While CSE is legally prohibited from directing its activities at Canadians, its capabilities of full take of content and metadata, mass surveillance, and the “incidental” bulk collection of personal and even intimate information on every Canadian Internet user pose a significant challenge to privacy rights and democratic governance more generally.

Renowned cybersecurity expert and director of the Citizen Lab, Ron Deibert, noted the following in 2015: “These are awesome [surveillance] powers that should only be granted to the government with enormous trepidation and only with a correspondingly massive investment in equally powerful systems of oversight, review and public accountability”.

Basic questions here are whether the government should make Canadians aware of this mass surveillance, provide them with robust assurances that this bulk collection is necessary, proportionate, and safe, and offer them an opportunity to decide collectively whether such practices are acceptable or not.

As mentioned by previous witnesses, a key concern with Bill C-26 is its failure to restrict the CSE's use of the information it collects under its extensive new Bill C-26 powers. As Kate Robertson made clear earlier, based on NSIRA reporting, if it is not explicitly prohibited from doing so, the CSE will consider itself authorized to use this information across any of its mandates. This accountability deficit must be fixed before granting CSE new powers under Bill C-26.

Privacy is a fundamental human right. It is essential that Bill C-26 be amended to explicitly define personal and de-identified information as confidential and to ensure that the government obtains a court order before requiring its disclosure. The government must not be allowed to use its sweeping new powers to undermine privacy, such as by weakening encryption or communications security. Data retention periods must be attached to the information it collects.

● (1720)

Before closing, I'd like to briefly raise an issue that is missing from Bill C-26, one that your committee has previously considered important—namely, how the government should handle cybersecurity vulnerabilities. Where Bill C-26 requires telecommunications service providers to conduct assessments to identify any vulnerability in their services—

The Chair: Mr. Clement, perhaps you could wait and maybe we'll get that feedback through questions. We're over our time.

I'm going to move on now to Mr. Motz, for six minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you very much, Chair.

Thank you to the witnesses, both here and online.

The first question is for all three groups.

I've been here since 2016, and during that time I've seen this government constantly attempt to use legislation to give itself excessive power and to avoid accountability. I think back to Bill C-59, the so-called National Security Act, 2017. As well, there have been their attempts during COVID to have over two years of unquestioned authority to spend taxpayers' money without accountability; their attempts to control what Canadians see and say on the Internet through Bill C-11 and Bill C-18; and of course their unprecedented use of the Emergencies Act in 2022, which the Federal Court has just recently, as you know, ruled as being illegal and unconstitutional. The pattern with this government and their legislation should concern Canadians.

Given the organization that each of you represents, and given Professor Clement's research, does this bill as it currently reads not give you pause, especially when it comes to legislating powers that limit Canadians' fundamental rights and privacy?

Ms. Mason, I'll start with you. It's nice to see you again, after seeing you at the Emergencies Act committee. This time, we're hoping to do something pre-emptive as opposed to trying to fix it after the fact, as we tried to do the first time. Could you answer that?

Could all three of you, in your responses, further to what you may have already suggested, suggest how the committee should address the concerns that Canadians have and that you have with those shortcomings?

● (1725)

Ms. Angelina Mason: As we mentioned in our opening remarks, we do need appropriate guardrails. You have to introduce the notion of proportionality. Right now, the powers with respect to cybersecurity directives are so broad that we're not even quite certain just how far those directives could go.

We definitely think the legislation needs to build in appropriate guardrails so that all participants can feel comfortable that the government is acting within a reasonable space.

Mr. Glen Motz: Mr. Clement, go ahead.

Prof. Andrew Clement: In addition to proportionality, which has been mentioned several times, much greater transparency about the operations of the security agencies and the measures that are being taken is required. At this point, we do not have that kind of transparency.

There have been many recommendations, particularly those within the reports I mentioned earlier, that address greater transparency so Canadians can know what's going on. Those would achieve a much better balance. At this point, Bill C-26 is not balanced in terms of those abilities.

Mr. Glen Motz: Okay.

Mr. Ghiz, go ahead.

Mr. Robert Ghiz: Thank you.

I think, as I said in my opening statement, we all agree that the premise of this bill is important and something that we do need, but when it comes to transparency, accountability and judicial rights, there are some areas that need to be tidied up. I think those are the main areas.

In the submission we sent in, we included specific amendments. I think part of parliamentary democracy is that this committee will have the opportunity to introduce amendments and hopefully send the bill back to the House having been improved from what it was when it arrived.

