HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

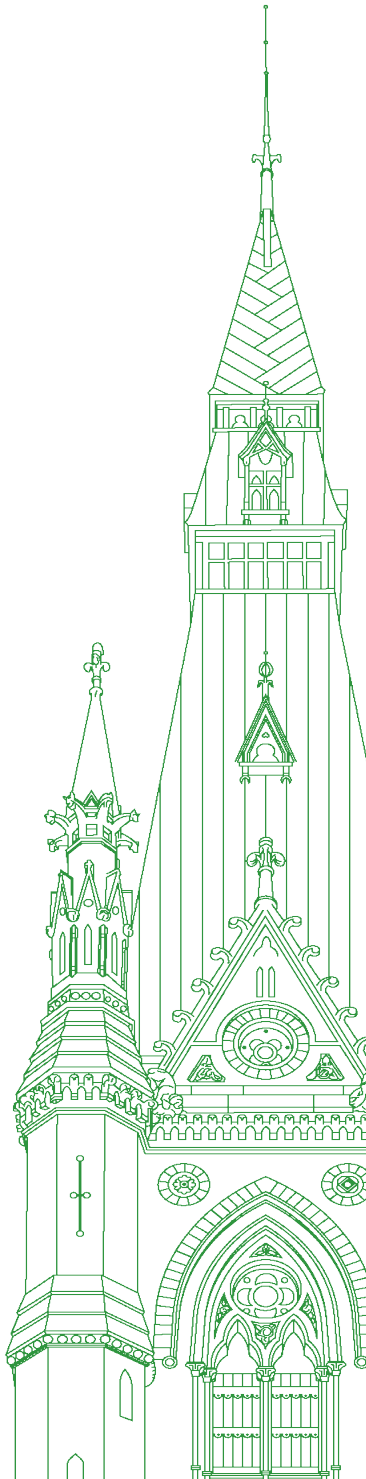
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 020

Tuesday, January 27, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, January 27, 2026

● (1535)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): I now call the meeting to order.

Good morning, everyone. I welcome you to this first meeting of the Standing Committee on Public Safety and National Security in 2026. On behalf of everyone, I would like to wish a happy new year 2026, filled with peace, happiness and good health to all those in this room and those listening to us via video conference.

This is meeting number 20 of the House of Commons Standing Committee on Public Safety and National Security. Pursuant to the House order of reference of October 3, 2025, the committee is meeting today on its study of Bill C-8, an act respecting cyber security, amending the Telecommunications Act and making related amendments to other acts.

I would now like to welcome the Minister of Industry and the officials who have kindly agreed to attend this meeting.

I invite you, Minister Joly, to make your statement.

Hon. Mélanie Joly (Minister of Industry): Thank you, Mr. Chair.

Thank you, colleagues, and I wish you all a happy new year as well.

I am here today to talk to you about Bill C-8, an act respecting cyber security, amending the Telecommunications Act and making related amendments to other acts. This bill has already been passed by the House of Commons and sent to the Senate in 2024. I am here, in good faith, to continue this essential work. This bill deals with something that Canadians depend on every day: our telecommunications networks.

Our telecommunications networks connect Canadians and support our economy. The growth of the digital economy, particularly through 5G networks, could add up to $112 billion to the Canadian economy by 2035. This is a great opportunity, and we have a responsibility to protect it.

[*English*]

With greater connectivity comes greater exposure. Cyber-threats are more sophisticated, more aggressive and borderless. Canadian businesses lose more than $5 billion every year due to cybersecurity incidents. This is a massive cost to our economy, our competitiveness and the jobs Canadians rely on.

If we want Canadians to trust these systems, and if we want businesses to continue investing and innovating, our infrastructure must be strong, secure and resilient. This is exactly what Bill C-8 does. Bill C-8 modernizes the Telecommunications Act by making security a core objective. It gives the government targeted and practical tools to act when there are serious risks to networks. It requires consultation with affected parties before any order is issued, ensuring transparency and collaboration.

At the same time, it is important to be clear about what this bill does not do. It does not allow the government to shut down services for individuals. It does not allow the interception of private communications. Infrastructure security is not freedom of speech. This bill is about protecting networks, not regulating expression or ideas.

Bill C-8 includes strong safeguards, and the government is accountable to Parliament. We will ensure that the bill is explicit in affirming Parliament's ongoing oversight of these powers. There is robust parliamentary oversight. NSIRA and NSICOP play a vital role in reviewing national security activities, and this legislation fully respects that framework.

● (1540)

[*Translation*]

Telecommunications networks are essential to the security, prosperity and well-being of Canadians. Bill C-8 allows the government to protect them in a responsible and targeted manner, under rigorous oversight. We will continue to work to keep Canadians safe and well connected.

With that, I am ready to take your questions. Thank you.

The Chair: Thank you, Minister.

We will now move on to the first round of questions, starting with Mr. Caputo for six minutes.

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you, Mr. Chair.

Thank you, Minister, and welcome.

[*English*]

Thank you for being here, Minister.

This act, I think we can agree, confers tremendous powers to the minister and the Governor in Council. We can agree on that, I take it.

Hon. Mélanie Joly: It's an important responsibility, and that's why there's parliamentary oversight.

Frank Caputo: Okay.

Parliamentary oversight happens after the fact, after a decision is made. Then Parliament looks at things. We know how that sometimes goes, because if the wrong decision is made, we try to repair it after the fact.

What I'm going to ask you, Minister, is this: Why wouldn't we have judicial oversight, a judicial authorization at the front end, whenever you—or the government—wish to take action, as in proposed section 15.2, to ensure that the government isn't breaking the law? Would you not support that, rather than looking at something after the fact to see if we got it right?

Hon. Mélanie Joly: I hear you. The goal is definitely to make sure that the government can act, particularly in times of national security when urgency is required, and that it is part of our intelligence system, but we already have NSICOP and NSIRA doing that work.

I must say, having dealt with a lot of security issues in my former role, I think this is an important power given to the Minister of Industry—

Frank Caputo: It's a tremendous power.

Hon. Mélanie Joly: —that we don't take lightly.

Frank Caputo: I understand that.

Hon. Mélanie Joly: At the same time, dear colleague, I would just like—

Frank Caputo: Minister, I'm sorry. We have only a few minutes.

Hon. Mélanie Joly: What preoccupies me right now is.... We passed this bill.

Frank Caputo: I understand that, but I'm not asking you—

Hon. Mélanie Joly: We already passed this bill in the past.

The Chair: I'm sorry. I have to stop both of you.

[*Translation*]

I think we all understand that we cannot speak at the same time as others. Otherwise, it is absolutely impossible for the interpreters to do their job and very difficult for everyone to follow the discussion.

Please continue.

[*English*]

Frank Caputo: I'm not trying to interrupt you, Minister. I have only four minutes and we have a lot to get through, so please do not take it personally if I interject.

Hon. Mélanie Joly: No, I don't.

Frank Caputo: Here's the thing: Everything you've discussed is after the fact.

You talk about robust oversight with NSICOP. There is a principle in law called exigency, as in when a warrant or judicial authorization can't be obtained. That's different. In some instances, a judge would have the time and the evidence, and warrants are often obtained within a few hours.

Rather than having the minister exercise unfettered discretion over such broad powers, would you not agree that we should have judicial authorization and an independent judge should be the one making the decision, where we can do that?

Hon. Mélanie Joly: If the committee comes up with amendments, of course we will study them. Our goal is always to make sure that we get to the right balance, because it's really important that the powers of a given minister in given circumstances have guardrails. I think it's important.

Frank Caputo: I understand that.

Hon. Mélanie Joly: At the same time, this must fit within the overall Telecommunications Act infrastructure, which is also in line with the CRTC, etc. We would need to make sure that it fits, and that's why, in the circumstances, this was proposed.

Kasi, do you want to add anything?

Frank Caputo: I would like to restrict my questions to you, Minister, with all due respect. We can ask the officials afterwards. I have two and a half minutes left with you.

Again, I don't understand. I don't think I'm being obtuse or anything. Why wouldn't we have an independent judge decide whether there is evidence for you to wield these significant, virtually unprecedented powers? Why wouldn't we give them over to a judge, Minister?

● (1545)

Hon. Mélanie Joly: Listen, I don't think they're unprecedented powers, Frank. I'm sorry. I think it's an important bill and it's about making sure that we can protect our critical infrastructure. We've already had unanimous consent for it.

We have a model right now that is based on a voluntary approach for telecommunications service providers that doesn't hold, because right now, we have policy statements on national security that are voluntary. It would make sense to give these powers and to make sure that telecommunications companies abide by them.

By the way, I must say—

Frank Caputo: I'm sorry. I have one—

Hon. Mélanie Joly: —the Minister of Industry, under the Telecommunications Act, also has great powers regarding how the telecommunications sector is organized.

Frank Caputo: I have just one minute left, Minister. I'm sorry.

Hon. Mélanie Joly: I think what's been presented to you here is very coherent and in line with the policy across the country already.

Frank Caputo: Minister, why should Canadians trust you with these extraordinary powers, given your government's record?

Hon. Mélanie Joly: This is not about personalizing the approach.

Frank Caputo: I'm talking about the government, not personally.

Hon. Mélanie Joly: Any of us could one day be Minister of Industry.

Frank Caputo: I'm talking about the government, though.

Hon. Mélanie Joly: It's about the responsibility that is given to that individual during the tenure of the government.

Our goal is to protect Canadians. This is our number one responsibility, and that's what we're doing through this.

Frank Caputo: Even when you sat at the cabinet table.... We have seen so many failures with this government, whether they be on Stellantis or the Emergencies Act. I don't know that Canadians have trust when it comes to balancing rights and protecting our infrastructure. That's why I believe in judicial authorization.

