HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

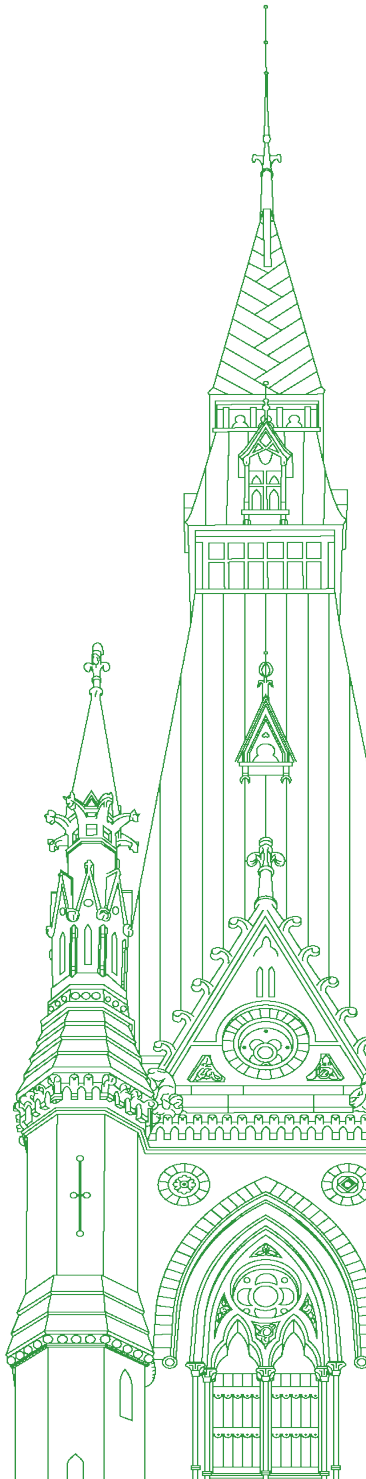
Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 009

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Tuesday, October 28, 2025



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, October 28, 2025

● (1210)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): Once again, welcome to the four senior officials who were kind enough to stay with us for the second hour. We have two other witnesses, Bridget Walshe, associate head, Canadian centre for cyber security, and Daniel Couillard, director general, cyber partnerships, Canadian centre for cyber security.

As I understand it, Ms. Walshe, you are the only one giving a presentation, so the floor is yours. You have five minutes.

Bridget Walshe (Associate Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair.

[*English*]

Good afternoon, Chair and members of the committee. Thank you for inviting us today to discuss Bill C-8, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts.

My name is Bridget Walshe. I am the associate head of the Canadian centre for cybersecurity—also known as the cyber centre—within the Communications Security Establishment Canada. I'm joined by my colleague Daniel Couillard, director general of partnerships and risk mitigation.

[*Translation*]

The Canadian centre for cyber security is Canada's technical authority on cybersecurity. We lead the government’s federal response to cybersecurity events and serve as a unified source of expert advice.

[*English*]

We're pleased to be here today to discuss Canada's cyber-threat landscape and the importance of cybersecurity in the context of Bill C-8.

I want to begin with a simple truth: Our world has never been more connected. From the smart phones in our pockets to the satellites orbiting above us, technology has woven itself into the very fabric of our daily lives. It powers our communications, our economies, our health care systems and even our democracies, but with this unprecedented connectivity and reliance on technology, we are exposing ourselves to its vulnerabilities. Whether it's the risk of state-sponsored cyber-threats, the exploitation of aging computer systems or the misuse of artificial intelligence, this interconnection brings with it a complex web of challenges that touch every sector and every Canadian.

[*Translation*]

Today, threat actors can bypass traditional foreign interference and espionage methods by deploying sophisticated malicious activities with unprecedented reach, all from the comfort of their home. In fact, through cybercrime-as-a-service platforms, with a few strokes on a keyboard, anyone with the means can quickly conduct large-scale campaigns that steal sensitive data, disrupt or deny services and influence public discourse.

[*English*]

As outlined in our 2025-26 national cyber-threat assessment, we are increasingly concerned about the enduring resilience of global cybercrime, as adversaries refine their methods, embrace new technologies and collaborate to expand their reach. I have a copy of the threat assessment report with me today available for committee members.