Mr. Glen Motz: Thank you to all three of you for that response.

We've heard repeatedly the terms “overly broad”, “proportionate” and “reasonableness”.

Ms. Robertson from the Citizen Lab, in the previous panel, said that we need to make the right decision now, and that's critical. I agree with her recommendation to have appropriate judicial oversight.

That being said, how would each of you, from the three groups, suggest that we achieve the appropriate balance between judicial oversight and the protection of privacy rights? How do we strike the right balance between protecting critical infrastructure and acting expeditiously, in some circumstances, on what the banking industry would call a priority one critical infrastructure breach? How would we go about protecting that infrastructure as well as the public and their information in those situations, when doing so is warranted?

I'll start off with Mr. Smith and then go to Mr. Clement and Ms. Mason.

Mr. Eric Smith (Senior Vice-President, Canadian Telecommunications Association): We're certainly not suggesting that there be judicial oversight over every aspect of the decision-making process before the decision has been made. Certainly, there needs to be judicial oversight for rights of appeal, rights for the targets of an order to be able to question the order and to challenge whether it's proportional and appropriate.

When the Privacy Commissioner was here, he talked about consultation in terms of making sure that privacy rights were respected. Depending on what aspect of the bill we're looking at, the role of the judiciary will vary. It's all part of what most witnesses are saying. Checks and balances need to be there.

● (1730)

Mr. Glen Motz: Thank you.

Mr. Clement.

Prof. Andrew Clement: One of the things that could be improved—and it was raised by Kate Robertson—is the role that NSIRA, the National Security and Intelligence Review Agency, can play. It's very concerning that it has reported repeatedly that it has not been able to establish that CSE has been operating legally, because it hasn't had access to the information it needs to make that assessment. That's very concerning.

Something in the bill, a recommendation that provides that transparency and that enables NSIRA to get access to that information, would be valuable.

Mr. Glen Motz: Ms. Mason, can you comment quickly? We're just about done.

Ms. Angelina Mason: It's providing thresholds of when orders would even be considered.

We're quite concerned, because if you are an operator and you're dealing with your situation, you're doing your darnest to make sure you're bringing it under control and doing the right things. At what point does the government then step in? Is it privy to knowledge that you don't have? What is it asking you to do? Is it reasonable?

To me, there should be thresholds, particularly when the operators themselves are doing their work in trying to manage the situation.

Mr. Glen Motz: Thank you.

The Chair: Thank you, Mr. Motz.

We'll move on to Mr. McKinnon, please.

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Thank you, Mr. Chair.

I'm going to start with the Canadian Telecommunications Association.

We've certainly heard a lot about the order-making powers of the minister and the concern about confidentiality. I think these are legitimate concerns. I'm wondering, first of all, if you can give us any insight. Do you have any idea what sorts of orders these might be? Can you anticipate the sorts of orders that might come, or is that too speculative?

Mr. Eric Smith: You have to be careful about being speculative, but we've already seen the government make a policy statement in 2022 regarding a requirement to remove equipment from specific suppliers from the infrastructure, namely telecommunications providers, so that's an example.

The order-making powers are very broad, as you know: “to do anything, or refrain from doing anything”. It could be cutting off service to a particular organization, individual, or what have you. It could be requiring you not necessarily to take out equipment from your infrastructure, but to put certain equipment into your infrastructure, or to comply with certain standards. It could be weakening encryption, or it could be requiring you to intercept communications.

The way it's currently drafted could be very broadly interpreted.

Mr. Ron McKinnon: One other concern, as I understand it, is that making such orders public would potentially expose vulnerabilities in various industry practices to bad actors. Do you have any comments on that?

Mr. Eric Smith: Are you talking about the confidentiality of the order, or the confidentiality of information supplied?

Mr. Ron McKinnon: If the order was made public, it might expose vulnerabilities to bad actors.

Mr. Eric Smith: That's a good question. We're definitely sensitive to that. Definitely, there are circumstances where there may be legitimate reasons why portions of an order or in some cases the entire order needs to be kept secret.

The way we look at it is that secrecy should be the exception rather than the norm. That's where I think it's appropriate to have.... Any judgment or requirement to keep an order confidential should be tested. It should go to a judge in order for the government to provide the evidence of why it should be kept confidential, so that there's the opportunity to test that assumption.