Hon. Mélanie Joly: I would like to answer that.

I think Canadians have already shown trust in our government, and that's why you're sitting on the right side of the table.

Frank Caputo: Well, that's—

Hon. Mélanie Joly: Thank you.

Frank Caputo: —a little inappropriate.

The Chair: I think we'll stop here and invite MP Acan to the floor for six minutes, please.

Sima Acan (Oakville West, Lib.): Thank you, Mr. Chair.

Thank you, Minister, for joining us today.

As we all know, this is our fifth meeting on Bill C-8. We heard from experts on the importance of this bill, and some of these experts are Canadian critical infrastructure leaders.

Throughout the study of this bill, we also heard Conservative colleagues claim that Bill C-8 will allow the government to kick Canadians off the Internet just for criticizing our government. We know this claim to be false, but can you please reiterate to the committee why claims such as these are not only inaccurate but also equally harmful misinformation that puts Canadians in danger?

Hon. Mélanie Joly: This is not about the content on the Internet, about free speech. This has nothing to do with what is discussed online. This is about the infrastructure of the telecommunications sector. This is about the towers, the wires. This is basically the mandate of the Minister of Industry, which is about protecting Canadians through protecting the critical infrastructure of the telecommunication networks across the country.

If I were the minister of heritage or the Minister of Justice, conversations would be different, obviously. It would be much more about the content online. It would be much more about the Broadcasting Act, everything linked to online harms or, potentially, the application of the Criminal Code. This is not the case.

I hear that colleagues want to make sure that there's certainty regarding that aspect. I'm willing to hear amendments that would make sense to all to make sure that we are clear about protecting people's rights online, but I just want to make sure that this very important legislation can pass.

I think the wisdom of the last Parliament was clear. It needed to be done. It was done. Because of a technical procedural aspect, this bill had to come back. Now we have to redo the entire work at a time when the world is more dangerous and more complicated. We just need to have the means to ensure the safety of Canadians through the Telecommunications Act.

● (1550)

Sima Acan: Thank you, Minister.

From my perspective, an engineering perspective, I would say that the resilience of our economy is only as strong as the physical and logical layers of our telecommunications networks. Previous testimony from Bruce Power highlighted that a nuclear facility's security means little if the downstream system of systems, such as the power grid and telecommunications lines, remains vulnerable.

How does adding security as a primary policy objective in the Telecommunications Act empower your department to enforce the unified technical baselines necessary to protect these critical interdependencies?

Hon. Mélanie Joly: As I said, it is not only important because it's overdue. I mentioned, when answering our colleague Frank Caputo's questions, that we needed to make sure that we were putting this bill forward because it is a way to ensure the security of Canadians online. The Telecommunications Act, decades ago, didn't put that as a priority, so we needed to make sure that it was.

I think what is important, Sima, to remember is that we're the only one of the Five Eyes that doesn't have legislation like this at this point, and time is of the essence. That is why I think our allies expect us to do that. It is just good governance to do that. I think we should not politicize this bill; I don't think this is the right content or the right forum.

Sima Acan: Thank you.

The Chair: You have a minute and a half.

Sima Acan: Minister, in your capacity as Minister of Industry, you met with the biggest industries. Could you tell us what priorities and concerns these key stakeholders have shared regarding the protection of our critical infrastructure from cyber-attacks?

Hon. Mélanie Joly: I think that when it comes to their expectations towards the government, they're expecting us to do our job and to pass this bill. The more they're able to have regulatory predictability, the better. This is because they will be able to address the risks and, basically, the investments required.

Right now we have a voluntary system, including a policy statement from back in 2022. That is important, but it doesn't give any form of teeth, if I can say that, to the government to make sure that it's complied with by the telecommunications service providers. That's an issue. I think the sooner we're able to pass this bill, the sooner it will be factored in by those in the telecommunications sector.

Sima Acan: Thank you, Minister.

[*Translation*]

The Chair: Thank you, Ms. Acan.

I will now give the floor to Mrs. DeBellefeuille for six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Thank you very much, Mr. Chair.

Thank you for being here, Minister.

When a bill is drafted, consultations are held beforehand to ensure that it truly meets the need for which it is intended. I was surprised to learn that the Privacy Commissioner's recommendations regarding the bill were not taken into account. He told us that the bill was somewhat uneven in terms of the criteria of necessity and proportionality. I wonder where you stand on this, because it seems to me that, throughout the work on the bill, the government has shown its commitment to the criteria of necessity and proportionality in the exchange of personal information. As you know, the protection of personal information is important to Quebeckers and Canadians.

Can you explain why you did not adopt the recommendations of the Privacy Commissioner?

Hon. Mélanie Joly: My colleagues and I inherited this bill, which had already been passed, but for unfortunate procedural reasons, it died on the Order Paper. We therefore reintroduced the bill, which remained unchanged. The parliamentary legislative work has already been done. However, I understand that my colleagues now have other points of view. As I said earlier in response to my colleague Mr. Caputo, I am quite willing to consider amendments.

Claude DeBellefeuille: You could consider amendments that would address the commissioner's recommendations.

Hon. Mélanie Joly: Yes, I am prepared to consider amendments related to the criteria of proportionality and necessity. My goal is to bring regulatory predictability and certainty, but at the same time to strike a good balance between government powers and privacy protection.

● (1555)

Claude DeBellefeuille: That's perfect.

My second question concerns back doors. Several witnesses have told us that the bill, in its current form, would weaken encryption standards, which could increase the risk of cyber-attacks. Agencies would have easier access to certain personal information, but this information would also be available to foreign entities that wanted to obtain it.

Why is there this desire to weaken encryption standards?

Hon. Mélanie Joly: There is no desire to weaken encryption standards. Perhaps Ms. McMicking could add something on that point.

Kasi McMicking (Associate Assistant Deputy Minister, Strategic Policy Sector, Department of Industry): I will turn to my colleague, Mr. Arbour.

Claude DeBellefeuille: Mr. Arbour, it's not that I don't want to hear you, it's more that I want to make it clear to the minister that this is a fairly important issue. It seems to be a matter of vocabulary…. I didn't know what an encryption standard was. I learned about it. However, weakening this standard is a very important issue, and it has been highlighted by many witnesses.

So I understand, Minister, that you may have difficulty explaining to me why it was not included in the bill.

Hon. Mélanie Joly: No, I just want to make sure that my colleague can provide a little more detail on that. I can also add some later.

Andre Arbour (Director General, Telecommunications and Internet Policy Branch, Department of Industry): Thank you for your question.

I understand the concerns in this regard, but the purpose of the bill is to secure the telecommunications system. However, it is already impossible to create a decree to break the encryption of a network.

Claude DeBellefeuille: Mr. Arbour, I don't want to interrupt you, but this issue is very important to me. I have asked this question several times. If it were as simple as you say, why are expert witnesses so concerned about this issue?

Madam Minister, can you explain to me why the witnesses we heard from expressed such concern about this issue?

Hon. Mélanie Joly: We have heard the comments related to the issue of encryption. We are prepared to examine amendments on these issues so that there are no problems with regard to the protection of the telecommunications system and its infrastructure, the path to encryption and the protection of privacy. We understand that this transition must be adequately covered by the bill. For this reason, I would welcome amendments on these issues. That said, I absolutely do not want this to lead us to the issue of freedom of expression. That is what I fear, and that is why I want to ensure that we limit ourselves to critical infrastructure issues.

Claude DeBellefeuille: Many witnesses have proposed amendments. We see that you are willing to discuss them.

I have only one minute left to speak. My last question concerns the overlap of standards. Electricity Canada made a recommendation to us on this subject. For example, in Quebec, Hydro-Québec already adheres to North American international reliability standards and is concerned about the overlap of standards and their duplication.

If we tried to clarify everything, we might be able to reassure Electricity Canada and Hydro-Québec. What do you think?

Hon. Mélanie Joly: I believe that the Telecommunications Act is a federal law. We do not believe that we are outside our jurisdiction.

We are happy to work with all the electricity companies in the country, which are, of course, under provincial jurisdiction—

Claude DeBellefeuille: I don't want to interrupt you, Minister, but is power transmission under federal jurisdiction? I believe it is excluded from the act.

Hon. Mélanie Joly: Telecommunications itself falls under federal jurisdiction. All systems of—

Claude DeBellefeuille: Power lines are not under federal jurisdiction.

Hon. Mélanie Joly: If they are interprovincial, they fall under federal jurisdiction. If they are in Quebec or within a province, they are a matter of provincial jurisdiction.

Claude DeBellefeuille: There is still a problem, however—

The Chair: I'm sorry to interrupt you. Unfortunately, your speaking time is up.

That was very interesting, I would have liked to let you continue.

Hon. Mélanie Joly: We were doing a course on the distribution of jurisdictions.

The Chair: Unfortunately, not only are we off topic, but we have also exceeded the time allocated for your discussion.

Mr. Lloyd, you have the floor for five minutes.

[*English*]

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

Thank you, Minister and officials, for being here.

Minister, one of the key reasons your government cited for bringing forward this legislation was the need for you, as minister, to have the authority to remove hardware or prevent the installation of hardware that could pose a threat to our telecommunications system. Specifically, I'm talking about Huawei and ZTE.

Can you confirm to this committee that, if granted these powers, you will make an order to remove any remaining Huawei technology from our telecommunications system?

● (1600)

Hon. Mélanie Joly: That's the goal of the 2022 policy statement regarding ZTE and Huawei. That's why I've mentioned, at least three times—

Dane Lloyd: Give a clear, yes-or-no answer, Minister.

