



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 022

Thursday, February 5, 2026

Chair: Jean-Yves Duclos



Standing Committee on Public Safety and National Security

Thursday, February 5, 2026

• (1530)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): Good afternoon, everyone. We'll start the work.

I officially call this meeting to order.

Welcome to meeting number 22 of the House of Commons Standing Committee on Public Safety and National Security. Pursuant to the House order of October 3, 2025, we're meeting on our study of Bill C-8, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts.

I would now like to welcome the witnesses, whom we are getting to know well and who will answer questions, if needed.

From the Department of Public Safety and Emergency Preparedness, we have: Colin MacSween, director general, national cyber security directorate; and Kelly-Anne Gibson, director, national security directorate.

From the Department of Industry, we have: Andre Arbour, director general, telecommunications and Internet policy branch; and Wen Kwan, director general, spectrum and telecommunications sector.

Other senior officials are seated in the room and can potentially move to the table if their presence is deemed necessary to answer questions.

We will now resume the clause-by-clause consideration of the bill. We're at amendment BQ-1, which has been put on notice.

Is amendment BQ-1 moved, Mrs. DeBellefeuille?

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Yes, I will move the amendment.

In my view, it essentially echoes the Privacy Commissioner's recommendation that the bill should be standardized based on the criteria of reasonableness, proportionality and necessity.

Therefore, this amendment clarifies the criteria and factors the minister or the Governor in Council will use to gather the information they need.

The Chair: Very good.

I will note that, if amendment BQ-1 is adopted, amendment CPC-10 cannot be moved owing to a line conflict. Notice was given on amendment CPC-10; therefore, it shows up a little later in the order of the amendments.

Mr. Caputo, the floor is yours.

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

Thank you, Mrs. DeBellefeuille.

[*English*]

I'm in favour of anything that limits the sweeping powers that are granted here. Let us not forget that Bill C-8 would grant unprecedented, substantial powers. While we perhaps lag behind our G7 counterparts, that doesn't mean any legislation we pass should be passed without scrutiny and without judicious forethought as to the powers we are granting, when we are talking about potentially removing people from the Internet for any sort of threat.

I know we've had a lot of discussions about any threat, but in this case, my understanding is that we will be curtailing power and adding an element of proportionality. In other words, Conservatives believe, and I hope this table will believe, that we should not be using a sledgehammer to kill a fly. Any government intervention must be proportional to the threat, and it is for that reason that I support BQ-1.

• (1535)

[*Translation*]

The Chair: Thank you, honourable member.

Is there any further debate?

Mr. Ramsay, go ahead.

Jacques Ramsay (La Prairie—Atateken, Lib.): Right now, our reading of the bill is that the Governor in Council and the minister can only make orders when necessary to protect the communications system.

Those orders must be reasonable given the seriousness of the threat. For us, the amendment simply confirms what our understanding of the bill was already. In that sense, if the goal is more clarity for everyone, we agree on the amendment.

The Chair: Thank you, Mr. Ramsay.

Is there any further debate?

Seeing none, we can go to a vote. As usual, I will ask the clerk to take a recorded vote on the amendment.

[*English*]

Dane Lloyd (Parkland, CPC): I have a point of order.

[Translation]

The Chair: Mr. Lloyd, the floor is yours.

[English]

Dane Lloyd: Would it be quicker if we just said “on division” or something like that—not that I’m against it—instead of going through the roll call?

The Chair: I can do that, but I prefer to be prudent, given that it’s not always possible to know the exact point of view of everyone just by looking at faces.

I always see the faces, but they don’t always indicate exactly how they would vote. I can do that on this amendment.

(Amendment agreed to on division [See Minutes of Proceedings])

The Chair: That brings us to CPC-4.

Is CPC-4 being moved?

Mr. Caputo.

[Translation]

Frank Caputo: Thank you, Mr. Chair.

I move amendment CPC-4.

[English]

I will speak to this amendment briefly, talking about whether a “specified person” refers to a telecommunications provider or to a person.

One of my greatest critiques of the bill as initially drafted was the nature of the vague language. I think all the lawyers here—or anybody here—would know that vague language leads to bad results. In fact, if you want to know why a lot of laws get struck down under the charter, it is vagueness.

Precision in language is always appreciated, which is why I support and am the primary mover of CPC-4.

[Translation]

The Chair: Thank you, Mr. Caputo.

Is there any further debate?

Ms. Acan, the floor is yours.

[English]

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

My understanding is that this requested change would create a massive security loophole. This amendment seeks to narrow the scope of security orders so that they only apply to telecommunications service providers or the persons directly responsible for the security of services.

This is described as having a dramatic and detrimental impact on national security. Specifically, it would technically prevent the government from using Bill C-8 to enforce the 2022 policy statement, which allows for the prohibition of equipment and services from high-risk providers such as Huawei in Canadian networks.

I would like to ask the experts’ opinion. Given that modern cyber-threats often exploit vulnerabilities within the global supply chain, could you please explain to us the technical risk to Canada’s national security if this amendment prevents the government from issuing orders against third party, high-risk vendors that are not telecommunications service providers? Would this not effectively strip the government of its power to enforce the 2022 policy statement regarding the ban of equipment and services from providers such as Huawei?

Andre Arbour (Director General, Telecommunications and Internet Policy Branch, Department of Industry): I’d start by saying that the scope of the section is already on a telecommunications service provider. It gives the government the ability to tell a telecommunications service provider what it can use in its network. The obligation is on the telecommunications service provider itself as to whether it can buy certain types of equipment or procure certain types of services.

The type of corporate entity that a TSP will buy goods and services from is much broader than just other telecommunications service providers. It’s equipment manufacturers. It’s software producers. It’s battery manufacturers, etc. There are a large number of those.

Basically, it’s already scoped to say that there may be obligations on Bell Canada, or whoever, in terms of what they can procure or put in their network. The reason it’s a “person” is that Bell Canada may procure goods and services from a wide variety of vendors.

If you limit the scope of that power to only taking action against buying from other telecom service providers or other people responsible for telecom services, you can’t prevent them from procuring from equipment vendors that are high-risk.

• (1540)

[Translation]

The Chair: Thank you, Ms. Acan.

Is there any further debate?

Mr. Caputo, the floor is yours.

[English]

Frank Caputo: Thank you, Mr. Arbour.

The concern generally when we talk about overbreadth relates to, for example, an individual citizen being targeted. In this case, is it your view or expertise that in some cases, individual people need to be targeted because they are high-risk vendors, or are we generally talking about a corporate vendor and that’s what we’re talking about as “person”?

I hope that makes sense.

Andre Arbour: “Person” in the Telecommunications Act is a common term used. It is not the same as “person” in a colloquial sense. Here we’re talking about corporate entities.

Random individuals do not sell goods and services to telecommunications service providers, so there’s no impact on individuals via this clause. “Person” is referring to the legal concept of a person, which includes corporate entities.

Frank Caputo: I suppose the legal concept of personhood does, and I’m aware of that, but the legal concept of personhood could extend to, say, a partnership or someone in a partnership that is just individuals. I guess that’s where I’m caught up here. It’s that the legal concept of personhood extends to corporations and to people.

How are we excluding individuals but including only corporate entities?

Andre Arbour: First of all, in the scope of the provision, the burden is only on telecommunications service providers. It is saying that telecommunications service providers may have restrictions on the entities they can contract with. If my brother-in-law had a business providing telecom services globally, he is not touched by this at all. The legal obligation would be on Bell, Telus or Rogers in terms of what they can put in their network.