Mr. Ron McKinnon: You mentioned, in this context, the notion of a special adviser or advocate, if you will. Can you outline what you see as the role and the powers of such a role? Is there any body within the government, presently, that could step into that role as part of its work?

Mr. Eric Smith: There already are existing mechanisms in situations or court hearings where there is confidential or secret information that can't be made public or shared with the target. A special advocate who has the required security clearance can question the government, test the evidence and test the assumptions that were made. It's not a perfect situation, but it at least provides some mechanism by which the government's evidence can be tested.

● (1735)

Mr. Ron McKinnon: You mentioned the need for checks and balances. You mentioned the need for the rationalization of these orders. Can you suggest any further checks and balances that would be required here?

Mr. Eric Smith: Certainly. Right now, the way it's worded is that, if the minister believes it's necessary to do or not do something.... I think it's important to require that the order be made only after consulting prescribed expert bodies. That could be a C-stack, for example. It could be other cybersecurity bodies within the government. It's to determine not only whether there's a security threat, but whether the order is proportionate and balanced.

Let's face it, our communications systems are very complex. It may seem easy to say to remove this equipment or do something, but we want to make sure that experts, including the targets of the orders, if appropriate, can advise the government of what some unintended consequences could be to the system, or even the viability of some of the smaller providers who are asked to comply with those orders. That's a very important requirement that should be in the legislation.

Mr. Ron McKinnon: As a consequence of some of these orders, different providers may be required to add or remove equipment or change their software. That entails cost. Is it part of your submission that they should be indemnified from such costs?

Mr. Eric Smith: We're not saying that they should be indemnified. It could be just a drafting issue, but the legislation right now says that providers are not entitled to compensation. That's open to interpretation. Does that just mean they don't have a right at law of compensation, or does that mean they cannot be compensated?

What we're suggesting is that there should be discretion for the minister or the Governor in Council to award compensation on a case-by-case basis and that providers who are impacted by those orders should be able to make representations as to whether or why they should receive compensation.

For example, in the United States, the government set up a multi-billion dollar fund to help a certain class of providers remove Chinese-supplied equipment from their infrastructure.

Mr. Ron McKinnon: My last question is on the due diligence defence. Could you give us more information about that?

Mr. Eric Smith: Sure. It's kind of a puzzling thing for us in the legislation, because all other affected parties in the legislation are able to show.... If they're alleged to have committed a violation, a defence could be that they've done everything reasonably possible to avoid making that violation. It could be, for example, that the government says that you must replace this equipment in your infrastructure with equipment from somewhere else, and it's not even available on the market.

For whatever reason, the legislation says that we're the only parties that are not entitled to make that defence.

The Chair: Thank you, Mr. Smith and Mr. McKinnon.

We're going to move on now to Ms. Michaud, please.

[*Translation*]

Ms. Kristina Michaud, Thank you, Mr. Chair.

I want to thank the witnesses for joining us.

I would like to put my first question to the representatives of the Canadian Telecommunications Association. I'll then put a similar question to the representatives of the Canadian Bankers Association.

Almost everyone agrees that Bill C-26 is a step in the right direction, and that it's relatively good news that the government wants to tackle the cybersecurity issue. However, there are fairly widespread concerns about the protection of personal information and privacy, in addition to the government's sweeping regulatory and order-making powers in particular.

You represent carriers and companies that invest in telecommunications networks, such as Vidéotron, Rogers or Bell. I imagine that these large companies are already investing in ways to protect themselves against any cyber-attacks. They have the workforce to do so.

You may also represent slightly smaller companies with fewer customers. This could mean an additional workload for them. Some of them may have already endured cyber-attacks.

At this time, how do the companies that you represent protect themselves against cyber-attacks? What will Bill C-26 change?

If the bill isn't amended, for example, to better regulate the government's powers, will somewhat smaller companies—such as small and medium-sized businesses—consider it a burden or a relief?

I know that it's a fairly broad issue.

● (1740)

[*English*]

Mr. Eric Smith: It's a very good question.

One of the things is that our members have very robust cybersecurity processes already, and, as Mr. Ghiz mentioned in his remarks, they already collaborate deeply with government. Many of the things that could come about as a result of Bill C-26 are things that the industry is already doing. There is CSTAC, the Canadian security communications advisory committee, which puts out best practices and guidance, etc., for all the telecommunication service providers. Bill C-26 could allow the minister to actually order specific practices, for example input.