Hon. Mélanie Joly: I want to finish—

Dane Lloyd: Answer yes or no, Minister. Will you use this legislation to remove—

Hon. Mélanie Joly: I'm sorry—

The Chair: I'm sorry. This was going well, and it's going to keep going well, but we can't interrupt. Otherwise, no one can interpret and no one can understand. Let's continue in the appropriate manner.

MP Lloyd.

Dane Lloyd: Answer yes or no. Will you use these powers to order the removal of any remaining Huawei technology from our telecommunications system?

Hon. Mélanie Joly: That's the goal of the 2022 policy statement: to make sure that there would be none.

Dane Lloyd: The whole reason for this legislation being brought forward, Minister, was to give you that authority. That is what your government stated it needed this for. We're talking about granting you these powers. You will now have these powers, if you get this legislation passed.

Will you use them to remove Huawei and any other threats from our telecommunications system?

Hon. Mélanie Joly: Of course. That's the goal.

Dane Lloyd: Okay.

Following your government's recent trip to China and the Prime Minister's efforts to reset the relationship, was there any discussion about reconsidering the ban on Huawei?

Hon. Mélanie Joly: No.

Dane Lloyd: Okay. I'm asking this because your office and the Public Safety office were asked repeatedly by The Hill Times about these discussions, and they refused to respond to any of those questions, so—

Hon. Mélanie Joly: Talk to them.

Dane Lloyd: —I think Canadians have a lot of concerns about that.

Minister, Bill C-8 proposes a number of new powers for you, including the ability "to direct telecommunications service providers to do anything, or refrain from doing anything" that you deem to be a threat to national security interests. What safeguards are in place to ensure that these are not abused?

Hon. Mélanie Joly: I've already answered that question. There's definitely parliamentary oversight by NSIRA and NSICOP. That was well noted the last time the bill was studied, and that was added. Having gone before NSICOP in the past and having worked with NSIRA.... They can go into the details of many key public safety and security questions.

Of course, everybody on this committee has their security briefings. We believe in security briefings being a key part of the work that can be done by parliamentarians, and we'll work with them. That will be at the core of any minister of industry's work in the future.

Dane Lloyd: Thank you, Minister.

The Privacy Commissioner has testified that this bill lacks key privacy safeguards and that it includes an inconsistent proportionality test, which is included in proposed subsection 15.2(3). Also, there's no requirement for his office to be notified by the Communications Security Establishment when a major cyber-breach threatens Canadians' private information. I find these omissions in the legislation concerning.

Are you supportive of these amendments to alleviate the Privacy Commissioner's concerns?

Hon. Mélanie Joly: That was the question of our colleague from the Bloc Québécois. Claude DeBellefeuille just asked that question.

I'm very sensitive to that question, because it's really important that we address the issue of proportionality. I really think Canadians should know. Should there be breaches of networks containing their data, they should be informed. I would be very interested in seeing amendments regarding that.

Dane Lloyd: Now, in my last minute or so....

I thought it was very interesting that you stated that an individual will never be cut off from their Internet access. That was a very unequivocal statement, which I'm pleased to hear you say. You know, nobody has been very clear that.... The officials were not that clear in saying.... So, you don't anticipate that there will be any situation in which an individual would have their Internet access cut off, like if they're a hacker or something like that.

Hon. Mélanie Joly: Well, the bill refers to the term “person”, and the term “person” was defined as, basically, companies. I think it was just lost in translation, but we can make sure that telecommunication service providers and, obviously, their suppliers could be.... We can make sure that we define that in a way that we're not creating any form of misinterpretation.

Dane Lloyd: Yes. One concern is that.... Let's say that somebody is caught up in this. They might not have the legal ability to challenge a decision like this. There is judicial overview. What resources are going to be made available to ensure that somebody who feels they've been unfairly targeted by this legislation can challenge this?

Hon. Mélanie Joly: Like I said, this legislation is not targeting individuals; it is targeting companies.

Dane Lloyd: Okay, well, we want to be clear about that.

Thank you.

Hon. Mélanie Joly: I think it's a fair point, and that's why we'll make sure that we address it.

Thank you.

[*Translation*]

The Chair: Thank you for that exchange, Ms. Joly.

Mr. Powlowski, you have the floor for five minutes.

● (1605)

[*English*]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Minister, I understand the importance of protecting privacy, and I understand the importance of transparency, so you need to have these checks and balances within the legislation. However, in responding to a cybersecurity threat, I think that you need to act very quickly. I'm thinking about nowadays, especially with AI. You put something—you ask some complicated question—into your computer or your laptop, and then it goes off into outer space and around and around. Within almost a couple of seconds, it comes back with a response that would have taken us days and days to have come to in the old days. So, obviously, the threat is going to be very fast, and you have to consider that when you're putting in your checks and balances.

If I were Mr. Putin, I'd say, “Oh, put in a lot of checks and balances. We have to be really certain that we don't violate civil liberties here, so it takes hours or days.” I know there's a balance.

Can you talk about this bill and how the order-making power under this bill provides the flexibility to respond quickly to cyber-attacks while still being subject to clear reporting and accountability mechanisms?

Hon. Mélanie Joly: Yes. I think I hear what the Conservative colleagues are talking about, but we're also inspiring ourselves with legislation that has been adopted within the Five Eyes.

We're also looking at what has happened in real-life events, such as ransomware attacks. I know Nova Scotia Power was the victim of one in 2025. There was also an AT&T breach of user information in 2024. I could go on; I have many in front of me right now. In South Korea, SK Telecom reported a cyber-incident with malicious actors accessing data. There was also espionage and disruption that happened primarily in the U.S.; that was the Salt Typhoon event in 2024.

I'm just saying that sometimes time is of the essence. We need to be able to inform telecommunications service providers that may not be aware. We sometimes need to be able to ask them to do things very quickly while dealing with an ongoing threat that is affecting many allies within NATO. That's why I think we cannot address.... How can I say this? Time is of the essence, and we need to be efficient. That's also why we need to create parliamentary oversight. The NSICOP and NSIRA approach is the right one because you're able to see whether the government did the right thing at the time, based on the intel that was offered to those who were making the decision.

Marcus Powlowski: How much time is left?

The Chair: You have two minutes.

Marcus Powlowski: Okay.

Mr. Caputo suggested that, if there is time, there should be judicial oversight and a requirement to ask for a warrant beforehand. Do you know or can some of your staff tell me—because you say that all the other Five Eyes countries already have similar legislation—whether in the legislation from those other countries there is that kind of judicial oversight? Is there a requirement for a warrant before you act?

Hon. Mélanie Joly: Andre can answer that question.

Andre Arbour: Thank you for the question.

In this particular context, where we're talking about authorities to regulate the operation of network infrastructure by the private sector, I'm not aware of any such example that exists. The circumstances where there is that type of warrant architecture exist when there is an investigative function. There's some type of either intelligence surveillance or other law enforcement surveillance that's outside the context of regulating the day-to-day operation of the networks. It's about government authorities having access to information that normally would be subject to the right to privacy.

Marcus Powlowski: The kinds of cybersecurity threats where an outside source is trying to shut down your system, your transmission lines or your power stations are not normally, in other countries' legislation, subject to that kind of judicial oversight.

Andre Arbour: No, not that I'm aware of. Certainly, the court in Canada does not currently have the expertise or the capacity to consider those types of questions that get into the substantive day-to-day operation of the network infrastructure, as opposed to questions about rights or investigations.

● (1610)

[*Translation*]

The Chair: Thank you, Mr. Powlowski.

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Minister, I have two questions for you.

The Honourable Simon Noël, the Intelligence Commissioner of Canada, made only two recommendations in relation to Bill C-8.

First, he proposed that an independent commissioner be appointed to provide independent oversight and regulate access to and use of personal information and its dissemination.

Second, he proposed that any inspection of premises, seizure of documents or collection of private information by a superintendent be preceded by a warrant issued by a judicial authority.

The intelligence commissioner tells us that he has only two recommendations to make for the entire bill, but they are still not included. Can you explain why the intelligence commissioner's recommendations were not considered relevant and included in the bill?

Hon. Mélanie Joly: I have already answered your question to some extent, as it is similar to the one you asked me earlier.

We reintroduced the same bill that had been passed in the House of Commons and the Senate, which had been unanimous and represented a consensus.

That said, I understand that there have been other interpretations since then. As I said, we are prepared to consider certain amendments. We can certainly work with the intelligence commissioner primarily to protect the personal data of Canadians. The goal is not to create a new commissioner's office infrastructure, but rather to work with the infrastructure already in place, particularly with the office of the intelligence commissioner.

With regard to—

Claude DeBellefeuille: I am not very familiar with the commissioner's specific duties, but why do you think he did not claim this responsibility and instead proposed another commission? How do you interpret this?

Hon. Mélanie Joly: You would have to ask him that question.

Currently, my concern is different, perhaps because my previous role was closely linked to geopolitical events that sometimes led to cyber-attacks against the Government of Canada's infrastructure or our businesses. When this kind of thing happens, things move quickly. Personally, it's our ability to respond to situations that actually occur that worries me. Suddenly, we have to make calls to protect ourselves quickly.

Once these situations have occurred, we are managing a crisis. So we need to be able to look back and see if things were done properly and how we are adapting.

The Chair: Minister, I am sorry to interrupt you.

We must move on to the next intervention.

Mr. Strauss, you have the floor for five minutes.

[*English*]

Matt Strauss (Kitchener South—Hespeler, CPC): Thank you, Mr. Chair.

Thank you, Minister, for being here.

You said in your opening remarks that this bill would not provide for the withholding of services to individuals. In answer to my colleague Mr. Lloyd, you said that even though the word "individual" is in the bill, going back to the definitions in the Telecommunications Act, an individual person wouldn't be included. I have with me here the definitions section of the Telecommunications Act. It defines "person" as "includes any individual".