The Chair: Thank you.

Are there any other questions or interventions?

Go ahead, Ms. Kirkland.

Rhonda Kirkland (Oshawa, CPC): Just to clarify, I have a question based on both of the questions asked by my colleagues.

I’m trying to understand how there’s a security loophole and to simply clarify who is referred to by “specified person”. I understand that “person” in this context doesn’t mean an individual person. However, could it in any way mean this, and what’s the harm in clarifying that it’s not that?

Andre Arbour: Again, the legal obligation is already on telecommunications service providers. The legal obligation would be on their ability to contract and procure, and “telecommunications service provider” is already much narrower than “person”.

The question is, who can they contract with? If you substitute “person” for “telecommunications service provider”, you can only restrict their ability to contract with other telecom service providers, but that’s not the issue. The issue is that they’re contracting with their supply chain, so that’s why it’s TSPs contracting with “persons”.

When we’re talking about something as technical and complex as the goods and services that Bell uses to run its network, there’s not an issue of individual rights. We’re talking about contracting between corporations.

• (1545)

Rhonda Kirkland: I understand that. Is it a security loophole? Is it dangerous to clarify it? That’s what I’m asking.

Andre Arbour: This isn’t, with all due respect, a clarification. This would reverse the whole legal construct of this provision. The whole *raison d’être* is to be able to.... If we’re talking about high-risk vendor equipment, it is provided by an equipment manufactur-

er, not a telecom service provider and not someone responsible for the security of a telecom service. They’re not involved, or they may not be involved, in the day-to-day management of telecom service. If you swap that language, you completely remove the ability for the government to set parameters on contracting for supply chains.

[Translation]

The Chair: Thank you.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Mr. Chair, I’d like to thank Mr. Arbour for those details. It’s not easy for us to understand legal language. So I very much appreciate his clarifications.

I would also like to thank the interpreters behind me, who interpret brilliantly and who really help me follow the discussions and explanations in real time.

I would like to reiterate to everyone that having interpreters on site really improves things when we have debates where the language is very legal. I greatly appreciate the work the clerk has done to get the interpreter, as that enables me to feel like a full participant.

The Chair: Mrs. DeBellefeuille, all those words are well received and welcome. Do you want to continue?

Claude DeBellefeuille: No. I didn’t want to discuss the amendment. I had some reservations, but with the explanations Mr. Arbour provided, I will be voting against the amendment.

The Chair: Okay.

Mr. Caputo, the floor is yours.

[English]

Frank Caputo: Thank you.

As I understand it—and I want to be sure—Mr. Arbour, you have spoken about proposed section 15.1, but our amendment also addresses proposed section 15.2, which says:

(b) direct a telecommunications service provider to suspend providing for a specified period any service to any specified person, including a telecommunications service provider.

There, we actually have a distinction, again going back to the basic principles of statutory interpretation. The words speak for themselves. If we're talking about corporate entities, that would be the telecommunications provider, would it not? Why are we delineating between "person" and "telecommunications provider" in proposed paragraph 15.2(1)(b)?

Andre Arbour: When it comes to the considerations of individuals for the disconnection power in proposed section 15.2, there are other ways to manage that. There is one CPC amendment, for instance, to exempt the consideration of individuals from that construct. It would do that in a way that is actually targeted towards what I'm hearing is the concern.

If CPC-4 is adopted, it would eliminate the government's ability to put restrictions on high-risk offenders.

Frank Caputo: Okay, that's fair enough. I understand that.

What if CPC-4 was adopted, but only insofar as paragraph (d) is concerned? Would that still pose the same risk that you mentioned?

Andre Arbour: Yes, because telecom service providers can be interconnected with servers, data centres or other corporations that can pose a dramatic risk to the telecom system. They are not themselves telecommunications service providers. If the concern with that further section is the application to individuals, there are much more targeted ways to address that concern, in my opinion.

• (1550)

Frank Caputo: As my last question, could this be used to target an individual?

Andre Arbour: I don't believe so. Individuals are not involved in the provision of any material goods and services into a supply chain. That is the business of corporations.

Frank Caputo: I'm not going to ask any questions, but that's where I think we disagree. I think proprietors come in all shapes and sizes—some big, some small. The assumption that people will necessarily be incorporated vendors is not an assumption I'm prepared to make.

The Chair: Thank you for that.

Is there anything more?

In that case, I would like to ask the clerk to proceed to a roll call vote.

Frank Caputo: It's defeated on division.

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: That brings us to NDP-1, which is deemed to be moved.

I see that Madam Kwan wants to speak to it.

Jenny Kwan (Vancouver East, NDP): Thank you very much, Mr. Chair.

Bill C-8 proposes unrestricted secrecy provisions with respect to the orders the government will be able to issue to telecommunications providers and other entities. The amendment that I'm proposing would implement safeguards by limiting the grounds that justi-

fy the use of secrecy around the issuance of these orders by adopting language that is similar to that used in the Canada Evidence Act, which constrains secrecy to where it is justified on the grounds that disclosures "would be injurious to international relations or national defence or national security".

There are two components within the amendment. I won't read them out because everybody has copies of it, but it basically incorporates that language into those respective sections.

The Chair: Thank you very much, Madam Kwan.

Is there any intervention on that?

Go ahead, Mr. Ramsay.

[*Translation*]

Jacques Ramsay: We are opposed to the amendment because limiting it to defence and national security obscures a number of aspects related to the networks' technical and commercial activities.

I think the government's proposed amendments G-1 and G-3 are going to meet the needs in a much more appropriate and focused way than this amendment.

The Chair: I forgot to mention at the beginning that, if amendment NDP-1 is adopted, amendments CPC-5, CPC-6, CPC-15 and PV-4 cannot be moved owing to a line conflict.

Is it the pleasure of the committee to adopt amendment NDP-1?

(Amendment negated [*See Minutes of Proceedings*])

The Chair: That brings us to amendment CPC-5.

Would someone like to move that amendment?

[*English*]

Frank Caputo: Yes, Mr. Chair, I will be moving CPC-5.

This is similar to the issue we discussed at length at our last meeting, which was that rather than after-the-fact review and determining what should happen and whether things were done right, we should figure it out at the time.

Consistent with this rationale is judicial authorization for a non-disclosure order. If an order is being made by a judge, it actually makes sense that the judge should be making an order for non-disclosure.

It is for that reason that I move CPC-5 and support it.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

I'm giving you my ruling on this amendment.

Bill C-8 amends the Telecommunications Act by granting new powers to the Governor in Council to include a non-disclosure clause to an order made under section 15.1.

The amendment seeks to amend the bill by preventing the Governor in Council from including such a provision in the order, instead requiring him to make an application to the court to do so.

In the fourth edition of the book you're so familiar with, section 16.74 states that, “[an] amendment to a bill that was referred to a committee after second reading is out of order if it is beyond the scope and principle of the bill”.

I agree with that, so this amendment is out of order.

• (1555)

[English]

Frank Caputo: With respect, I will challenge the chair's decision.

[Translation]

The Chair: The chair's ruling has been challenged, so we will go immediately to a recorded vote on this.

(Ruling of the chair overturned: nays 5; yeas 4)

The Chair: This brings us to the discussion of amendment CPC-5. Therefore, I'll open the floor to debate.

Is there any debate?

Ms. Acan, go ahead, please.

Sima Acan: Thank you, Mr. Chair.