The evolving threat environment requires thoughtful and forward-looking measures. Strengthening Canada's cyber-defence capabilities is essential, but so is fostering meaningful collaboration between government and industry. By working together, we can move toward a more proactive approach to threat mitigation. To support this, a comprehensive incident reporting framework would help ensure that Canada remains responsive and resilient in the face of increasingly sophisticated cyber-threats.

[*Translation*]

Bill C-8 builds on its predecessor, Bill C-26, to advance Canada’s comprehensive, whole-of-society approach to cybersecurity.

[*English*]

Although CSE will gain no new authorities, this legislation will provide the government with tools and authorities to enhance cyber-defences and protect critical infrastructure. It will establish a regulatory framework for baseline cybersecurity of critical industry sectors, facilitating information sharing with the cyber centre and allowing regulators to seek CSE advice and guidance.

Bill C-8 underscores the importance of mandatory incident reporting by reinforcing the cyber centre's role in helping organizations resolve incidents and improving our collective ability to detect, respond to and prevent cyber-threats through sharing of cyber-threat information.

● (1215)

[*Translation*]

Incident reporting helps us to understand what transpired, share threat indicators and strengthen our defences. The information the cyber centre would receive from designated operators under Bill C-8 is strictly technical, focusing on indicators of compromise and exploited vulnerabilities.

[*English*]

In closing, let me leave you with this. Cybersecurity is a shared responsibility. If there's one lesson we've learned in cybersecurity, it is that no single entity, whether an agency, a government or a company, can succeed alone.

[*Translation*]

The Chair: Thank you, Ms. Walshe.

Now we'll turn to Mr. Lloyd for six minutes.

[*English*]

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

Thank you to the witnesses. We had you for an hour just before this. It was in camera. We asked some good questions and we got some answers. In the interest of transparency, I'm going to re-ask similar questions and hope that we can get the same answers.

I noted that under the CSIS Act, for threat reduction measures, you have to get a warrant from the Federal Court in order to move forward. It's not clear under this legislation whether the government would need a warrant to move forward with the actions they're giving themselves the power to do. Why is that?

Andre Arbour (Director General, Telecommunications and Internet Policy Branch, Department of Industry): The powers under Bill C-8 concern the ongoing regulation in terms of the security of underlying infrastructure.

In the instance of telecommunications, it's Bell's network infrastructure. They do not engage with certain charter rights or privacy considerations in that context. Similarly, that's how telecommunications operators are currently regulated. For instance, in the allocation of spectrum licences that are necessary to run their wireless networks, that's currently an authority under the Minister of Industry and there's no need for judicial oversight.

Dane Lloyd: We talked about a specified person in the previous hour, and you told me that they're a legal entity, not necessarily a natural person.

There's a concern that.... When you have legislation that's written to say that the minister has the authority to order the telecoms to cease providing services to a specified person, there's a fear that we're talking about individual Canadians. If you believe that an individual Canadian is a threat to the telecommunications system—they're degrading the system, disrupting the system or manipulating the system—why is there no requirement for a warrant in that case?

Andre Arbour: If I understand the question correctly, regarding the authority to withdraw services from an entity, in that context, first of all, the authorities are scoped in terms of needing to protect the Canadian telecommunications system. That means the individual commentary of Canadians or their ongoing traffic online is not germane to that in practical terms. That would be in the context, for instance, of a distributed denial of service attack, which is like flooding a network and essentially preventing the operation of it for other Canadians.

The use of that authority needs to be reasonably necessary to advance the stated goal. It can't just be on a whim. It needs to actually be tied to the gravity of the threat in question. We are dealing with circumstances where time is of the essence. These are services that Canadians rely on for life and death—to be able to call 911 or things of that nature—so there are considerations about being able to move quickly.

Dane Lloyd: Why the secrecy? Why are there secrecy provisions provided in this?

● (1220)

Andre Arbour: Generally speaking, the secrecy provisions are both not necessary and not operationalizable. When we're dealing with equipment that applies to all telecom carriers, 99.9% of the time we'll be going out with a public consultation with rules, and we want everyone to know the rules of the road.

There can be some specific circumstances where, for instance, an operator has a vulnerability in their network—it's very specific—where disclosing that vulnerability would essentially invite hackers to flood the zone while that operator is trying to get that under control. That's the use case for the confidential order-making provision.