Are you undertaking here to change that definition so that it does not include any individual?

Hon. Mélanie Joly: I'm willing to make sure there's even a section—if you bring in an amendment, we could definitely work with it—to make it clear that this will not have any impact on freedom of speech online or anything linked to the type of content that could be put online.

Matt Strauss: Would you remove the definition of “any individual”?

Hon. Mélanie Joly: That was part of my answer to our colleague from the Bloc Québécois: I want to make sure we're talking only about the critical infrastructure and that it doesn't go into the connectivity part of ultimately how we are addressing what people are discussing on the Internet. That's really important, because I think it's not the role of the Minister of Industry. This is not how the government is organized. That question should be addressed by the Department of Canadian Heritage.

● (1615)

Matt Strauss: Okay, thank you.

The bill as it's written right now says that you would have oversight to withhold services to an individual if “any threat” to the telecommunication system arises. It doesn't say any physical threat or any structural threat; it says “any threat”. What particularly concerns me about this is that there are several internal Government of Canada documents describing misinformation and disinformation as threats to the telecommunication systems of Canada.

I'll put it to you like this: Do you and your government believe that misinformation and disinformation are threats to the integrity of the telecommunication system in Canada?

Hon. Mélanie Joly: This is not about misinformation or disinformation. That is a question that should be asked much more in the context of anything linked to the online harms act or anything that would be much more about content. At the Department of Industry, we're not addressing these questions. It has nothing to do with it.

Matt Strauss: I hope not, but the bill that's before us says “any threat”, so are you hereby undertaking to change the language to mean any physical or structural threat?

Hon. Mélanie Joly: The bill is clear that this is about critical infrastructure and threats to the telecommunication networks, the wires and the towers, etc. It has nothing to do with what is being discussed online. I think the last Parliament saw that clearly, and this should be clear here as well.

Matt Strauss: I think it should be clear.

Hon. Mélanie Joly: I understand that if it's not clear enough, we can make sure there's an amendment regarding that.

Matt Strauss: Okay, that's fantastic.

In the previous Parliament, when this bill existed as Bill C-26, it was thoroughly criticized by the Canadian Civil Liberties Association, the Canadian Constitution Foundation and the Justice Centre for Constitutional Freedoms. I've discussed the bill with the directors of many of those organizations. None of the criticisms they made turned into amendments when that bill was passed by Parliament, and none of the Conservative amendments, as far as I can tell in the archaeology of this bill, were passed at the last committee.

It sounds like you're now expressing an openness to amendments, but none of that occurred when amendments were sought for Bill C-26 in the previous Parliament. Why the change?

Hon. Mélanie Joly: Doug Shipley, the member for Barrie—Springwater—Oro-Medonte, said this:

> Madam Speaker, I am proud to rise in the House today to speak to this important legislation on behalf of the good people of Barrie—Springwater—Oro-Medonte. I am pleased to see Bill C-26 come forward in the House. Improving the resiliency of our critical infrastructure is of the utmost importance to our national security and the everyday safety of Canadians.

That's what your colleague said.

Matt Strauss: Thank you. I've never met that colleague.

I'm interested in your opinions about that.

Hon. Mélanie Joly: Here's another one. Pat Kelly said, “Bill C-26 is a bill that addresses an important and growing topic. Cybersecurity is very important, very timely. I am glad that, in calling this bill today, the government sees this as a priority.”

Matt Strauss: I'm sorry, but I'm not interested in those opinions.

Hon. Mélanie Joly: That was the member for Calgary Rocky Ridge, Alberta.

Matt Strauss: I'm sorry, but that has no bearing on my concern or the concerns of my constituents.

Hon. Mélanie Joly: I also have something from Garnett Genuis, member for Sherwood Park—

[*Translation*]

The Chair: Thank you very much, Minister.

Mr. Strauss, you have the floor.

[*English*]

Matt Strauss: Thank you very much.

Do you accept that the powers in this bill potentially touch on the fundamental freedoms protected in section 2 of our charter, the freedom of expression, if an individual were to find themselves not receiving services from an ISP?

The Chair: We have 20 seconds left.

Hon. Mélanie Joly: We have the Charter of Rights and Freedoms, and every single piece of legislation abides by it. It's a constitutional responsibility, and we are making sure that's the case, period.

Matt Strauss: Thank you.

Do you regret violating section 2 with the invocation of the Emergencies Act, as the Federal Court—

The Chair: MP Strauss, I'm sorry to interrupt you. That's all the time we have.

Let me turn to MP Lavoie.

[*Translation*]

Mr. Lavoie, you have the floor for five minutes.

Steeve Lavoie (Beauport—Limoilou, Lib.): Thank you, Mr. Chair.

Minister, thank you for joining us today.

Allow me to put on my economist's hat today. I come from the world of economics. I have worked with businesses for over 25 years. Cybercrime is a nightmare for businesses. In manufacturing, when a machine stops working, we know what to do to fix it. However, for most businesses, a cybercrime-related problem is truly one of their worst nightmares.

The business community firmly believes that we must give ourselves the means to protect Canada, to protect businesses, to protect investments and, ultimately, to protect jobs. Protecting the jobs of Canadians is important.

That being said, I would like to talk to you a little bit about predictability today. I sit on another committee that deals with trade. The two words we hear most often are "predictability" and "unpredictability." We have always known that businesses need predictability in order to invest and attract investment. Right now, we are living in a world of unpredictability, and we are being told that this is the new normal. As they say, they have to keep learning to dance with it.

How does this legislative framework provide more predictability and certainty for Canadian businesses so that they can continue to invest, grow and innovate with confidence?

● (1620)

Hon. Mélanie Joly: That is a very good question.

Indeed, there are many things in the world that we cannot control, particularly those that originate in the White House or occur south of our border. However, there are many things that we can control, including how we control and secure our telecommunications services and networks.

Your question leads me to explain the cost of cybersecurity. I mentioned this in my introduction, but every year, cyber-incidents and cybercrime cost the Canadian economy approximately $5 billion. A cyber-incident costs businesses an average of $7 million, which is enormous. This does not necessarily apply only to large companies; it also affects small and medium-sized businesses.

Our goal is therefore to provide the predictability you referred to. It is unfortunate that we were not able to pass this bill earlier. There is an urgent need for action. We are lagging behind our allies, and certainly behind the Group of Five. We must therefore take action.

Steeve Lavoie: You mentioned billions of dollars of investment in our economy.

Can we expect that an increase in cybercrime will create new specialized jobs in the technology and digital sectors in Canada?

Hon. Mélanie Joly: Yes, absolutely.

There are a number of things. We believe that we can increase employment in the telecommunications sector, but also in the digital services sector in general.

The Prime Minister often talks about the importance of artificial intelligence. We believe that many people working in the telecommunications and digital services sector will also be very useful in developing an artificial intelligence industry in this country. We have already seen major players in the telecommunications sector, such as Bell and TELUS, invest heavily in artificial intelligence. Even recently, agreements have been signed with a very important Canadian company in the field of artificial intelligence, namely Cohere, which we want to continue to develop.

So yes, I think the potential is huge, but we still need a more developed regulatory infrastructure. The issue of security is at the heart of what is missing in the Telecommunications Act.

Steeve Lavoie: I would like to add something to what you said earlier. You mentioned a cost of $5 billion for businesses. We currently estimate that amount to be $5 billion dollars, but it has enormous repercussions for employees, the supply chain and customers. So it's eagerly awaited.

Thank you.

Hon. Mélanie Joly: Thank you.

The Chair: Thank you, Mr. Lavoie.

Ms. Kirkland, the floor is yours for five minutes.

[*English*]

Rhonda Kirkland (Oshawa, CPC): Thank you, Chair.

Thank you, Minister, for being here.

I'm pleased to hear some of the things that I'm hearing today. It sounds like you're open to recommendations from the Privacy Commissioner. I think it sounds like you can understand why leaving out the standard of what's necessary and proportionate would create uncertainty about how these powers will be applied. I'm saddened to hear that you left them out. You said that you inherited the bill. It's almost like you just rubber-stamped it without looking at what that would have meant. I would have liked to see that not having to be part of the amendment process, but we are certainly happy to hear that you and your government are open to those amendments.

At the October 30 meeting, the Centre for International Governance Innovation raised concerns about proposed sections 15.1 and 15.2 for the Telecommunications Act, which give the Governor in Council or the minister a broad authority to impose secrecy around certain orders and decrees. They recommended that clear guidelines be included to govern the use of these "extraordinary" non-disclosure powers.

Can I ask why the government chose not to include those guiding criteria in the legislation to limit how these secrecy powers can be used?

Hon. Mélanie Joly: I think it's important for people to remember that since we're living in a much more chaotic and dangerous world, the government has to deal with a lot of hostile actors that can sometimes go after our critical infrastructure, including the state one. We indeed deal with intel, with intelligence services information. While the industry minister and the Department of Industry are not in charge of that, they will work with other departments, including the public safety agencies, Global Affairs Canada and Defence to make sure we can help them address the threats.

We have an entire policy infrastructure when it comes to national security, and we've been able to put guardrails regarding the way we address sensitive information, particularly when we're dealing with hybrid warfare and particularly when it comes to Ukraine. What we did was develop NSIRA and NSICOP. That's why.... I think that in the first part of the bill, years ago, when it was first presented, that wasn't there, and there was great work done by parliamentarians to make sure it would be there. Now, I think the parliamentary oversight has been added, and that's why I'm confident that we can deal with things in a way that is consistent with protecting the interests of Canadians.

Now, I hear you—

● (1625)

Rhonda Kirkland: Again, I only have limited time, Minister.