[English]

I'm looking at my notes again for CPC-5. Making non-disclosure conditional on a Federal Court application, as we spoke about again and again, could delay urgent action and may not capture other legitimate reasons that non-disclosure may be needed, such as commercial, reputational or technical risks to an entity or a broader system.

On that, my question will be on the response speed.

Given that cyber-attacks can occur at digital speeds—and we repeatedly say we are talking about milliseconds—how would the requirement to obtain prior judicial authorization for a non-disclosure order impact the government's ability to act instantly to stop an on-going breach without alerting the attacker that we are onto them?

Andre Arbour: For this type of concept, as officials who have been talking to different parts of Justice since Tuesday, we are still grappling with all of the scope of its applications, given how unprecedented it is in administrative law. There are different parts and pieces of it that we're finding out are new problems, and it's going to take weeks for us to unpack it all.

With regard to the judicial authorization of a cabinet decision, we're going to need to come up with a new process for cabinet confidence. We can't bring cabinet confidence to court.

We're not sure, but it likely does not match the crosswalk to the confidential evidentiary provisions of the Canada Evidence Act, so we're not sure if we could use confidential evidence with the court.

On your question, though, in terms of a specific time, our best guess at this point is that for something that was truly urgent, we couldn't accomplish it in a matter of days under Bill C-8 as tabled. It is probably going to be months, and what would be months would likely be years.

Sima Acan: Continuing on that question, does this amendment not create a gap by ignoring the valid non-security reasons for secrecy—such as protecting a company's commercial reputation or preventing a market panic—that fall outside the narrow national security definitions used by the courts?

Andre Arbour: There are some secondary considerations around the criteria cited, and that is why the text of G-1 is more appropriately scoped to the subject matter of part 1, though the judicial authorization is the most novel part and the most challenging to implement, if it can be implemented.

• (1600)

Sima Acan: Thank you so much.

[Translation]

The Chair: Thank you.

I give the floor to Mr. Lloyd, followed by Mr. Caputo.

[English]

Dane Lloyd: Thank you.

I think it's interesting that we're kind of being sold this fantasy that the government doesn't already have the capabilities of stopping a cyber-attack that, as the member across said, could be happening in a millisecond.

We have a report from the Communications Security Establishment that talked about the cyber-attacks they have stopped, as recently as 2024. The government does have the capability of stopping these attacks. What this legislation is talking about is the removal of telecommunications equipment that could potentially cause a threat to the telecommunications system.

Mr. Arbour, I want to bring you back to what I believe was your testimony earlier at this committee—not today, but earlier in the study. You said it would be extremely rare for the government to use a non-disclosure order. Do you recall making that statement? Can you clarify that you did make that statement?

Andre Arbour: Yes, that is correct. I did say that, or a version of that.

Dane Lloyd: Mr. Arbour, given that you have stated that it would be very rare for the government to put in a non-disclosure order, it would have to be a situation of quite some gravity for you to want to put a non-disclosure order in. Wouldn't you agree that it would have to be a serious situation?

Andre Arbour: The reasoning behind why it would be a good idea to have an order or part of an order be confidential is that if there is a specific vulnerability in a provider's network, you may not want to advertise that vulnerability as they are fixing it and until that work is completed.

How long it would take to remedy the issue in question and the seriousness of it is very case-specific and would depend on the circumstances.

Dane Lloyd: But surely, if it is a serious issue—this is serious legislation—would a judge not consider that as important information in the speed at which they make their decision?

Andre Arbour: There are different considerations of what speed is in a judicial context. The processes I've been familiar with that are not done on a speedy basis are in the 12- to 18-month zone. When there is an expedited process in place, then you are more into weeks and months.

Dane Lloyd: As my final question, we're being told by members from the government side that this is about stopping live attacks on our telecommunications system, but what we're actually talking about are potential vulnerabilities in equipment, not live attacks that are happening.

Andre Arbour: Both circumstances are the risks we're concerned about. You could discover a circumstance of a vulnerability that's not known and is unlikely to be discovered and that might take some time for the telecom service provider to remedy, or you might discover something that is subject to an ongoing attack and would only get worse if it's not remedied as soon as possible.

[Translation]

The Chair: Thank you, Mr. Lloyd.

Mr. Caputo, the floor is yours.

[English]

Frank Caputo: Thank you.

We talked a lot at our last meeting about what we colloquially have been calling “exigency”, but it's what I will call “impracticability of judicial authorization”.

Ms. Acan said this is going to be happening in milliseconds. If something is happening in milliseconds, it is impracticable to get judicial authorization. I think we can all agree on that. That is why I requested—and I will reiterate my request—that the drafters draft an amendment that addresses situations in which judicial authorization is impractical.

In other words, when you don't have time to get judicial authorization but there is a threat, and that threat materializes before you can get before a judge, the government would be empowered to act: You get before a judge then and you get your authorization. This happens very frequently in other areas of law in which we aren't getting a warrant in the next three minutes and we have to take action to secure the evidence, or in this case the system or whatever it is—the infrastructure—and then we get it.

With all due respect, Mr. Arbour—and you are much more an expert on this than I am—where I part company with you is where you say that it will take months. Please walk me through that.

This is the proposed amendment. It says, “A judge of the Federal Court may”. That also goes to Ms. Acan's point about whether you have to do something. This is permissive; it is not compulsory, so there is no requirement that a judge must institute an order.

A judge can create a non-disclosure order. When can they do this? It's subject to conditions. That's pretty normal: A judge may make an order of prohibition of disclosure “if the judge is satisfied that there are reasonable grounds”—reasonable grounds are usually made under oath or affirmation—“to believe that the disclosure would be injurious to international relations, national defence or national security”.

Normally what happens in other areas is that somebody sets out why and how the disclosure would be injurious to international relations, national defence or national security. It need not be a doctoral thesis; it would simply be somebody telling a judge, “I believe this is injurious to national defence because....”

Where I further part company with past remarks is on the notion that the judge has to be an expert. The judge is listening to evidence, and that evidence is sworn to or affirmed on reasonable grounds. If that's the case, why are we talking about proposed subsection 15.1(4.1) taking months, when, as I see it, this is in affidavit form?

Maybe I'm just completely missing something. If I am, please let me know.

• (1605)

Andre Arbour: The practice and conduct of criminal law and administrative law are quite different. We are dealing with administrative law in this context.

In the scope for review in an administrative law context, there's a body of case law, but the most important decision is probably the Supreme Court's 2019 Vavilov decision. This spells out what are reasonable criteria in an administrative law context.

The proposed provision in question is so new and so outside of the normal practice of administrative law that we're still grappling with it and still trying to unpack exactly how it could be operationalized. It will take us some time to do so. That's one example of the types of things we are trying to think about—how this could be implemented—along with some of the other things I mentioned, such as the provision for the use of confidential information in this context in the Canada Evidence Act.

We probably don't have a crosswalk here, but it's going to take us a while to try to figure this one out.

Frank Caputo: I'm mindful of that. This is new, but sometimes the law develops in new ways.

Vavilov is obviously common law from the Supreme Court of Canada, which Canadian tribunals and courts on judicial review are bound by, but we're creating something other than common law. We're creating statute law that tells a judge, in the administrative context, which I know is a novel one.... Yes, this could be very new, as you would say, and perhaps, dare I say, groundbreaking. I don't like to say that, but you're smiling.