It does include oversight—for instance, notification requirements to NSIRA and NSICOP so that they have line of sight and can ensure that the power is being used appropriately. It's also subject to annual reports to Parliament.

Even though—

Dane Lloyd: Is there an opportunity for judicial review if somebody feels that these decisions are infringing on their charter rights?

Andre Arbour: Certainly anyone can go to the courts with an application of judicial review and—

Dane Lloyd: What if it's secret, if they've been ordered not to say anything? How would they go to the courts?

Andre Arbour: We still need to consult the affected parties. That's a provision of the bill, and it's also a bedrock provision of administrative law.

The entity affected still needs to have the opportunity to make their case about how the order may affect them, and they can go to the court. There is also, again, the notification to review bodies and the annual report to Parliament, which, even if it doesn't disclose the detailed nature of the order, still needs to describe the activities, as well as their necessity.

Dane Lloyd: Is there a time limit on those things? It says specified time.

Andre Arbour: We have 90 days to notify NSIRA and NSICOP, and the report to Parliament is tabled annually.

Dane Lloyd: Thanks.

The Chair: Thank you, MP Lloyd, for these good questions.

Let me turn now to MP Acan for six minutes.

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

Thank you for being with us today.

I was going to ask this of Ms. Walshe, but Mr. Arbour and Mr. MacSween can contribute to the answers.

Canadian companies have been using offshoring, development outside of Canada. The critical cyber systems protection act part of Bill C-8 establishes a fundamental requirement for designated operators who manage vital services such as telecommunications, banking and energy to mitigate supply chain and third party risks.

If, so far, development is being offshored, the responsibility should still be on the Canadian company that ordered the development, and they should scan and verify the product they receive before they deploy it to production.

How does placing the explicit responsibility on Canadian companies, the designated operators, to establish and maintain comprehensive cybersecurity programs, including steps to identify and manage risk associated with the designated operator supply chain and its use of third party products and services, ensure compliance with high Canadian security standards, regardless of the physical location of the development or of the support team?

Kelly-Anne Gibson (Director, Cyber Protection Policy Division, Department of Public Safety and Emergency Preparedness): I think this gets to a really important aspect of the bill. As you say, the obligation is on the designated operator to make sure that any third party services or products they use are up to a reasonable standard to mitigate those risks.

The way this would work is that the designated operator would have a cybersecurity program in place. They would have a plan for how they mitigate those risks, which means they would have a plan for how they would assess the various services and products that they might contract to be used in their networks.

There's advice and guidance that comes from the cyber centre, and they can use that advice and guidance to understand how best to identify the products and services that will maintain the safety and integrity of their network.

One element of this that will help the cybersecurity ecosystem writ large is that it means that companies that are selling their products and services to critical infrastructure will have to make sure that their products are secure by design and that they're not rushing to market and fixing potential flaws after the fact.

● (1225)

Sima Acan: Thank you.

In addition to the general risk mitigation, foreign state actors and entities from high-risk countries pose direct threats to our national security.

How do the expanded emergency powers granted to the Governor in Council under part I of the Telecommunications Act—specifically the power under the proposed new section 15.1 to “prohibit a telecommunications service provider from using all products and services provided by a specified person” and to direct their removal—provide the government with the precise and necessary tool to safeguard the Canadian telecommunications system against interference, manipulation, disruption or degradation?

Andre Arbour: There are products and services that can be under the control of a hostile adversary, either in terms of the producer of those products and services being subject to extrajudicial oversight or in terms of other means by which they could be used to infiltrate Canadian infrastructure.

In that context, especially given that software is increasingly important, risk mitigation may not be possible in using that equipment or service. Therefore, the authority in question gives the government the ability to restrict its use entirely or to have it removed from the Canadian telecommunications system.

Sima Acan: Thank you very much.

Considering the scenario where foreign support teams remotely access the runtime environments, it is critical that they adhere to the same mandatory security posture as Canadian employees, ensuring competitive fairness across the sector.

Since designated operators must integrate steps into their cybersecurity programs to protect critical cyber systems from being compromised, how does the implementation of mandatory security standards and risk mitigation measures address the concern that companies utilizing international supply chains might otherwise gain an unfair economic advantage by circumventing necessary domestic cybersecurity costs?