In terms of the regulatory burden, I don't know of any industry that welcomes additional regulations, as it does add some burden. Again, our members already have robust practices, so I think the additional burden is mostly around things like the reporting requirement. That's where the legislation could require some improvements. It says that we must "immediately report" an incident. Well, "immediately" is right away, and you wouldn't have enough information to even know if you'd had an incident. Some of those things can be improved.

I hope that has answered your question.

[*Translation*]

Ms. Kristina Michaud, Yes, it did, Mr. Smith. Thank you.

I would like to put the same question to the representatives of the Canadian Bankers Association.

According to the Office of the Superintendent of Financial Institutions, banks are increasingly the target of cyber attacks. We've seen some examples in recent months. I imagine that this may lead customers to worry about the protection of their personal information. As in the case of telecommunications companies, I imagine that banks already have certain mechanisms in place and that, as Mr. Smith was saying, they're already meeting the requirements of Bill C-26.

What does this mean for banks? Is it a relief or a burden?

In your opinion, what should be better regulated?

[*English*]

Ms. Angelina Mason: I will confirm the view given by the Office of the Superintendent of Financial Institutions, that we do treat the reporting as mandatory.

I want to clarify a couple of things. One is that the reporting that goes to OSFI is for technology and cyber. If there's a technology incident, even if it's not cyber-related, or if you think of some sort of infiltration into your system, that is reported, because what OSFI is very concerned about is the resilience of our systems in being able not just to secure but also to deliver our services.

When you look at that type of reporting, it's intended to help identify areas of potential concern so that can then be shared back and people can have stronger systems. That's now being done within silos. We do that with OSFI.

The whole point of this legislation is to identify the critical sectors and say that the major players in these sectors, because of what they represent to the security of our whole ecosystem, should be reporting to one central location, so that you're not only hearing what's happening here but you're hearing what's happening in that sector, and we can identify if there's a shared concern, if there are learnings there and if somehow what's going on is connected.

A key part of this legislation is really to improve the available information to help combat cyber-threats. That's definitely a positive that we see, and that's why we've encouraged you to go even broader and allow voluntary sharing at all levels within the ecosystem. That's very positive. Also, there's the fact that we do our cybersecurity planning, and others do their cybersecurity planning, and now that will be validated and centralized so that, again, we can look for learnings about different things in different jurisdictions.

The Chair: Thank you, Ms. Mason.

Mr. Julian, go ahead, please.

Mr. Peter Julian: Thanks, Mr. Chair.

Thanks to our witnesses.

I'll start with you, Mr. Ghiz.

How many cyber-attacks has the Canadian Telecommunications Association had in the past year? I'd like to know whether you're finding that the trend is increasing, staying stable or decreasing.

● (1745)

Mr. Robert Ghiz: Unlike the financial individual who was on earlier, we're not a regulator and we're not privy to the private information of our members. Unfortunately, I don't have that information.

Mr. Peter Julian: However, anecdotally, there would be some discussion within the association, wouldn't there?

Mr. Robert Ghiz: In terms of private, personal business within, no, we're not privy to the information.

Mr. Peter Julian: I'll ask you this, then. If you were sharing best practices, surely the types of cyber-attacks may be similar across your sector. Is there information sharing that helps other companies, for example, put in place protections against cyber-attacks?

Mr. Robert Ghiz: They do that with themselves and with government through CSTAC. It's not through our association that this would happen.

Mr. Peter Julian: Okay.

To what extent were you consulted around the drafting of Bill C-26?

Mr. Robert Ghiz: As an association, we were not consulted. We work with our members to find best practices, and there's a chance that they may have been consulted, but we were not advised on that either. As an association, we were not consulted. We participated in the submission to the committee.

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

Ms. Mason, I have the same question for you. To what extent was the Canadian Bankers Association actually consulted on the drafting of Bill C-26?

Ms. Angelina Mason: We did not participate pre-drafting. We have advocated, for some time now, for common industry standards. We were able to share our thoughts once the first draft was out by meeting with Public Safety and highlighting a number of the recommendations that we've presented here today at committee.

Mr. Peter Julian: Okay.

OSFI—you may have heard their testimony earlier tonight—talked about a move.... In 2022, there were 10 priority one cyber-attacks. In 2023, that tripled to 30 priority one cyber-attacks. Is this your experience as well, within the Canadian Bankers Association? Is the number of cyber-attacks against members of your association increasing?