I'm sure it's giving some people fits and they're saying, "What are they doing?" but sometimes we have to challenge the process. If challenging the process means that despite it being in an administrative context, we would like a judge to see this and to make a decision on what could be a life-changing issue for parties.... I get that it's new, but I just don't get how.... You talk about the crosswalk, but saying that we don't know how it's going to work and that this is going to be different doesn't mean it's going to take months for somebody to satisfy a judge that, in terms of disclosure, there are reasonable grounds to believe something would be injurious to international relations, national defence or national security.

I guess where I'm struggling, sir, is that I don't see how that would take months simply because this is something we're figuring out. Sometimes we do have to figure things out. Sometimes we do have to change things. Perhaps this is that time or perhaps it isn't. That is ultimately up to the House of Commons. That's why I'm pushing back.

I'm not trying to be rude or anything. I'm just trying to put something on the table and clarify why I believe what I'm putting forward, in order to get legislation that balances privacy, charter rights and the government's necessity to protect our digital infrastructure.

● (1610)

The Chair: MP Powlowski.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): I'm trying to understand the issue here. I understand that the government may want a non-disclosure agreement because they don't want to advertise a vulnerability, but wouldn't that agreement be with the telecommunications provider that has the vulnerability? Also, why would a telecommunications provider that has a vulnerability advertise that they have a vulnerability?

Andre Arbour: The telecom service provider would have no objection to a confidentiality provision. There's no tension there. The issue is that there needs to be a positive power to give the government the ability to make an order confidential. Otherwise, it has to be public. It's one of the reasons why, for the government's proposed amendment G-1, the representations by the telecommunications service provider are one of the factors suggested for consideration.

Marcus Powlowski: The de facto is that an order would have to be public?

Andre Arbour: Yes.

Marcus Powlowski: Where is it published, or how is it made public?

Andre Arbour: It's within the Canada Gazette.

Marcus Powlowski: Everyone knows about the vulnerability because it's published in writing.

[Translation]

The Chair: Before I intervene again to recognize a member or to move to a vote, I will do what I should have done at the very beginning of the discussion on amendment CPC-5. I want to inform you that, if amendment CPC-5 is adopted, there would be a line conflict with amendments CPC-6, CPC-7 and NDP-2, which means that those amendments could not be moved.

That said, are there any other comments?

In that case, we'll go to a recorded vote on amendment CPC-5.

(Amendment agreed to: yeas 5; nays 4)

The Chair: Normally, we would have to go to amendment CPC-6, but there is a line conflict with amendment CPC-5, which was just adopted. Therefore, we will move on to amendment NDP-2.

I'm sorry, but we won't be discussing amendment NDP-2, as there is a line conflict with the amendment we just adopted. That is also the case with amendment CPC-7. As a result, we will go faster.

We'll move on to amendment G-1.

Do I have a mover for that amendment?

● (1615)

Jacques Ramsay: The amendment seeks to introduce a set of factors that the Governor in Council must take into account before making an order confidential. These factors are set out in paragraphs (a) through (f) of subsection (3.1).

- (a) the extent to which the disclosure could, in the Governor in Council's opinion, compromise the objective of the order;
- (b) the necessity of including such a provision in light of the nature of the threat;
- (c) the possibility of limiting the scope of the prohibition;
- (d) the impact of non-disclosure on the principles of transparency and accountability of the Government of Canada;
- (e) any representations made by the affected telecommunications service providers; and
- (f) any other factor that the Governor in Council considers relevant.

This way, the amendment lays out what we think is fundamental to the bill, specifically in paragraph (a). It also reflects the significance of the threat, specifically in paragraph (b).

The Chair: Thank you, Mr. Ramsay.

Mr. Caputo, go ahead.

[English]

Frank Caputo: Thank you.

I'm going to ask the officials about something. This is a bit of a mishmash. The reason there is no line conflict is that this is a new provision.

Given what we have decided in CPC-2 and CPC-5 and that this talks about the Governor in Council, in order to keep the language clear.... I'm not asking for your opinion on prudence, but just from a technical standpoint.... We've talked about judicial authorization. Now we're back to talking about the Governor in Council. In order to be clear given what has passed, should this not say "judge" or "justice" where it says "Governor in Council"?

Andre Arbour: Given that CPC-5 was carried, for G-1, while there is not a line conflict, there is at minimum a tension between them. G-1 is probably unnecessary in this context because there's already the judicial authorization piece with different criteria. That was carried as part of CPC-5.

Technically speaking, factors that the GIC would consider in recommending or suggesting that an order be confidential don't need to be the same thick criteria that a judge would consider in approving it, and there is overlap in those considerations. G-1 was more of an alternative to CPC-5, even if there's not a line conflict.

The Chair: I believe there is a little uncertainty. The legislative clerk may want to have a little time to investigate this and might seek some guidance from outside. I'll suspend for a couple of minutes.

• (1615) _____ (Pause) _____

• (1625)

[Translation]

The Chair: I call the meeting back to order.

We're at amendment G-1, which is procedurally in order, as it doesn't conflict with any of the amendments that have already been adopted.

Do any members want to comment on amendment G-1?

Mrs. DeBellefeuille, you have the floor.

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

I don't know to whom to put this question. When we did the clause-by-clause study of Bill C-12, your rulings were challenged two or three times, and the amendments were adopted. Then, at report stage, the Speaker of the House rejected the amendments we had adopted. I fear that it will happen again.

So I will vote in favour of amendment G-1. If the Speaker of the House happens to reject amendment CPC-5, I want to make sure that we will still retain amendment G-1, which I consider to be very important.

Therefore, I would encourage my colleagues to adopt amendment G-1 to give us the very important tools proposed in that amendment.

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Caputo, go ahead.

[English]

Frank Caputo: Thanks, Chair.

I want to build on what Madame DeBellefeuille just asked. I'm trying to think of a time when this has happened. I haven't been

here as long as others. I know that Ms. May is very knowledgeable about procedure, as are others.

If an amendment is ruled out of scope by the Speaker, it doesn't then come back here. The bill is just as is with that excised. Is that accurate?

The Chair: That is correct.

Frank Caputo: Okay.

If I understand Madame DeBellefeuille, she's saying that if that happens, G-1 will not be in the bill if we do not agree with the amendment, which leaves what is essentially a hole. I think that's her point.

The Chair: Well said.

Are there any more interventions?

[Translation]

In that case, we will proceed to the vote.

Is it the pleasure of the committee to adopt amendment G-1?

(Amendment agreed to on division [See Minutes of Proceedings])

The Chair: We're moving on to amendment BQ-2.

Do I have a mover for amendment BQ-2?

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Thank you, Mr. Chair.

We want to amend the text so that, when making an order, the Governor in Council must take into account not only its effect on the provision of telecommunications services in Canada, but also the confidentiality and security of telecommunications.

• (1630)

The Chair: Does anyone want to comment on amendment BQ-2?

Is it the pleasure of the committee to adopt amendment BQ-2?

(Amendment agreed to on division [See Minutes of Proceedings])

The Chair: We'll now go to amendment NDP-3, which is deemed moved.

Ms. Kwan, the floor is yours.

[English]

Jenny Kwan: Thank you very much, Mr. Chair.

This is amendment NDP-3. As it stands, the broad information collection powers under proposed sections 15.1 and 15.2 could be used to undermine the privacy of Canadians, including the security of their communications.

This amendment proposes stronger privacy protection by requiring the Governor in Council and the Minister of Industry to consider the effect on privacy and the security of communications of orders issued under proposed sections 15.1 and 15.2.

I note that this amendment is similar to BQ-2, BQ-3, CPC-8 and CPC-9. Hopefully, it will pass.