Kelly-Anne Gibson: If I understand the question, you're asking how a company would manage the financial aspect of having to mitigate these risks and whether it puts them at a competitive disadvantage. Is that right?

Sima Acan: That's correct.

Kelly-Anne Gibson: The bill itself does not directly address that. However, what we have looked at, in the context of this bill, is trying to ensure that we create a cybersecure environment in a way that does not put undue burden on industry. In this particular case, having a cybersecure environment is important because the bigger risk is an incident. One incident can outweigh years of profits and, frankly, can incur so much damage that it would eclipse the expense of trying to keep the environment secure from the get-go.

The bill does not address this directly, but it is meant to protect the Canadian economy and the industries themselves in that way, just because the threat and the cost of a cybersecurity incident are so high, if it were to materialize.

Sima Acan: Thank you very much.

[*Translation*]

The Chair: Thank you for those great questions, Ms. Acan.

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

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

Ms. Walshe, we had Ms. Gibson in the previous panel, and she said that the government was well aware of the jurisdictional overlap with provincial cybersecurity authorities when it was drafting Bill C-8.

The Chair: Mrs. DeBellefeuille, sorry to interrupt you, but you mustn't refer to information that was provided in camera.

Claude DeBellefeuille: That's right. My apologies.

Ms. Walshe, Bill C-8 will probably lead to interference in certain provincial and territorial responsibilities. Our party came to the same realization in relation to agreements between Hydro-Québec and the U.S.

You play a central role in protecting government information, and you said at the outset, in your presentation, that the government could not tackle cyber-threats on its own. It has to be a team effort, bringing together businesses, provinces and territories.

Under Bill C-8, how do you plan to share information with your provincial and territorial partners?

● (1230)

Bridget Walshe: Thank you for your question. I'm going to answer in English.

[*English*]

We have very strong working relationships with our counterparts in all the provinces and territories. For example, we meet regularly with those responsible for cybersecurity. We have a working group that meets in person at least once a year to exchange information on cybersecurity issues, and in fact we have discussed Bill C-8 and Bill C-26, the predecessor, with our counterparts and have really heard from them about the fact that....

Hydro-Québec is a good example, because they are subject to regulation within Quebec and they are subject to regulation within the U.S. because of the transborder energy they sell. They would also be subject to regulation under Bill C-8. We really have a good connection with them to understand their concerns with new regulation and the processes involved.

Also, we work regularly, on a day-to-day basis, when it comes to cyber-threats. We work very closely with all critical infrastructure providers and provinces and territories to share threat information.

For example, if we hear about a cyber-incident impacting Canadian critical infrastructure, while we don't have mandatory reporting requirements today, we receive voluntary reports. We take that information, understand it, and distill what we can share. We share that information with critical infrastructure partners and with the provinces and territories so that everyone is able to take that information and use it to defend their own networks.

I might turn to my colleague Dan Couillard to share a little more detail about our interactions with the provinces and territories.

[*Translation*]

Daniel Couillard (Director General, Cyber Partnerships, Canadian Centre for Cyber Security, Communications Security Establishment): Since the Canadian centre for cyber security was created, we have worked extensively on our relationships with the provinces and territories. As my colleague mentioned, incidents are reported to us, and that's been the case since the centre opened.

In 2024-25, more than 1,400 cybersecurity incidents were reported to the centre. In every case, we worked with other jurisdictions. We shared information. Many cases involved regulated entities with cross-border operations in the U.S., Canada or the provinces. We are familiar with those situations, and we've been examining them for a number of years now.

Under Bill C-8, it will be mandatory to report certain incidents. The idea behind the approach is that the more information we have, the better equipped we are to identify the threat and notify the targeted entity, as well as other entities in the sector. They can then work proactively to protect themselves, while protecting other sectors as well. As we know, Canada's critical infrastructure sectors are highly interconnected, so timely responses are key. We are familiar with all that, and with Bill C-8, we'll be able to gather and share that wealth of information.

Claude DeBellefeuille: Bill C-8 sets out penalties. In light of the jurisdictional overlap, I was wondering whether Hydro-Québec, for instance, would be subject to a double penalty if it violated Bill C-8.