I'll ask you a question very similar to the one I asked Mr. Ghiz. To what extent do you share best practices? To what extent is there communication among the members to make sure that you are able to head off what may often be similar types of cyber-attacks against your members?

Ms. Angelina Mason: We definitely share best practices. I don't believe that we would get into the specifics of a particular number reporting.

In the case of OSFI, it covers all federally regulated financial institutions, so I'm not privy to which of those would have been our members. However, I think the point is that they are being reported with a view to making sure that they can be shared within the network and addressed appropriately.

Mr. Peter Julian: Thank you.

I'd like to move on to Professor Clement.

You signed on, along with a number of important organizations—the Canadian Civil Liberties Association, la Ligue des droits et libertés, the National Council of Canadian Muslims, OpenMedia, the Privacy & Access Council of Canada—pushing for a series of amendments, 16 recommendations that would help to, in the words of the briefing, “restrain ministerial powers”, “protect confidential personal & business information”, “maximize transparency”, “allow special advocates to protect the public interest”, and “enhance accountability for the Communications Security Establishment”. These are very valuable recommendations that you've brought forward to us, that the coalition has brought forward to us.

What are the most important ones, the ones that we need to be absolutely cognizant of in putting forward amendments to Bill C-26?

Prof. Andrew Clement: There are many recommendations there. We've just talked about a number of them, but I would say that the first recommendation, about constraining the scope of the ministerial orders—which, at this point, is relatively unbounded except by a general sense of necessity—would be one of them. A number of them call for transparency measures, reporting and so on. Those, cumulatively, are very important.

As I was saying earlier, they need to create a much better balance between the security interests and the other rights.

I'll leave it there, and I can follow up with a more specific priority, if you would like.

● (1750)

Mr. Peter Julian: Thank you for that.

What you're saying is that there are some major difficulties with Bill C-26 that need to be responded to, that the bill itself needs to be considerably improved, and that there are a number of amendments that need to be considered for the bill to do what it purports to do but also to ensure that the protection of information and the transparency are there. Is that not true?

Prof. Andrew Clement: Yes, absolutely.

The Chair: Thank you, Mr. Julian and Mr. Clement. Your time is up.

We're moving to the next round—

Mr. Peter Julian: Chair, I'm sorry, but it's six o'clock. I have to go, and I do not consent to continue the meeting.

The Chair: That clock is fast. It's 5:51 p.m.

Mr. Julian, let me proceed. I'm going to suggest two and a half minutes each. Mr. Julian, you have the last question, so if you want to forgo those two and a half minutes, that's great; we'll get out of here a little more quickly. However, we have two and a half minutes each.

Mr. Kurek, you're up, please.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thanks very much. I appreciate the opportunity to engage on this important subject matter.

Professor Clement, I believe the term you used was “awesome powers”, if I'm recalling correctly. Certainly, the surveillance capacity potential, if there are no appropriate safeguards in place, is awesome—or I would maybe suggest another word to use would be “terrifying”.

Are you confident that, as the bill stands right now, there are safeguards in place that would protect Canadians' privacy, their data and their rights?

Prof. Andrew Clement: I'm not confident, as it stands now, that those rights are protected. It's a very one-sided bill in that regard. It gives too much discretion and power to government agencies without the necessary transparency and accountability.

Mr. Damien Kurek: Thank you very much. I appreciate that.

I'll go to our witnesses in telecom and the banks, two industries that are about as popular as politicians.

This has been described as a one-way street in terms of reporting and the mechanisms required to release data to government. There is some uncertainty as to where data would go, whether it's proprietary information or whatnot.

I'm wondering, in the minute I have left—you have about 20 seconds each—if you could describe some of the concerns that you have that the reporting mechanisms are right now a one-way street. Do you feel that needs to be addressed?

I'll start with the folks in the room.

Mr. Robert Ghiz: Well, obviously, I have the double whammy on that, in politics and telecom.

When it comes to that, I agree with a lot of what has been said already—that this bill is good-intentioned but it needs to be improved, and it gets improved with openness and transparency and making sure that the right checks and balances are in place.

Mr. Damien Kurek: Thank you very much.

To our last witness, you have about 20 seconds, if you could.

Ms. Angelina Mason: I'm happy to jump in.

I think there's a strong focus on intervention, and there should be a stronger focus on sharing information to the benefit of the participants in the system.

The Chair: Thank you, Mr. Kurek.