[*Translation*]

The Chair: Thank you, Ms. Kwan.

Do any members wish to speak to this amendment?

Mr. Ramsay, go ahead.

Jacques Ramsay: Given that we have different wording in other amendments, we prefer the other amendments, especially since amendment BQ-2 has already been adopted.

Therefore, we will be voting against this amendment.

The Chair: Thank you, Mr. Ramsay.

Is it the pleasure of the committee to adopt amendment NDP-3?

(Amendment negated [*See Minutes of Proceedings*])

The Chair: We'll move on to amendment BQ-3.

Could someone move amendment BQ-3?

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: We want to make a small change.

We propose that Bill C-8, in clause 2, be amended through point (a) by adding the following after line 20 on page 2:

(c.1) its potential impacts on the privacy of Canadians; and

This is a recommendation made by the Privacy Commissioner.

The Chair: Thank you, Mrs. DeBellefeuille.

Do any members wish to speak to this amendment?

Mr. Ramsay, you have the floor.

Jacques Ramsay: We maintain that this is consistent with the objectives of the act. That's in line with our reading of the act. So if the purpose of this amendment is to provide more assurance and to make some people more comfortable, we support it.

The Chair: Thank you, Mr. Ramsay.

Mr. Caputo, go ahead.

[*English*]

Frank Caputo: This is for the officials.

Can BQ-3 and CPC-8 essentially coexist? My sense is that CPC-8 goes further than BQ-3. Is that accurate?

Andre Arbour: Yes. CPC-8 refers to the privacy of persons, which, once again, in a legal context includes corporations. That is not a charter right under normal circumstances, so the framing under BQ-3 of the privacy of Canadians is much more legible to us and is something tractable that we know how to interpret.

The Chair: Are there any further interventions?

[*Translation*]

Is it the pleasure of the committee to adopt amendment BQ-3?

(Amendment agreed to on division [*See Minutes of Proceedings*])

The Chair: We're moving on to CPC-8.

Does anyone want to move CPC-8?

[*English*]

Frank Caputo: I will move CPC-8. It may be redundant given what was just stated, but the officials can feel free to chime in on whether it is redundant to BQ-3, on which we just voted on division. I'll leave that to the officials.

• (1635)

Andre Arbour: CPC-8 is likely to introduce quite a bit of confusion. Some parts of it are duplicative of the BQ amendment that was adopted. We'd have two different factors. One is the privacy of Canadians and one is the privacy of persons. The privacy of Canadians is a tractable legal concept that we can interpret. The privacy of persons includes corporations and is quite problematic and confusing.

Hopefully that is clear.

Frank Caputo: Given the incongruence and that BQ-3 has passed, if it was different timing, I would likely ask for a vote on it. However, I'll make the decision to seek unanimous consent to withdraw CPC-8, and we can move on to CPC-9.

The Chair: Is there unanimous consent to withdraw CPC-8?

Some hon. members: Agreed.

(Amendment withdrawn)

The Chair: This brings us to CPC-9.

Is CPC-9 being moved?

Frank Caputo: I will not be moving CPC-9. My apologies.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

CPC-10 has a line conflict with BQ-1, which was adopted a little earlier. As a result, it cannot be moved.

We're moving on to CPC-11.

Does anyone want to move CPC-11?

[*English*]

Frank Caputo: Before I move CPC-11, is there a line conflict? There is no line conflict, as there was with CPC-10, because we're dealing with only a very small text. Is that correct, Mr. Chair? Okay.

I will move CPC-11 to change “threat” to “serious, systemic threat”, just to gain more precision in language. We are talking about infrastructure.

I invite the officials to weigh in if they have any conclusions on that, but I am moving that now.

Jacques Ramsay: Are you removing “systemic”?

Frank Caputo: Are you asking me to remove “systemic”?

Jacques Ramsay: No. I thought that's what you said. No, you didn't say that.

Frank Caputo: Oh, no. My French is bad, but I didn't know my English was that bad.

The Chair: Given that this is very technical, just to make sure that everyone understood it in both languages, can you summarize again what you just said?

Frank Caputo: I am moving CPC-11. We'll leave it at that.

The Chair: Good. That should be easily understood.

MP Acan.

Sima Acan: Thank you, Mr. Chair.

This amendment seeks to narrow the government's focus to only serious systemic threats. Here, the word “systemic” is technically dangerous—I will repeat the same thing from a technical perspective—because it implies that a threat must only affect the entire national system to justify an order.

In reality, a major cyber-attack might target one specific service provider to gain a foothold or cause localized but severe damage. This amendment would prevent the government from acting against a significant threat if it was not deemed systemic, leaving individual parts of the infrastructure vulnerable.

I would like to ask the experts this question. In your experience, do cyber-actors always launch broader, systemic attacks, or do they often target one specific provider to gain a foothold? If this amendment passes, would the government be legally barred from issuing the ministerial order to protect a single TSP from a devastating non-systemic attack?

Andre Arbour: There are definite risks with this language. In part, it's a cumulative effect. We already have a requirement that the use of this authority needs to be reasonable in relation to the gravity of the threat. That already specifies that the use of the power needs to be commensurate with the level of the threat, so it can't be used for no good reason or for trivial reasons or anything like that, given the nature of the power itself.

The word “systemic” is not defined or is not a technical term that is familiar. Given that the phrase “telecommunications system” is existing language, which this is a novel variant of, it appears that it could imply that only an attack on the entire system is what the power could be used for. An attack on an individual service provider could still affect millions of Canadians.

• (1640)

Sima Acan: Technically speaking, if a threat is detected that has the potential to become a systemic threat but currently impacts only one network, does the inclusion of the word “systemic” force the

government to wait for the damage to spread before it has the legal authority to intervene?

Andre Arbour: It's possible. We don't know how this term would be interpreted. Given the other guardrails on the use of the power, there is a very real risk that it would be interpreted in such a way that only something on the scale of the entire system would be a threat that we could target with it.

Sima Acan: My last question is from a policy perspective. How would the ambiguity of the term “systemic” impact the speed of a response during a cyber-attack or cyber-emergency if government lawyers have to first determine whether a threat meets this high threshold before an order can be issued?

Andre Arbour: Certainly, these types of things add a non-trivial delay to how we work through things. With this level of ambiguity, it's difficult for me to predict how much time the lawyers would need in order to work through this in an individual context, and it would depend on the nature of the threat. However, it could impose a non-trivial delay before the government is comfortable to act.

[Translation]

The Chair: Thank you, Ms. Acan.

Mr. Caputo, you have the floor.

[English]

Frank Caputo: What about if “or” was added, so it would read “serious or systemic”? In that case, either one could be satisfied. How would that compare with G-1.2, for instance?

Andre Arbour: If the “or” were to be added, that would remove the issue with “systemic”, because the government could act with respect to a “serious” threat. It would make the language potentially a little redundant, given the reasonable grounds clause, but that would likely be manageable.

Frank Caputo: I'm not sure if my colleagues would consider it a friendly amendment to change the comma to “or”.

[Translation]

The Chair: Mr. Ramsay, you have the floor.

[English]

Jacques Ramsay: Could there be any confusion when you say “serious threat” for something that potentially can become very important and have huge consequences but at the time is not that serious? Could it be interpreted that this is not serious so we can't do anything about it at that point in time? It's relating to the potential of becoming huge, necessary and important.