Hon. Mélanie Joly: —regarding the criteria of proportionality, because I think that's also something that we could really look at.

Rhonda Kirkland: Yes, exactly. We're past that for sure.

The Privacy Commissioner warned that the minimum privacy requirements in Bill C-8 are “insufficient” to govern “the sharing of information with foreign governments”, particularly where sensitive or personal data may be involved. Given those concerns, what specific limits does Bill C-8 place on the sharing of Canadians' information with foreign governments or entities?

I ask this with the backdrop that, during the election, the Prime Minister publicly stated that China is “the biggest security [threat] to Canada”. In March 2023, you accused China of “trying to sow division in many democracies.”

I lived in China for a couple of years. I've experienced what that can look like.

Does the government still stand by that assessment today? If so, how does Bill C-8 ensure that sensitive information collected under this legislation cannot be shared directly or indirectly with hostile states or bad actors?

Hon. Mélanie Joly: I think that we can't look at Bill C-8 in a silo. We have to look at it with all the other legislation that is linked to public safety and national security and all the agreements we have with states around the world. We only have agreements on intelligence with our allies. That's how the Government of Canada operates and protects Canada's interests in a very complicated geopolitical world.

Rhonda Kirkland: Sometimes it seems like we're talking out of both sides: One minute we're allies with China, and the next minute we're not, so excuse my question.

The Liberal government assured Canadians that invoking the Emergencies Act complied with the Canadian Charter of Rights and Freedoms. The courts have since ruled—twice—that the government violated the charter and failed to meet the legal threshold. Do you regret voting for and enacting the Emergencies Act?

The Chair: We have 10 seconds.

Rhonda Kirkland: Yes or no?

Hon. Mélanie Joly: I think this is a question that is before the courts—

Rhonda Kirkland: Do you regret it, yes or no?

The Chair: I'm sorry, but this is all the time we have.

[*Translation*]

Mr. Ramsay, you have the floor for five minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Thank you very much, Minister, for being here. I appreciate that.

Minister, industry representatives who appeared before this committee told us that they were concerned about having to make major investments as a result of the recommendations on telecommunications security. They suggested that an amendment be made to Bill C-8 that would allow for discretionary compensation. We know what discretionary compensation is worth: not much.

At this point, I would be satisfied to know that the Minister of Industry is perhaps open to the idea of such a possibility, because all kinds of programs are moving in that direction.

Is that something you could consider at some point if major investments were indeed necessary?

Hon. Mélanie Joly: I would say that most of the investment that will be needed in the circumstances will come from the telecom companies themselves. It's in their own self-interest to make these investments.

I think our role as a government is to explain what needs to be done to protect citizens. We will therefore be moving forward with Bill C-8. That's why we're introducing it.

At the same time, I think that, knowing this, companies have to make the necessary investments, because they can't compromise the security of their operations or the data of their customers or stakeholders they do business with.

I think we're in an increasingly digital world, where security can't be taken for granted. Under the circumstances, I expect the business community to do its job.

● (1630)

Jacques Ramsay: Basically, you're telling us that the cost of not investing could be higher than the cost of investing.

Hon. Mélanie Joly: I would use the English expression:

[*English*]

It's part of the cost of doing business.

[*Translation*]

Jacques Ramsay: You briefly mentioned harmonizing standards. We understand that, with the provinces and other international organizations, all kinds of standards will apply. We understand that they may not be necessary to include them in the legislation. I hope that one day these standards will be included in regulations.

At this point, I would once again be satisfied with your opinion on a statement that you are going to try to reduce red tape and unnecessary regulations in order to harmonize things with other provinces and internationally, as far as possible.

Hon. Mélanie Joly: It's a constant frustration. I see it. Ms. McMicking is aware of it. The team at the Department of Industry is aware of it. I think there's still far too much red tape, and we need to do even more to reduce it. It's a problem. Things need to move faster, because the American economic threat is real. Whether it's to protect the telecommunications sector or other economic sectors, including steel, aluminum and the entire automotive sector—in other words all sectors that can be subject to tariffs—our decisions need to be made more quickly.

Jacques Ramsay: You told us that all the other Five Eyes countries—New Zealand, the United Kingdom, Australia and the United States—already have similar legislation. I think that's reassuring. We can assume that Canada probably needs this kind of legislation as well.

I'm sure you've reviewed the legislation of these other countries. Are you convinced that Bill C-8 will achieve its objectives and that it may even be better because it has the benefit of being improved upon later?

Hon. Mélanie Joly: This bill is extremely necessary. We're behind, that's the reality. We introduced a protection policy in 2022 that was basically voluntary in nature. The government doesn't currently have the power to impose it more strictly on telecom companies with regard to telecommunications equipment within their networks that could jeopardize the security of Canadians' telecommunications networks. It makes no sense.

So I understand the debate. It's important. Honestly, we need to pass this bill quickly. That's what I think. The sense of urgency should be shared, in my opinion. I certainly feel it, and I hope all members around the table feel it too.

The Chair: Thank you, Minister.

We'll now go to your last intervention, Mrs. DeBellefeuille. You have the floor for two and a half minutes.

Claude DeBellefeuille: Minister, I want to return to the parliamentary secretary's request, namely, to hear you say that you will make every effort to avoid overlap between the provinces and territories, in accordance with and in line with the very high standards that exist.

We're talking about NERC, the North American Electric Reliability Corporation. I'd like to hear it, too. It would reassure me. What's in the regulatory part is one thing, but when an intention is expressed more formally in a bill, it's even more reassuring.

Hon. Mélanie Joly: I'll give you some real-life examples.

For example, when a huge cyber-incident affected the Newfoundland health care system and really affected the telecommunications system and data, the government could have worked even more closely with the telecom companies. We did so from a federal-provincial perspective to provide support and even transfer funds to help resolve the issue. We did the same for the Northwest Territories, because there were cybersecurity issues there as well.

When an incident affects the cybersecurity of a provincial government, its agencies or a company, the Department of Industry isn't the only one to respond. Several of us respond at the same time. This often involves security agencies and us. We work with the local government. So we adapt to the situation.

● (1635)

Claude DeBellefeuille: Minister, the bill refers to fines and penalties. Electricity Canada's concern is whether Hydro-Québec could be doubly penalized. There's some confusion, especially on the issue of fines.

In closing, let me say this. You said earlier that the major telecom companies have a responsibility to equip themselves to deal with cyber-threats. I think you know that in Quebec, there are small Internet providers, co-operatives, that often operate in rural areas that were of no interest to large providers such as Bell Canada, to name just one.

We're a little concerned. How will they be able to afford to meet the new requirements? Do you have any thoughts on these small suppliers?

Hon. Mélanie Joly: Yes, I do.

The Chair: There are about 15 seconds left, Minister.

Hon. Mélanie Joly: Thank you, Mr. Chair.

Absolutely, Mrs. DeBellefeuille.

With regard to matters relating to respect for jurisdictions, my goal is and always will be to respect federal and provincial jurisdictions.

The Chair: We've used up all the time allotted.

Thank you very much, Minister Joly, not only for preparing for your appearance, but also for being here today.

We will suspend the meeting for a few moments to give you time to leave, and so that the officials can get settled for the next part.

● (1635)

_____(Pause)_____

● (1645)

The Chair: I call the meeting back to order.

Before giving the floor to committee members, I would like to quickly introduce the people who are before us.

We have Mr. Arbour, director general, telecommunications and Internet policy branch; and Ms. Kwan, director general, spectrum and telecommunications sector. Both are from the Department of Industry.

We have quorum, so we'll start with Mr. Lloyd.

Mr. Lloyd, please go ahead for six minutes.

[*English*]

Dane Lloyd: Thank you.

It's good to have officials back here today.

Here is my first question. Can you confirm whether the government currently has the technical authority to force telecom providers to remove hardware—for example, Huawei hardware—from their telecommunications systems at this time?

Andre Arbour: No, it does not. The policy currently in place is a voluntary policy, and the policy further stipulates the government's intent to introduce legislation to implement it. That led to the tabling of Bill C-26 and now Bill C-8.

Dane Lloyd: That's confirming that Bill C-8 would give government the legislative authority it currently lacks to order telecoms to remove or to prevent the installation in the future of hardware that could threaten our telecommunications system.

Andre Arbour: Yes, that's correct. The legislation is just a framework. It is not specific to any one country. It's agnostic to the types of threats that threaten the underlying infrastructure. Yes, it would give the authority to manage supply chain risks, including high-risk vendor equipment.

Dane Lloyd: Do you understand and remember the context in which Bill C-26 was first brought in? Do you acknowledge that the context of that legislation was to give the government the legislative authority to remove Huawei specifically from the telecommunications system?

Andre Arbour: That was a substantial factor, but it was far from the only one.

Dane Lloyd: I agree. It wasn't the only factor.

Now, as far as you know, is it still the government's objective to order the removal of any remaining Huawei infrastructure from the telecommunications systems, if it does remain after this legislation is brought into force?

Andre Arbour: The 2022 policy still stands. There's been absolutely no change to that.

The tedious bureaucratic addition to that is that ultimately any legal removal via an order in council, via the Governor in Council, can only be considered after royal assent. Also, the provisions of the law in question require consultation, and the government has been consistent, including in its 2022 policy, that it will consult before finalizing any rules.

Dane Lloyd: Given the Prime Minister's recent trip to China and the reset of relationships, are you aware of any...? You said that there's currently no change from the 2022 policy. Are there any proposed changes in relation to China's hardware and our telecommunications systems coming out of the recent meetings in Beijing?

Andre Arbour: I am not aware of any changes to the government's 2022 policy. Also, any rules, should Bill C-8 receive royal assent, will be subject to consultation.

Dane Lloyd: Thank you for that.