Ms. Michaud, please, you have two and a half minutes.

[*Translation*]

Ms. Kristina Michaud, Thank you, Mr. Chair.

I would like to take this opportunity to—

[*English*]

The Chair: Ms. Michaud, it's my mistake. I apologize. I will get back to you.

It's Ms. O'Connell. I forgot she was here.

Ms. Jennifer O'Connell: Thank you, Mr. Chair. I've been too quiet. You forgot.

Thank you to the witnesses.

Ms. Michaud asked a question that is similar to what I wanted to ask.

Ms. Mason, you pretty much touched on it. I suspect banking will be ahead of the game already in terms of what this legislation is doing, so I'm going to direct my question to our telecom witnesses.

The issue around privacy and privacy protection is very real, and we definitely want to make sure that the balance is right, but on the other side, one could argue that if you are not dealing with critical infrastructure, such as telecommunications infrastructure, in the right way, those bad actors who could access that do not care about the privacy protection of Canadians.

The telecoms and banks—which, again, I think Ms. Mason touched on—hold a lot of data for Canadians, including location data, credit card data and a lot of personal information. If your systems are not protected, with the constant ebb and flow of cybersecurity—let's remember that it is constantly changing—and you're not able to react to those changes and work with government, don't you think the risk to Canadians' privacy would be far greater, being exposed to bad actors who want to access that data and sell it or produce it for nefarious reasons? Wouldn't the privacy of Canadians be better served by strong cybersecurity infrastructure?

● (1755)

Mr. Eric Smith: Yes. I also think our industry is doing a very good job of that. It's a critical function of what our members do. As you mentioned, bad actors are constantly evolving their techniques. We're always having to modify our processes and technology.

Ms. Jennifer O'Connell: Thanks.

You asked questions, too, about physical changes within what some of your membership might be able to access, or not. Again, I would argue that, if there are concerning trends worldwide—they may not even be in Canada—and there is an opportunity to secure our critical infrastructure, working with government would.... Again, it's not just the operations of the telecoms. You hold a large responsibility, which government has been helpful with. You owe it to Canadians. If we are concerned about trends, you have to implement those changes to protect Canadians' data.

The Chair: Thank you, Ms. O'Connell.

Ms. Michaud.

[*Translation*]

Ms. Kristina Michaud, Thank you, Mr. Chair.

I have a fairly simple question. It's the same question that I've asked various stakeholders at other meetings.

Bill C-26 sets out quite heavy financial penalties for organizations that fail to comply with decisions or demands imposed by the government. We don't know what these demands might be, because the power granted is quite broad.

I asked the stakeholders whether these penalties were excessive. Some said that, instead of imposing penalties, incentives should be introduced to encourage organizations to comply with the government's demands. Others said that the penalties should be maintained, but that incentives for organizations should still be implemented.

Mr. Smith or Mr. Ghiz, what do you think of the penalties targeting companies such as the ones represented by your association?

[*English*]

Mr. Eric Smith: Thanks for the question.

Incentives are always good. There are some smaller organizations that have a greater burden to introduce new measures. I think we have a lot of incentive already. Our members' reputations are built on protecting privacy, security, etc.

Our concern with the penalties is this: They are very large and they are cumulative. Also, as I mentioned before, for some reason we're the only industry not afforded a due diligence defence. To be clear, this means that an organization could have done everything reasonably possible to comply, but there could be something in the order that, for whatever reason, is outside of their control and that they were not able to do—yet they're subject to huge monetary penalties and even criminal sanctions against individuals.

[*Translation*]

Ms. Kristina Michaud, Thank you, Mr. Smith.

If there's time, I would like the other speakers to answer the question if they want to.

[*English*]

Ms. Angelina Mason: Sure. I'm happy to jump in.

We are a highly motivated, highly compliant industry, so incentives aren't really necessary in that regard. I agree that incentives could come into play for small and medium-sized businesses to help them achieve compliance, but not for the large, designated operators and players contemplated by this legislation.

The Chair: Thank you, Ms. Michaud.

We're right on schedule.

I appreciate the witnesses today.

Before asking for adjournment, I want to make people aware that our last meeting for Bill C-26 is Thursday. We're contemplating having the amendments in and ready for clause-by-clause when we come back, so that will be by Wednesday noon next week. I know there is some discretion, so we'll likely have further discussions on that on Thursday. That is the outline.

We're adjourned.