Andre Arbour: It's unlikely that it would be an issue. Given the nature of the power we're talking about in terms of the suspension or disconnection of service, in plain language, it would be used only for a serious issue. Otherwise, there are less intrusive means that could be used, most likely.

The main issue when we looked at this is that it's a bit odd in its drafting given the other parts of the bill. As I mentioned, it's a bit odd to put this in when there's already the reasonable grounds proportionality consideration, because that's already all we need to tell you—that you could use it only for a serious threat. When we engage with the lawyers, sometimes they frown and are concerned about that. Other than some potentially awkward drafting, we didn't identify major concerns with the word “serious”.

• (1645)

[*Translation*]

The Chair: Thank you, everyone.

Are there any other interventions?

In that case, is CPC-11—

Michelle Legault (Legislative Clerk): Is there a subamendment?

The Chair: Mr. Caputo, if you wish to propose a subamendment, someone else must move it on your behalf.

[*English*]

Frank Caputo: I had suggested a subamendment, but perhaps I can just speak directly with Madame DeBellefeuille. I'm not sure whether she would be open to the subamendment. If it's not going to be voted on with a yes, there's no point in dealing with it.

My sense is that this is going to be rejected on division, so I won't put forward a subamendment. The amendment can be rejected with a vote on division, please.

The Chair: You want to submit...

Frank Caputo: I don't want to put a subamendment on the floor, because it will just be rejected.

The Chair: Understood. Thank you for the clarification.

Is CPC-11 adopted?

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: Is CPC-12 being moved?

Frank Caputo: I will move CPC-12 to clarify—and I believe this may have been raised by the officials—that an order under section 15 of the act cannot be used against an individual. Again, it's to add precision to the language.

The Chair: Are there any interventions?

Is CPC-12 adopted?

(Amendment agreed to on division [*See Minutes of Proceedings*])

[*Translation*]

The Chair: This brings us to NDP-4, which is deemed to be moved.

Ms. Kwan, you have the floor.

[*English*]

Jenny Kwan: Thank you, Mr. Chair.

The rationale behind NDP-4 is that, despite the bill's stated objective of strengthening cybersecurity in Canada, many experts and civil society groups have noted that it would create broad powers that can be used to undermine Canada's cybersecurity. Proposed subsection 15.2(2) in Bill C-8 could be used to issue orders that weaken the encryption standards in telecommunications networks. Currently, the government could use Bill C-8 to compel telecommunications providers in Canada to install back doors inside of Canada's networks, including lawful access-related capabilities.

This amendment would add an interpretive clause to proposed subsection 15.2(2) that is intended to limit the government from demanding that telecommunications providers enable invasive activities, doing so by balancing the confidentiality, integrity and availability of Canada's networks. This amendment was, in fact, recommended in the joint civil society Senate submission on Bill C-26.

I know this is the same amendment as CPC-13 and CPC-14. Hopefully it will pass.

The Chair: Thank you, Madam Kwan.

Indeed, NDP-4 and CPC-14 are identical. To my knowledge and understanding, CPC-13 and NDP-4 are not the same. We will now debate and eventually vote on NDP-4, but we will not thereafter turn to CPC-14, it being an identical amendment.

We have heard MP Kwan. Are there any interventions on that amendment?

Madam Acan.

• (1650)

Sima Acan: Thank you, Mr. Chair.

While the term “confidentiality, integrity or availability” sounds protective, it is, in my opinion, dangerously overbroad in the technical sense. The term “availability”, specifically, is a major issue. If the government orders a company to replace faulty or vulnerable equipment, that process might temporarily take a system off-line, which technically impacts the availability. These amendments could be used to legally block the government from requiring the removal of high-risk equipment, such as from Huawei, or from fixing legitimate security flaws because the act of fixing them causes a temporary disruption.

My questions will be for the experts and are technical.

If the government identifies a piece of hardware in our network that has been compromised by a foreign actor or others, it's immediately replaced. Would the inclusion of the legal ban on impacting availability prevent us from acting if the replacement process requires a temporary service outage?

Andre Arbour: That is a very substantial risk with the way this amendment is worded.

I would start by saying that order-making can only be used to protect the telecommunications system. That's how Bill C-8 is scoped. It cannot be used to order processes to further law enforcement or other matters. There's already not an ability to order the breaking of encryption under this provision. I totally appreciate that there are some civil society concerns about that possibility and that they're seeking a "for greater certainty" clause. In this case, though, it doesn't mention encryption; it's just very vague.

Given that encryption is already not permitted under the act, there's a very high risk that this would have substantial collateral damage. Sometimes replacing or fixing equipment can be done without any interruption, but sometimes you need to take a piece of hardware off-line in order to patch it or replace it. This would have that collateral damage. I believe that's why the government's G-2 amendment, which speaks specifically to the issue of encryption, focuses more on the issue at hand.

[Translation]

The Chair: Mr. Ramsay, the floor is yours.

Jacques Ramsay: Mr. Chair, I would simply like to draw your attention to the amendment we put forward in relation to this concern that has been raised. It has the advantage of being particularly clear: The minister cannot order the decoding of a private communication that is encrypted within the meaning of section 183 of the Criminal Code. It states exactly what the witnesses wished to hear when they appeared. Therefore, I much prefer this amendment to the one currently being proposed.

The Chair: Thank you, Mr. Ramsay.

Are there any other interventions?

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Mr. Chair, I am one of the members of the committee who expressed significant concerns about the issue of encryption. I understand Ms. Kwan and her concerns. Like Mr. Ramsay, I believe that amendment G-2 accurately reflects what I wanted to avoid and what I wanted the minister to clarify. Moreover, I think the minister made a commitment when she appeared before us. I am quite pleased to see that the government has taken this into account and that it is written clearly in black and white.

I will therefore unfortunately oppose amendment NDP-4 and instead support amendment G-2, which addresses the same needs as Ms. Kwan's amendment regarding encryption, but more clearly, in my view.

• (1655)

The Chair: Thank you, Mrs. DeBellefeuille.

Are there any other interventions?

(Amendment negatived on division [See Minutes of Proceedings])

The Chair: We're moving on to G-2.

Does anyone want to move it?

Jacques Ramsay: Yes.

For the same reasons I just mentioned, it responds exactly to the concerns that were raised during the committee's work. It serves to

reassure anyone who might think that communications could be decrypted. It's an additional safeguard that the government wished to include in the bill.

The Chair: Mr. Lloyd, you have the floor.

[English]

Dane Lloyd: Thank you.

I appreciate what the government is trying to do here, but I note that there are other amendments later on that seek to expand the definition of a private communication beyond what the Criminal Code states currently.

I wonder if the officials could answer this. There's some concern that under the Criminal Code, the definition of a private communication is not expansive and doesn't include things like metadata. If we were to pass this amendment, what would be the impact on future amendments that seek to expand the definition of a private communication beyond what the Criminal Code states?

Andre Arbour: The text here is specific to this provision, so it refers to just this provision specifically.

I'm sorry. I'm actually not entirely sure I understand the question.

Dane Lloyd: Okay. Maybe I'll ask the analysts.

They note that later on, there are some amendments that deal with the idea of the definition of a private communication. Private communication is outlined in the Criminal Code under section 183, as it says in this, but there was some concern from witnesses that the definition is not as encompassing as it needs to be to protect the privacy of Canadians' communications. I believe there's a Green Party amendment on this as well.

I'm wondering what impact the passing of this amendment would have on future amendments that touch on the definition of a private communication as outlined in the Criminal Code.