In reference to the bill's previous iteration, the intelligence commissioner, whom we had at committee—and I think he was actually sitting beside you at the time—testified that he thinks there's a "glaring absentee" in this bill, and that is "the Canadian public". The information that is collected is Canadians' personal information.

He went on to say that in every case he's seen as the intelligence commissioner, a warrant is needed. You can obtain it from a justice of the peace, from the Federal Court or from a quasi-judicial officer. In the present bill, there doesn't seem to be a requirement for such a warrant. Why is that not in Bill C-8?

● (1650)

Andre Arbour: The scoping of Bill C-8—colloquially, but this is how it's actually drafted—is regarding the regulation of the underlying telecommunications systems. Therefore, information collected from the private sector can only be collected if it's relevant to protecting those systems. Someone's personal information is not germane to that activity.

Dane Lloyd: However, the intelligence commissioner said that, in every case he'd seen, personal information was included in all of the reports that crossed his desk.

Andre Arbour: If there has been a cyber-breach and information has been accessed, for instance, that may be one circumstance where personal information is involved. However, if I want to establish a rule that requires a regular installation of software patches and underlying network infrastructure, I don't need anyone's personal information, and it's not—

Dane Lloyd: You said that it's not germane, so are you saying that people's personal information would not be included in Bill C-8 and that there wouldn't be situations where people's personal information would be shared under Bill C-8?

Andre Arbour: We have not been able to think of a scenario where that would be necessary.

The powers in Bill C-8 are modelled on existing powers for non-security reasons in the Telecommunications Act and in the Radiocommunication Act. There are similar authorities in the Insurance Companies Act and in nuclear safety.

They are scoped by the fact that what is relevant is regulating the ongoing conduct of these network industries, and someone's personal information doesn't have bearing on that. The network infrastructure doesn't care about the content of the information. It's all zeros and ones, and—

Dane Lloyd: Concerning these threats to the cybersecurity system, maybe we're talking about natural disaster threats, but the threats that I think we're talking about have people behind those threats. Wouldn't there be context provided that so-and-so or such-and-such an entity that contains these people is planning to do something that could threaten the integrity of the telecommunications systems? Would that not be a scenario where personal information could be included?

The Chair: Could we have a very short answer, please? We may be able to come back to that.

Andre Arbour: The information can only be collected when it's relevant to an order-making authority. This is about the management of the underlying infrastructure. That is the circumstance already scoped by which that can be done, not for law enforcement or criminal investigations.

The Chair: Thank you.

MP Acan, you have six minutes, please.

Sima Acan: Thank you, Mr. Chair.

It has been repeatedly noted in this committee's studies that Canada is currently the only G7 country without mandatory cyber-incident reporting or legislation explicitly protecting critical infrastructure. Could you explain how Bill C-8 will address this gap, ensure that our vital systems are secure and align Canada's regulatory posture with Five Eyes partners like the U.S. or Australia, particularly with respect to the speed of response when threat actors are already prepositioned?

Andre Arbour: Part 1 of the bill concerns amendments to the Telecommunications Act. That is a long-standing piece of legislation. This would ensure that there is a new policy objective that gives explicit authority to regulate in advance of the security of the telecommunications system, along with associated authorities to issue rules to collect information and to ensure compliance.

This allows the government to take action to ensure that companies have the appropriate security and response plans in place so that they are preventing threats and responding to them, and installing vital systems to ensure that their networks are as reliable as practical under the circumstance. It also allows the government to collect information on the threats to that infrastructure as a mechanism of continuous improvement, to issue the new sets of rules, but they're limited to the management of the infrastructure itself.

Part 2, led by the Minister of Public Safety, has a set of baseline cybersecurity protections across federally regulated sectors, and that's to ensure a level of consistency, given the interdependent nature of cybersecurity threats that affect different aspects of critical infrastructure.

● (1655)

Sima Acan: Thank you very much.

I'll get into the national security portion and the economic threats to our industries in a little bit more depth.

We've heard concerns about the financial burden of rip and replace orders for high-risk equipment; however, Public Safety Canada has indicated that a single data breach costs Canadian business—as the minister confirmed—nearly $7 million on average, with the total economic impact of cyber-incidents reaching $5 billion annually.

In your view, how does Bill C-8 provide a necessary framework for long-term economic stability and for preventing the catastrophic loss of productivity and reputational damage associated with a critical infrastructure failure? Could you please also explain the implications for the industry and how this would also damage our economy and our national security?

Andre Arbour: Certainly, the damage from cyber-incidents is substantial, as the minister outlined, and dwarfs the extent of costs in terms of protection up front. It's a cliché, but an ounce of protection is worth a pound of cure. It's much better to have protections built in as part of your ongoing business activities, so when you buy that next generation of equipment—we're on 5G now, but 6G is going to be the next thing—you have security principles built into your procurement and planning up front.

Certainly, when we contemplate rules under our current authorities—for example, for spectrum management planning, when we are thinking about spectrum auctions and that type of thing—we design the rules with the life-cycle considerations for industry, to minimize the impact on that industry so that they can build that planning into their normal procurement cycles.

Sima Acan: Thank you very much.

You mentioned 5G and 6G technologies. Experts have also noted that the legacy mobile networks were often insecure by design. As we transition to 5G and 6G infrastructure, which rely heavily on software-defined networking, the attack surface for state-aligned actors increases. Can you elaborate on how the new order-making powers will allow the government to proactively mandate vulnerability assessments and secure-by-design principles, rather than relying on the private sector to bolt on security after the breach has already occurred?

Andre Arbour: The department has an ongoing dialogue with industry, but it's purely on a voluntary basis at this time in terms of trying to socialize and encourage best practices.

I think the authorities enabled by Bill C-8, first, would allow for clearer information on the nature of those threats, to allow for prioritization of actions. It also moves beyond the purely voluntary toward being able to establish rules in terms of the procurement of the equipment or services that are going into the network.

With cybersecurity and response plans, the first objective is to prevent an incident, but the reality is that you're going to have one. That's unavoidable. You're going to have a hurricane or you're going to have a cyber-attack. Those exist. A core aspect of resilience is having a response mechanism so that when there is an incident, you can address it, manage it and secure the network as quickly as possible after the fact.

[*Translation*]

The Chair: Thank you very much, Ms. Acan.

Mrs. DeBellefeuille, you have the floor for six minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

I would like to come back to the issue of harmonizing the reliability standards of the North American Electric Reliability Corporation, or NERC. I'm thinking a lot about the fact that Electricity Canada really insisted that Bill C-8 include a provision that a member who meets NERC standards complies with Bill C-8. That would be much simpler than proceeding through regulations and negotiations, because I think that this North American reliability standard is very high. It is widely used, and disclosure practices have been developed. It's as if Bill C-8 were playing around with these very reliable players.

Mr. Arbour, would it be complicated to add a provision stipulating that compliance with the NERC standards, the international standards, is sufficient to satisfy Bill C-8?

● (1700)

Andre Arbour: Thank you for your question.

Questions about the regulation of the electricity system fall under the jurisdiction of the Department of Natural Resources, rather than the jurisdiction of the telecommunications sector. However, I know that they are already in the habit of taking harmonization issues into consideration to avoid a conflict or overlap in the rules of the electricity system.

Claude DeBellefeuille: Therefore, it wouldn't be inconsistent—it might even be appropriate—to include a provision in Bill C-8 that would send a strong signal of intent to recognize those who meet these very high reliability standards. This is a major concern for Electricity Canada, of which Hydro-Québec is a member. However, I wanted to let you know that this is something that concerns them greatly.

The provinces often have dealings with the federal government. They aren't always harmonious, they are lengthy, and the provinces are concerned. I thought that perhaps an amendment should be proposed to make that very clear. The minister's goal is to provide robust protection. If they already have it, why not recognize it? That's what I'm wondering.

My other question concerns the retention of personal information.

Witnesses told us that the bill didn't really provide any framework for the collection of personal information, how it is stored, how long it is kept and so on.

Do you think those concerns are justified? Should the bill be improved to provide a better framework for the retention of personal information?

Andre Arbour: I thank the member for her question.

With respect to part 1 of Bill C-8 and the Telecommunications Act, I would first like to say that personal information is outside the scope of our activities when it comes to regulating telecommunications networks.

Personally, I don't see a problem with the management of that information. The information that is important to us is the type of equipment, the tower's location, the battery system and the backup system in the context of a network outage. In addition, personal information is not relevant to those activities.

Claude DeBellefeuille: Mr. Arbour, I'm surprised you're telling me that. I don't want to question what you're saying, quite the opposite. However, many witnesses have told us about the risk, the breach of personal information, the poor governance, among other things. It seems as though those witnesses did not understand Bill C-8. When I listen to you, I get the impression that the witnesses did not understand the bill. They talked a lot about privacy. That's what surprises me about your answer, when you tell us that privacy is excluded. The witnesses we heard from are experts, after all, and they did express their fears about this to us.

Andre Arbour: I thank the member for her question.

Part 2 brings up some concerns about the possibility of some personal information being accidentally transmitted when incidents are reported. That situation currently exists in the case of voluntary reports. So there are systems for managing that type of situation, under the Privacy Act and Communications Security Establishment Canada's system. That system currently exists, and having mandatory reporting in part 2 would not change that system or the existing controls.

● (1705)

Claude DeBellefeuille: Okay.

Do I have any time left, Mr. Chair?

The Chair: Unfortunately, your time is up already, Mrs. DeBellefeuille. We'll come back to you a little later.

I will now give the floor to you, Mr. Caputo, for five minutes.

Frank Caputo: Thank you, Mr. Chair.