[*English*]

Kelly-Anne Gibson: Bill C-8 was created in a way that lets us rely on the existing regulator for the entities. The reason we did that was that those regulators already know their business, so they're already very familiar with working in a regulatory environment where there is another provincial regulator and where they can deconflict.

I can't speak to how they would deconflict or whether there could be a case of a double AMP or something of that nature. However, what I can say is that we would rely on the existing regulators, who are already used to managing provincial and federal regulation in those industries to promote compliance in those industries.

● (1235)

[*Translation*]

The Chair: Thank you, Mrs. DeBellefeuille.

Over to you, Mr. Gill, for five minutes.

[*English*]

Sukhman Gill (Abbotsford—South Langley, CPC): Thank you, Mr. Chair, and thank you to the witnesses for being here today.

My line of questioning is going to be on freedom of speech and expression.

The Canadian Constitution Foundation has raised concern about the civil liberties implications of Bill C-8 in proposed section 15.2, which would give the minister the ability to make decisions to kick someone off the Internet.

What safeguards are in place to prevent the government from using cybersecurity as a pretext for silencing speech?

Andre Arbour: I certainly appreciate the importance of the subject raised. There are protections at the outset, during the use of the authority and after the fact. For instance, the policy objective specifies the protection of the Canadian telecommunications system as the overarching scope of action, so individual speech has no bearing on the ability of Bell Canada or Rogers to maintain its network or the reliability of its services. There is no relation there.

There's further precision that the use of the authority needs to be reasonable relative to the gravity or the nature of the threat that you're trying to combat. There are criteria established by the Supreme Court over many decades, including in the 2019 Vavilov decision, which specifies what reasonableness will be. There are other oversight and reporting requirements, including to NSIRA, NSICOP and then, finally, to Parliament.

Sukhman Gill: Okay, thank you for that.

Well, it seems that if this legislation is passed in its current form, unamended, we are going to be giving the Minister of Industry sweeping powers, with virtually no checks or balances. In theory, the minister could wake up one morning, as one of my colleagues referenced, and not be impressed by a post on social media, going further to basically say that it poses a threat to our telecommunications services. Without a warrant, without a trial, without any automatic judicial review, the minister could compel Rogers or Telus to go seek these people's private data.

What do you have to say about that?

Andre Arbour: I would note the scoping mechanisms that limit any action with respect to the disconnection of services. Furthermore, to the question about personal data, first, the scoping applies to those considerations as well. Again, the personal data or browsing history of individual Canadians is not germane to the underlying maintenance or reliability of the telecommunications infrastructure in question.

There is a further amendment that was adopted with Bill C-26. For greater certainty, it explicitly prohibits the use.... This was already prohibited, but it adds an extra level of clarity so that the order-making powers cannot be used to intercept private communications.

Sukhman Gill: What measures can be put in place to ensure that this isn't misused, or worse, turned into a political tool for the Liberal government against people or organizations they disagree with?

Andre Arbour: Ultimately, what the committee decides is the committee's prerogative, so I can't speak on behalf of the committee. I would note that the set of authorities that were introduced with the bill and that were adopted in the previous committee study add protection both at the outset of the scoping.... The concerns that have been raised are already prohibited within the scoping of the law currently. There are also consultation requirements that allow for additional oversight and consideration of the use of those powers. Then, there are notification requirements and reporting requirements, including for the narrow confidential use of authorities, that ensure oversight.

● (1240)

Sukhman Gill: I have a final question.

Multiple civil society groups have raised concerns about federal governments trying to grant themselves the power of intrusion into our private lives in the name of security. Have these organizations been genuinely consulted before the development of this bill?

The Chair: You have about 15 seconds.

Kelly-Anne Gibson: The short answer is yes. We have received multiple submissions from civil liberties organizations. I can say for sure that my team looked at them, studied them very carefully and considered them very carefully, including submissions that were made to the committee in the previous Parliament. We studied those very carefully.

[*Translation*]

The Chair: Thank you for your questions, Mr. Gill.

It is now Ms. Dandurand's turn for five minutes.

Marianne Dandurand (Compton—Stanstead, Lib.): Thank you, Mr. Chair.

Thank you, ladies and gentlemen, for the very clear answers. It's all very interesting.

I want to follow up on my fellow member's questions about privacy. Ordinary citizens are very concerned. Can you enlighten us and tell us who exactly the cybersecurity legislation covers?