The Chair: I will suspend for a minute, because I'm uncertain as to whether they are able to answer that on their own. I'll be back in a second.

• (1655)

(Pause)

• (1700)

[Translation]

The Chair: We are resuming the meeting.

[English]

Thank you for your patience.

There are two pieces to MP Lloyd's question. There's the procedural piece and there's the legal piece. The legal clerks are advising me, as I understood earlier, that all of these amendments, including this one, are in order, so we can and should be discussing them. If there are legal conflicts, it's up to the experts to establish whether they exist and why they exist.

Mr. Arbour, if you have something to add, the floor is yours.

Andre Arbour: Thank you, Mr. Chair.

I was able to do a cross-reference with PV-3. Those have two different definitions, but there's nothing to say that for this part...at least from a policy standpoint. They both refer to the Criminal Code. A different one gets into some other issue, but the government amendment has to deal with issues around encryption and—

Dane Lloyd: You don't think they conflict.

Andre Arbour: I do not think they conflict.

The Chair: Thank you.

Is there anything more on G-2?

(Amendment agreed to on division [*See Minutes of Proceedings*])

The Chair: We're moving to CPC-13.

Is CPC-13 being moved?

Frank Caputo: I will move CPC-13.

The Chair: Is there any input on CPC-13?

[*Translation*]

Ms. Acan, the floor is yours.

[*English*]

Sima Acan: Thank you, Mr. Chair.

I have the same concerns I had with NDP-4. I feel like it's applying exactly the same thing I mentioned with regard to NDP-4. It is affecting the government's ability to act.

I will be opposed to this. I have the same concerns.

[*Translation*]

The Chair: Thank you, Ms. Acan.

Are there any other interventions?

Shall CPC-13 carry?

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: We're now moving on to PV-1, which is deemed to be moved.

Ms. May, you have the floor.

[*English*]

Elizabeth May (Saanich—Gulf Islands, GP): Thank you, Chair.

As you'll know, I want to put it on the record that the procedure—I don't know if Madam Kwan objects to the procedure—of each committee passing an identical motion makes a mockery of the idea that committees are masters of their own work. This has been how MPs belonging to parties of fewer than 12 MPs have had to work for some time since the motion was first invented by Mr. Harper's PMO. It was adopted by Mr. Trudeau's PMO and now by Mr. Carney's PMO. I need to put it on the record that we would have the right, as smaller parties, as MPs, to put individual amendments, such as we are doing here, on the floor at report stage. Those are our rights under the rules. They are denied when we have this particularly strange procedure.

I know that it may stretch credulity that I'm not thrilled that this is my opportunity to participate. I appreciate that amendments that are being carried on Bill C-8 are very close to what we want to see, having heard the witnesses and looked at the evidence from so many groups, but I'll keep my remarks brief. Your motion allows them for each member of Parliament—I'm not a member of any committee—whose motion is deemed to be before you. I find the strictures unpleasant compared with the rights we have at report stage.

[*Translation*]

Thank you, Mr. Chair. Once again, I'm sorry.

[*English*]

The Green Party's first amendment here is to deal with the question of encryption—to bring it back to mind. Many witnesses before this committee have spoken to the notion that, particularly, we've seen a weakening in Bill C-8 of some technical safeguards, notably encryption. Witnesses, particularly the Canadian Civil Liberties Association, have pointed out that robust encryption is critical to any efforts to secure telecommunications systems. Despite this technical reality, government agencies have repeatedly failed to prioritize cybersecurity over surveillance and sought to bypass encryption.

This amendment is very clear. On page 4, after line 41, in new proposed subsection 15.2(3.1), the language remains the same except for including encryption.

[*Translation*]

Thank you, Mr. Chair.

• (1705)

The Chair: Thank you, Ms. May.

Is there any debate?

Go ahead, Mr. Ramsay.

Jacques Ramsay: I simply think it's redundant, given that we adopted amendment G-2. We will therefore vote against this amendment.

The Chair: Any other interventions?

Shall PV-1 carry?

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: We are moving on to PV-2, which is deemed to be moved.

Ms. May, would you like to introduce it?

[*English*]

Elizabeth May: Thank you, Mr. Chair.

This amendment again relies on evidence before the committee from the Canadian Civil Liberties Association and others. I know there are some policy overlaps with other motions, but there are no line conflicts of which I'm aware.

In Bill C-8, service providers can be compelled to install highly intrusive surveillance capabilities for cybersecurity purposes. Once these capabilities are in place, it's the belief of a number of experts, and certainly the Green Party view, that Bill C-8 fails to ensure that their use is limited to cyber-defence. Again, the civil liberties associations are particularly concerned that the capabilities that are enabled and imposed through Bill C-8 could be used or will be used by security agencies to achieve objectives that are unrelated to cybersecurity, intruding on the rights of Canadians.

The Chair: Are there any interventions?

Is PV-2 adopted?

We haven't exercised this for a little while, so let's do a roll call vote.

(Amendment negated: nays 5; yeas 4 [*See Minutes of Proceedings*])

[*Translation*]

The Chair: We are moving on to BQ-4.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: I won't move it because I consider that G-2 addresses the same concerns.

The Chair: Okay.

We're moving on to PV-3.

[*English*]

Madame May, would you like to speak to amendment PV-3?

Elizabeth May: Yes, I will address it briefly.

The amendment you have before you affects line 3 on page 5. This again was a recommendation that the risk of...as the government is able to compel telecom service providers to intercept categories of Internet traffic that are of a highly sensitive nature. The amendment as proposed limits this to say "tracking data or transmission data" as those terms are defined under the Criminal Code. This is an amendment to ensure that the intrusions are balanced and limited as much as possible.

• (1710)

The Chair: Are there any interventions on PV-3?

Is PV-3 adopted?

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: Would you like to speak to PV-4, Madame May?

Elizabeth May: Thank you very much.

This is dealing with the telecom service provider being ordered to disconnect targets in order to access Internet and mobile networks, were there reasonable grounds to do so. Our amendment would require individual notification for people whose Internet access is blocked, as well as public notification for blocked websites. I know there are similar provisions in the bill for notification and public awareness, but this is specific in ensuring that the minister must, without delay, notify the person affected of that order and then take that information public.

The Chair: Thank you, Madame May.

[*Translation*]

If amendment PV-4 is carried, CPC-15 can't be moved because of a line conflict.

Jacques Ramsay: A point of order.

The Chair: Go ahead, Mr. Ramsay.

Jacques Ramsay: Can we have a ruling from the chair on the admissibility of CPC-15? It goes beyond the scope of the bill.

The Chair: The advice I received from the legislative clerks indicates that this amendment is admissible, but there is a line conflict. If the committee adopts PV-4, we won't then be able to consider CPC-15.

Is it the will of the committee to adopt PV-4?

(Amendment negated on division [*See Minutes of Proceedings*])

The Chair: We're moving on to CPC-15.

Would anyone like to move it?

[*English*]

Frank Caputo: I will move CPC-15.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

I'd like to share with you my decision regarding CPC-15.

Bill C-8 amends the Telecommunications Act by giving the minister new powers, including the power to include a non-disclosure provision in an order made under section 15.2 of the act. The amendment seeks to change the bill by preventing the minister from including such a provision in the order, instead requiring the minister to apply to the court to do so.

In *House of Commons Procedure and Practice*, fourth edition, at section 16.74, it states:

An amendment to a bill that was referred to a committee after second reading is out of order if it is beyond the scope and principle of the bill.