[*English*]

Monsieur Arbour, I want to pick up on something that was mentioned. I believe it was one of my Liberal colleagues who asked the minister whether a warrant is commonplace in any other of our Five Eyes jurisdictions. You commented that a warrant is typically used in criminal law based on evidence that has been gathered by the police.

I want to reorient, though, how we're looking at this. A warrant is a type of judicial authorization, and a judicial authorization permits the government or the state, if you will, to take certain action. Where somebody has an expectation of privacy, that's where you get a warrant in criminal law, for instance.

Bearing that in mind, that judicial authorization or whatever you want to call it, some sort of judicial order.... Would this legislation be precluded by...? I'm not talking about exigency, in terms of exigent circumstances, but where there is a threat and the government is going to act under section 15, could this legislation not be amended to give the Federal Court the ability to give some sort of judicial authorization—based on oath or affirmation, which is how an authorization works—so that it's not the minister making the call, but it's the court making the call?

Am I being clear on this?

Andre Arbour: Certainly, what the committee chooses to do with amendments is the committee's prerogative. I think there are two considerations that I would flag just to provide information to the committee. The first one has to do with a more substantive set of considerations, and the second is more procedural.

In terms of a substantive basis—and I speak on this having been involved in the regulation of the telecommunications system, infrastructure, providers, for quite some time—the activities that go into that regulatory activity are very different from those that courts contemplate. It is quite rare, in a regulatory context, to have a non-expert court having oversight in that context. In terms of establishing rules for how.... These have the force of law. These are not something that can be done just willy-nilly; they have to be done with due care.

Frank Caputo: Can I stop you there, please?

The point I'm trying to make is this. If the government is going to take action, what does the government have to say? There is a threat, and this is a threat.... Right now it says “any threat”, and it compels any actor to potentially take any action.

I don't know that you need expertise. With all due respect, I'm sure the minister isn't an expert on all of these areas. They rely on the bureaucracy to advise. In that case, could you not have something procedurally that says that a government official must, on oath or affirmation, detail the nature of the threat and detail the action to be taken and how it fits within the act? Could a Federal Court judge not look at that and say, yes, you have met the requirements of the legislation, without being an expert, because it's clearly laid out in legislation what that is. The person is swearing it's true, in fact.

Andre Arbour: There are additional criteria as drafted: for example, that an order taken must be reasonable in relation to the gravity of the threat, and those types of things.

Frank Caputo: Of course. I oversimplified. I know that, yes.

Andre Arbour: Just to be clear, this would still be quite a new activity for any court trying to consider this.

● (1710)

Frank Caputo: I acknowledge that.

Andre Arbour: I'll maybe just add that I've seen that when some of these questions come up that are completely new and unrelated to any type of established process, it's quite a lengthy and involved set of considerations.

The second aspect, from a procedural standpoint—and this would be ultimately a question for the chair, should an amendment come forward—is that there may be questions about scope and whether a royal recommendation would be needed. Under Bill C-26, it was quite a different subject matter. An amendment from the NDP member that had to do with the provision of special counsel was—

The Chair: I'm sorry, but I will have to interrupt abruptly and rudely, because we now need to turn to MP Powlowski for five minutes.

Marcus Powlowski: This law protects critical infrastructure, power grids, nuclear reactors, transportation systems, pipelines, finance. We have concerns about cyber-attacks from China. We've heard about Huawei. Obviously, Russia is of concern. We are part of the Five Eyes.

How much is this act, and cybersecurity, blind to the country of origin of a cyber-attack? Could one of the members of the Five Eyes attack Canada, and would this legislation also guard us from that possibility?

Andre Arbour: The bill is country- and threat-agnostic in terms of the source. Cyber-attacks can come from many different places, including from organized crime, that are not affiliated with a government entity. Ransomware is an increasing tendency that we are seeing, enabled by cryptocurrency, which makes it much more profitable to engage in those types of attacks, and we see organized crime involved in those activities.

Marcus Powlowski: We're part of the Five Eyes. Is our cybersecurity so integrated with those other countries that we couldn't detect an attack from those countries? I would think that, given we're Five Eyes, we're all interconnected in cybersecurity. I mean from one of those countries, not a bad actor in those countries—let's say one of the governments in these countries decided they may want to attack some part of our economy.

Andre Arbour: I would start by saying, because I don't want to overstate the capabilities of my colleagues at CSE.... First and foremost, in terms of my mandate, it's related to the Telecommunications Act and working with my colleagues on securing, with the private sector, their underlying infrastructure. However, I do know that CSE, as part of its ongoing activities unrelated to this bill, has very impressive capabilities of identifying possible threats. Then, one benefit of the bill before us is the incident reporting, which allows for better visibility of what threats are interfacing with different vulnerabilities.

Marcus Powlowski: Okay. Well, here's a very broad question: What are you hearing from the business community? Is this something that protects and furthers their economic interests, or is it something that undermines their economic interests?

Andre Arbour: I speak to my colleagues in different telecommunications companies on a regular basis. Any time any government says, “I have some new regulatory obligations for you”, they don't necessarily jump up and down and say, “Oh, great! That's amazing!” There is some understandable caution: “Let's not go overboard here. Let's make sure that what you have in mind is realistic and practical.” That's perfectly understandable. At the same time, they recognize that this is absolutely necessary. These types of things are inescapable in any type of modern economy, as they've seen in our peer nations.

They also recognize that there are some real advantages to predictability. When something is just voluntary and just a suggestion, it can add a degree of vagueness that makes it harder to justify decisions to their corporate board, and they're in a bit of a grey area, whereas if something is clear in terms of regulation, then they know what their responsibilities are, and they know what they have to do.

● (1715)

[*Translation*]

The Chair: Thank you very much, Mr. Powlowski.

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

With the minister, we touched on the issue of companies being responsible for building infrastructure that is robust enough to withstand cyber-attacks. Those are big players, and we started talking about smaller players, such as co-operatives and Internet providers. In my area, we have Coop CSUR and TARGO. Those are small companies that serve rural regions abandoned by the major providers.

Have you estimated the costs that small Internet providers will have to bear to comply with Bill C-8, if it is passed? That concerns me a lot, as a lot of small Internet providers have set up shop in Quebec.

Have you estimated those costs?

Andre Arbour: Right now, the bill is a mechanism to implement the rules. In part 1, there is no specific obligation, but rather powers related to the implementation of the rules.

At ISED, Innovation, Science and Economic Development Canada, we're quite used to working with small players and with many obligations around the issue of spectrum management, for instance. Given the level of consultation, we are able to strike a balance among certain obligations.

Claude DeBellefeuille: Will that be done in the regulatory part?

Andre Arbour: Yes. In this kind of context, it's really about the fine details. The obligation is relative to the size of the participant in question. For smaller companies, the rules are less detailed or they don't exist, as they're not very important for a small provider with hundreds of customers. In that context, the obligations are simpler and they correspond to the capacity of a small provider without a government relations office.

Claude DeBellefeuille: I'm quite curious. The intelligence commissioner approves or doesn't approve national security and intelligence activities planned by the Communications Security Establishment Canada and the Canadian Security Intelligence Service, which are authorized by their ministers. How would Bill C-8 become more complex if an independent body approved an intervention or not?

The minister said that it was a matter of responding quickly. After all, it was the intelligence commissioner who recommended to add an independent resource.

Andre Arbour: In the context of part 1 and telecommunications issues, the Communications Security Establishment Canada, or CSE, does not play a role in the implementation of those powers. It's a matter of the private sector's obligations in the management of its infrastructure.

● (1720)

The Chair: Unfortunately, I have to interrupt you, as we are well over time.

Ms. Kirkland, the floor is yours for five minutes.

[*English*]

Rhonda Kirkland: Thank you, Chair.

I appreciate that you're here now. I have some questions that may be repeating slightly questions that I asked the minister, so we can hear the department's perspective on that.

On October 30, we heard a lot of testimony from different departments, including the Centre for International Governance Innovation, raising concerns about proposed sections 15.1 and 15.2, which give the Governor in Council and the minister broad authority, quite broad, to impose secrecy around certain orders and decrees. They recommended that clear guidelines be included to govern the use of these extraordinary non-disclosure powers.

From your perspective, can you give any insight into why the government chose not to include guiding criteria? Is there a reason for not including guiding criteria in terms of safety? Shouldn't we limit when and how the secrecy powers can be used?

I'd be interested in your perspective.

Andre Arbour: I'll start with just underscoring the minister's response that, absolutely, there is openness to consider amendments, including along the lines of the CIGI recommendation for criteria there.

In terms of the history of how we got to where we are today, with the existing provisions, first of all, it's not practical to have confidential orders on telecom operators, of which there are hundreds, as a matter of course. There's already a fair bit of.... We have no choice but to work in open consultation with many partners, so it's open by default.

Then, protections were added in the context of Bill C-26 to add some guardrails on the use of these authorities. The first was a requirement that if a confidential order is being made, there is a notification to NSIRA and NSICOP, so they can validate that the power is being used appropriately. Second, there are more detailed requirements in terms of an annual report to Parliament. We are required to report on our activities, including on the making of confidential orders. We can't get into the level of detail of what was in the order, but we have to describe at a high level what was done and why.

Rhonda Kirkland: In that same meeting, the Privacy Commissioner acknowledged improvements. I mean, there are some marked improvements in Bill C-8 with respect to its predecessor, Bill C-26.

Several ongoing privacy concerns, though, include lower thresholds for the exercise of certain powers that may have privacy implications, and a lack of mechanisms to ensure that the Office of the Privacy Commissioner is informed of material cybersecurity breaches that have an impact.

Do you have any insight into why the bill does not provide a formal mechanism to notify the Office of the Privacy Commissioner when a cyber-incident involves protected information?