[*English*]

Kelly-Anne Gibson: I can speak to part 2, and then perhaps I can turn to my colleague for part 1.

Part 2 would apply only to designated operators who have been established in schedule 2 of the act. Currently, the way the act is written, schedule 1 lists vital services that we need to protect, and then within those sectors, we would designate, through the regulation-making process, specific operators. The obligations act only upon those designated operators, so those are the owners and operators of critical infrastructure. It's those companies that it would act on.

[*Translation*]

Andre Arbour: In short, the proposed act in part 1 applies to telecom service providers such as Bell and Rogers.

Privacy came up because, generally speaking, the networks of telecom providers hold customer data, Canadians' and businesses' data. That is why the powers provided for in Bill C-8 have a limited scope. The bill includes clarifications such as the one prohibiting personal communications from being intercepted. That is all to make clear that Canadians' personal information is not subject to these powers. Instead, the purpose is to protect networks and critical infrastructure.

Marianne Dandurand: I understand that the bill, in its current form, in no way applies to people's personal information, but are more safeguards necessary? Since the proposed act does not apply to personal data currently, can we be sure that that won't change in the future?

Andre Arbour: The powers set out are really aimed at telecom service providers and their networks. Specific powers make it possible to collect information from those providers. The idea is to understand what equipment their networks use. Canadians' personal information is not covered by the measures, which are aimed at protecting the networks in question.

The powers in this part of the bill and their scope are directly tied to the order. Although some situations engage just one aspect of the bill, the part has to be read as a whole in order to better understand the safeguards it contains.

● (1245)

Marianne Dandurand: Thank you, Mr. Arbour.

Ms. Walshe, we haven't talked about the impact of cyber-threats and ransomware attacks. Currently, what is the financial toll on Canadians?

[*English*]

Bridget Walshe: Thank you very much for the question.

[*Translation*]

I will answer in English.

[*English*]

It's difficult to measure the impact that cybercrime has on Canadian organizations, for a few reasons, but we know that the impact is large.

From a financial perspective, we do know that Canadian organizations make payments to crimeware groups that total in the hundreds of millions of dollars, but not all of those figures are reported to us. To understand the complete impact.... We have incomplete information.

We also know that it's not just the impact of a payment that somebody makes to a criminal that has a financial cost to an organization. It's also the loss in productivity and the recovery from those attacks that are quite expensive.

Those sorts of figures are also difficult to understand because those are things that a private enterprise may disclose as part of its public reporting or that may be kept private, so it's difficult to say.

[*Translation*]

The Chair: Thank you, Ms. Walshe. That's all the time Ms. Dandurand has.

Mrs. DeBellefeuille, you may go ahead for two and a half minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

I commend you, Mr. Arbour, for answering questions in French. It's always a bit disappointing when senior officials aren't proficient in both official languages. As a francophone, I must tell you how happy it makes me to hear you answering questions in French. It shows that you are fluent.

I have a short question about providers. You mentioned big providers like Bell. However, many small businesses are involved in bringing high-speed Internet to small, rural communities. Where I'm from, for example, we have Targo and the co-op CSUR.

Do you think those small providers are equipped to meet the requirements in Bill C-8? Can they afford it? Are there any plans to provide them with support?

Andre Arbour: The Department of Industry is used to working with small telecommunications service providers. One of our objectives is to support these types of operators to promote competition within sectors and expand networks in rural and remote areas. It's important for us to establish rules that match the skills of service providers of all sizes, even small businesses.

For example, during the spectrum auction, we set rules specific to small service providers. The same goes for the implementation of this bill. For example, in our consultations, we take into consideration the time needed to achieve the objective of a regulation based on the size of the supplier. The large players have a certain level of systematic risk compared to a small provider that serves 500 consumers.

The Chair: Thank you. I'm sorry, Mrs. DeBellefeuille, but your time is already up.

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

[*English*]

Dane Lloyd: Thank you.

There have been some groups, such as the Canadian Civil Liberties Association, that have talked about encryption standards. There's a fear that this legislation will give unprecedented powers to break encryptions.

Is there anything specific in this bill that deals with encryption-breaking powers?