The chair is of the view that transferring to a judge the exclusive authority to extend the order introduces a new concept that goes beyond the scope of the bill. Therefore, I rule this amendment out of order.

Mr. Caputo, you have the floor.

[*English*]

Frank Caputo: With the greatest of respect, I seek to challenge the chair's decision, please.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

We will therefore proceed to a recorded vote on sustaining the chair's decision.

(Ruling of the chair overturned: nays 5; yeas 4 [*See Minutes of Proceedings*])

• (1715)

The Chair: We will therefore move on to CPC-15.

Are there any interventions?

Jacques Ramsay: Mr. Chair, I think we can move to the vote. We've already spoken on this several times.

The Chair: If that's the will of the committee, yes.

Are there any further interventions?

Shall CPC-15 carry?

(Amendment agreed to: yeas 5; nays 4 [*See Minutes of Proceedings*])

The Chair: We're now moving on to G-3.

Would anyone like to move it?

Mr. Ramsay, you have the floor.

Jacques Ramsay: This amendment seeks to introduce a number of factors that the Governor in Council must take into account before issuing a confidential order. These factors, which the minister will be required to consider, will help provide clearer parameters around the power to issue such orders.

As I mentioned earlier, Bill C-8 contains several safeguards, but at the request of the witnesses we heard from, we added these to make things clearer. These six paragraphs clearly set out the circumstances in which an order may be made. They are the same as those already found in amendment G-1 concerning the Governor in Council.

The Chair: Thank you.

Are there any comments?

Mr. Caputo, the floor is yours.

[*English*]

Frank Caputo: This is for the officials.

I assume this is the same situation we were dealing with before. There is a fundamental disparity between amendment C-5 and amendment G-3, in that the only reason to pass G-3, given the language in C-5, is in the event that CPC-5 is ruled out of scope by the Speaker. Is that correct?

Andre Arbour: Ultimately, it's up to elected officials how they wish to proceed with this type of circumstance, but yes, if you are concerned about the Conservative amendment being struck down the road, then supporting this amendment would make sure this one is in place should that eventuality occur. It is similar to what we had with G-1.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

Are there any other interventions?

Shall G-3 carry?

(Amendment agreed to on division [*See Minutes of Proceedings*])

The Chair: We're moving on to CPC-16.

Would anyone like to move it?

[*English*]

Frank Caputo: Wait one moment. Could I ask the officials a question before I move this, please?

The Chair: Yes.

Frank Caputo: Given that there is judicial authorization, does this still need to be moved? I ask because it would allow TSPs to request judicial review. In one case, you're seeking judicial authorization in advance. In the other instance, this is requesting judicial review.

Do the officials have any comment on whether the two go hand in hand?

• (1720)

Andre Arbour: This provision is doubly duplicative, most likely. At a minimum, it's duplicative of the rights that TSPs would already have to challenge an order to the Federal Court.

Even if the authorization circumstance didn't exist, there are problems with this. When you have a provision in law, the assumption from a statutory interpretation standpoint is that it's there for a reason and that it's doing actual work. Adding something duplicative creates confusion, and you run the risk that in another provision that doesn't mention the right to appeal to the Federal Court, it could be interpreted as the drafters saying that you don't have that right in a subsequent process.

Frank Caputo: To be clear, it is your position, Mr. Arbour, that there is 100% a right to judicial review as the bill is drafted.

Andre Arbour: Yes, 100%. It's how appeals work more broadly in terms of the Federal Courts Act and subsequent—

Frank Caputo: That was the issue. It was the necessity of spelling it out. If you're 100% confident and we have the other issues, I will not move this amendment.

The Chair: Thank you for that clarification, MP Caputo.

That brings us to CPC-17.

Is CPC-17 being moved?

Frank Caputo: No. I will not move this amendment.

The Chair: Thank you, MP Caputo. I shouldn't say this to someone from another party, but you are doing a very good job. It's not easy to follow the flow and coherence of all of these amendments, so well done.

This brings us to CPC-18.

Is CPC-18 being moved?

Frank Caputo: Yes. I would like to move this amendment, please.

The Chair: Are there any interventions on CPC-18?

[Translation]

Shall CPC-18 carry?

We'll proceed with a recorded vote.

(Amendment agreed to: yeas 5; nays 4 [See Minutes of Proceedings])

The Chair: We are moving on to PV-5, which is deemed to be moved.

[English]

MP May, would you like to speak to that amendment?

Elizabeth May: Yes, please. Thank you, Mr. Chair.

Of course, under the terms of the motion the committee adopted, all of my amendments are deemed moved. Thank you for having somebody magical put them before you. Nobody else is allowed to speak to them, I suppose, so I will at this point.

I feel very strongly about this one. I note that there's a line conflict with the Conservative Party's amendment CPC-19. It's nice to be in such strong agreement with Mr. Caputo on so many amendments.

I'm quite shocked that we have legislation brought before us that so clearly will not meet the standard of section 8 of the charter. The witnesses noting this were many, but I was particularly struck by how our intelligence commissioner, the Honourable Simon Noël, spoke so clearly to this point.

This amendment attempts to redress that problem by ensuring that before the interception and production of information is compelled, there is a process of judicial review, and that such personal information can only be obtained if it is proportionate, necessary and judicially authorized.

The evidence before this committee from the intelligence commissioner was very strong. Having read and weighed the charter statement put forward by the minister.... To remind you, the intelligence commissioner said, "I haven't seen anything in that statement that would give a justification under section 1 of the Charter." In fact, he said, "it's totally absent."

● (1725)

[Translation]

PV-5 is a little longer than the others.

[English]

We're putting forward important principles, and they need to be set out as to how the minister is constrained. The amendment reads:

The Minister must not require, under subsection (1), the provision of information relating to a person or a group of persons unless the Minister first obtains the authorization of a judge

I could go on, because it's very clearly important—

The Chair: Unfortunately, Madame May, with all due respect and the esteem I have for you, I have to, for reasons of equity—

[Translation]

Elizabeth May: Yes, I understand, but it's important, and I hope that this amendment will be adopted.

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

I have two comments on this.

First, as Ms. May mentioned, if this amendment is adopted, amendments CPC-19 and CPC-20 cannot be moved because of a line conflict.

Second, the chair finds this amendment inadmissible for the following reason. The bill before us allows the minister, under section 15.4, to order that information be provided to the minister if the minister considers it relevant to establish or verify compliance with an order made under sections 15.1 and 15.2. PV-5 would require the minister to obtain authorization from a judge to issue such an order in certain circumstances.

In the well-known reference work, it states that "an amendment to a bill referred to a committee after second reading is out of order if it goes beyond the scope and principle of the bill." The chair therefore concludes that introducing a requirement for judicial authorization prior to issuing such orders constitutes a new concept that goes beyond the scope of the bill. Accordingly, I rule this amendment inadmissible.

Mr. Caputo, you have the floor.

[English]

Frank Caputo: I don't know if we can pick this up tomorrow or if this is Ms. May's last time here—when I say "tomorrow", I mean the next meeting—but I will be challenging the chair.

[Translation]

The Chair: The chair's decision is being challenged. We will therefore proceed immediately to a recorded vote.

(Ruling of the chair sustained: yeas 5; nays 4 [See Minutes of Proceedings])

The Chair: Seeing the time, I think we will adjourn the meeting and resume next Tuesday. As you know, we have a different agenda next Thursday.

Thank you, everyone, and have a good evening.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

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

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

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

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

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

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

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

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

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

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>