Andre Arbour: I'll start with part 1 and then speak briefly on part 2.

In terms of the authorities around the information collection, I know there was some question about what explains the different wording in proposed section 15.4 versus proposed sections 15.1 and 15.2.

First, the information collection authority is already within the scope of.... It can only be exercised pursuant to proposed sections 15.1 and 15.2. You can only engage in an order-making activity if it's reasonably necessary to do so. We can only collect information if it's related to an order-making authority.

Rhonda Kirkland: Correct me if I'm wrong, but that's not checked until after the fact.

Andre Arbour: Those are the criteria that are in the bill already, in terms of scoping our ability to use the authority up front. It's an *ex ante* consideration. There are other protections around the use of that authority. For instance, the reasonableness criterion is an established threshold that's used in law, and proportionality is an aspect of reasonableness there.

To your question about CSE notification, this gets more into part 2 for my colleagues from Public Safety. It's not obvious to CSE when a privacy breach has happened, when they receive an incident report. They get an incident report that includes some technical information. Whether there are privacy implications.... There are already reporting requirements, though, under PIPEDA, so the private sector still has to report to the Privacy Commissioner under PIPEDA.

● (1725)

The Chair: Thank you very much for that.

[*Translation*]

Mr. Lavoie, go ahead for five minutes.

Steeve Lavoie: Thank you, Mr. Chair.

I thank the witnesses for being here today. I'm very happy to see them.

I'll ask you a secondary question first.

My colleague talked about small players in communications. We often talk about the big players, such as Bell, Telus and so on.

What does a “small provider” mean to you in terms of size? Where does it begin and end?

Andre Arbour: I thank the member for his question.

There is a very wide variety of types of players. There's a small provider in northern Manitoba whose business is truly family-owned, with a few hundred customers. There are medium-sized companies that have a few hundred thousand customers or a million customers, such as Cogeco and Xplore.

Steeve Lavoie: At what point is a provider no longer considered a small provider, but a larger one? Is it based on the number of customers?

Andre Arbour: There are no specific criteria in this context. It depends on the context and the aspect of the market in question.

In terms of developing the rules, in each context, consultations are held to determine where size is most relevant and how the impacts on the private sector can be managed. In some contexts, the rule is simple and necessary, and application is universal. In some other contexts, it's not worth it, or you have to consider the impact on the small players in question. So the context of the activities should be taken into consideration.

Steeve Lavoie: Okay.

As far as I understand, there are still rules to be established. It's not just a matter of size; it's also a matter of geography, and so on.

What I'm also interested in is the impact on smaller businesses. We often talk about the bigger players. We're talking about telecommunications, but there are also private companies. In fact, in Quebec alone, 72% of businesses have 10 or fewer employees.

Still in the interest of efficiency, I want to understand what the immediate impact will be for small private businesses. They often don't have the resources that large companies have to comply with regulations. That's when the situation becomes problematic. You talked about “powers” versus “obligations”. I would also like to hear what you have to say about that later on.

How will the government apply this new legislation, while thinking about small businesses, most of which are SMEs and don't really have the same staff, the same financial means, and so on?

Will they receive support? Will there be direct and indirect costs?

I'd like to hear more from you about SMEs, which basically make up the vast majority of our businesses in Quebec and Canada.

Andre Arbour: Thank you for your question.

The government has an interest in supporting small businesses because they are a source of competition for the big players. A number of mechanisms exist to support them.

Application of the rules must be taken into account. Some of those rules only apply to larger players. Basically, there's an exemption. There are mechanisms related to support resources, including discussions with us to explain the application of the rules. Some measures, such as information requirements, may be simpler to apply to a provider with a small number of customers than to Bell or Telus.

● (1730)

Steeve Lavoie: Thank you.

The Chair: Thank you very much, Mr. Lavoie.

[*English*]

Next is MP Gill for five minutes.

That will be the last intervention.

Sukhman Gill (Abbotsford—South Langley, CPC): Thank you very much for being here today.

I wanted to start off by saying thank you. Then I will be asking a couple of questions that might be a repeat from before, but these are concerns that my community members and I have, and I want to make sure I get the best response I can. I would appreciate it if you could answer to the best of your ability, please.

First, can the officials please tell us whether the department has assessed the extent to which major providers or contractors are outsourcing network-related telecom outside of Canada? What analysis has been conducted on the economic and employment impacts of this outsourcing, as well as its implications for the overall security objectives of Bill C-8?

Andre Arbour: I'll start, and then my colleague Wen may supplement.

First, in terms of telecommunications equipment and services, that is a global market. When we're talking about the equipment that's used in their network and supporting services, there's a relatively small number of global players. They may have substantial investments in R and D within Canada, but if we're talking about Ericsson or Samsung or Nokia or those types of places, we are dealing with a global supply chain with global standards. We operate in a global market rather than having a purely Canadian context.

In terms of our ongoing engagement with carriers within CSTAC, we have posed questions along these lines to better understand their operations. In terms of their operations, they are dealing with best-in-the-world companies that are providing mission-critical services to large Canadian companies but also, say, AT&T, Orange in France or that type of thing. They are providing best-in-class services to support that.

Wen Kwan (Director General, Spectrum and Telecommunications Sector, Department of Industry): Thank you for the question.

I would add that in the context of maintaining a telecom network, it is in the context of global equipment manufacturers. There are efficiencies to be gained. I'm not suggesting that this is the reason jobs are being offshored, but that's a consideration for the telecom companies to decide. What we are interested in is the security of the infrastructure.

As some members mentioned earlier, if there are already standards they are following, and they're strong, we do not have any objection, because the objectives of the Telecommunications Act are being met. We leave that decision to them. What we're interested in is the collaboration of the telecom service providers with intel agencies and security agencies, to ensure that we have the best protection and reliability of the network in Canada.

Andre Arbour: I apologize. I would add one last thing. Should a risk be identified in this type of context, Bill C-8 would give the authority to remedy that risk, but there would need to be a clear risk and we would need to be taking action that's reasonable in relation to that risk.

Sukhman Gill: I want to highlight the importance of this question.

When telecom operations or data are handled outside Canada, they are subject to foreign laws and governments. How does the department see this affecting privacy, data protection and national security risks, especially given the objectives that you guys are bringing forward with Bill C-8?

Andre Arbour: Bill C-8 is concerned with the management of telecommunications networks and services and allows for action to manage those instances.

In terms of the handling of personal information, there's a set of existing requirements under PIPEDA, but I also know Minister Solomon has plans to improve those, and there will be more to come in due course on privacy reform.

● (1735)

Sukhman Gill: Okay.

Right now, the Telecommunications Act and policy direction to CRTC prioritize competition, affordability and innovation. Employment in Canada, data sovereignty and system-wide network security aren't explicit objectives. Does the department see a gap, particularly in Bill C-8, in trying to improve these telecom securities?

Andre Arbour: Certainly the government's 2023 policy direction does not get into questions of security, in part because it was made pursuant to the Telecommunications Act, and those considerations did not exist in the Telecommunications Act at that time. However, that is part of the raison d'être of adding the protection of the Canadian telecom system to the policy objectives of proposed section 7 in Bill C-8 and establishing a legal framework by which the government can actually take legal action to protect telecommunications infrastructure.

Sukhman Gill: Okay.

Has the department—

The Chair: Thank you.

I'm sorry, Mr. Gill. Again, I'm being rude because that's all the time we have for this intervention.

Let me thank both of you, Mr. Arbour and Mr. Kwan, for your presence today and for the hard work.

Let me also take advantage, which perhaps I'm not supposed to do from a procedural perspective, and signal that behind you there is a lady, Shawna Khamis, who is a student in law at the University of Ottawa, who is working with the analysts and one day might be sitting on this side of the room. Who knows?

Thank you, Ms. Khamis, for your early interest in law and politics.

Mr. Ramsay.

[*Translation*]

Jacques Ramsay: Mr. Chair, I just want to let you know you that there may have been discussions among the parties, either at the Standing Committee on Finance or with the leaders. I hope to get unanimous consent from the committee to adopt the following motion, in relation to Bill C-15:

> That, pursuant to Standing Order 108(2), the committee undertake a study of the subject matter of Bill C-15, specifically clause 371 (Division 19), and clauses 380 to 385 (Division 21); that it invite the Minister of Public Safety for one hour, followed by the National Police Federation for one hour to appear by Friday, February 13, 2026; and, that it forward any recommendations or suggested amendments to the Standing Committee on Finance by Thursday, February 26, 2026.

The Chair: Thank you, Mr. Ramsay. As you know, we need unanimous consent to be able to discuss this motion.

Is there unanimous consent?

Some hon. members: Agreed.

The Chair: Mrs. DeBellefeuille, the floor is yours.

Claude DeBellefeuille: Can we be assured that the clerk will forward what we decide to the Standing Committee on Finance before February 4?

The Chair: Yes. We'll look into that. If the motion is adopted, we will indeed have to make sure that the decision is sent.

Is there any further discussion on this motion? Seeing none, I guess it's adopted.

(Motion agreed to)

The Chair: I will take a few seconds to quickly talk about what's coming.

On January 29, we will not be sitting, as the House schedule has been changed. On February 3, February 5 and February 10, we will be doing a clause-by-clause study on Bill C-8. On February 12, we will most likely follow up on the motion that was just adopted. February 17 and February 19 will be constituency days.

With that, thank you.

Claude DeBellefeuille: Mr. Chair, I'd like to say something quickly.

Could you ask the clerk to get in-person interpretation for the clause-by-clause study? That would really help me keep up with the pace of the debate on the amendments.

The Chair: You're asking with a lot of sincerity and a big smile. I think the clerk will be charmed by your request and will follow up.

Thank you and have a good evening.

(The committee adjourned)