● (1250)

Andre Arbour: There isn't a specific provision governing encryption; however, the ability to break encryption for the purpose of surveillance is out of the scope of the powers here.

Being able to access individual information for the purpose of law enforcement is certainly an important issue. It's a very hotly discussed topic. We've seen it in Bill C-2, for instance. It is deliberately out of the scope of this bill. For instance, breaking encryption does not advance the protection of telecommunications network infrastructure. It has nothing to do with that.

Dane Lloyd: Thank you for that clarification.

I think the argument that has been advanced.... I apologize to these organizations if I've mislabelled their argument. They talk about the wording that the minister can order the telecoms “to do anything, or refrain from doing anything”, and they're saying that's a very broad power that could lead to the breaking of encryption.

Can you describe why that power has been worded like that? I even thought to myself that this seems like very interesting wording to use, “to do anything, or refrain from doing anything”. It seems very broad.

Andre Arbour: The wording is meant to capture the range of risks to the telecom infrastructure that can exist. For instance, one may want to tell a service provider that they cannot use a particular product or a service in their network, or that they need to take some positive action to protect their network.

A bedrock principle of statutory interpretation is that you need to look at the bill as a whole. For instance, the policy objective, at the outset, sets the overall scoping. There are additional requirements—for instance, that the order-making power needs to be reasonable to the gravity of the threat, etc. Those all still apply and structure the government's ability to act.

Dane Lloyd: Thank you.

We've talked about personal data. You've said it's outside the scope of this. We've gone over that. However, the intelligence commissioner has stated in testimony that this power of the minister to ask the telecoms to do something or refrain from doing something could give them the ability to ask telecom providers to provide the private information of Canadians. I believe the Privacy Commissioner has also raised this concern.

Can you elaborate on those concerns? Is that a concern, and if not, why not?

Andre Arbour: The information collection authority in part 1 is modelled on the existing section 37 of the Telecommunications Act, which has been in place for decades without incident. It's just carried forward, because it needs to be applied to the new security network protection authorities. It is still structured within the scope of what can be done to protect the Canadian telecom system, and not to advance general security or law enforcement aims. It is still limited to the order-making authorities and the protection of Canadian telecom systems. It cannot be used to advance a generalized fishing expedition or investigation into personal information.

Dane Lloyd: Thank you.

Finally, how is it determined that the minister's decision, under this power, is reasonable? Who determines if it's a reasonable thing that the minister has done?

Andre Arbour: First, there is consultation on the rules. We are required to take into consideration what those views are. There are notification and transparency requirements after the fact. Then, ultimately, all decisions of the minister are reviewable by the courts. The telecom operators are not shy to go to the courts. They are well resourced and frequently make use of that avenue.

● (1255)

[*Translation*]

The Chair: Thank you, Mr. Lloyd.

We will conclude with Mr. Ehsassi.

[*English*]

Hon. Ali Ehsassi (Willowdale, Lib.): Thank you, Mr. Chair.

Thank you, witnesses, for your very comprehensive responses.

Does this legislation now make it mandatory for all these operators to report every single breach they may experience?

Colin MacSween (Director General, National Cyber Security Directorate, Department of Public Safety and Emergency Preparedness): The mandatory reporting requirement appears in part 2 of the act. The answer to your question is no. The intention there is that the legislation will set out the requirement for mandatory reporting, and then the regulations will define exactly what that looks like.

I mentioned earlier that we have had some discussions with Five Eyes counterparts about what their mandatory regimes look like. Those have been specifically on the threshold for reporting. Our colleagues from the cyber centre certainly aren't interested in receiving information on every single cyber-incident. A lot of those are day-to-day things everybody experiences that we have good traction on. What we want to understand is when there's an incident that has a certain level of significance. That's what we want reported to the cyber centre.

Hon. Ali Ehsassi: Thank you.

Then there's the mention of AMPs in this legislation. Do we have any sense yet of what the highest administrative monetary penalties would be?

Kelly-Anne Gibson: Yes. It's in the bill. I'm sorry, but I don't remember the exact number. I can tell you that because this is a cross-sectoral framework and different industries have different thresholds, it's set high, but it will be set within a range that is typical for the industry being regulated.

Hon. Ali Ehsassi: Thank you very much.

I have one last question, if I may. In the information you've provided to us, it says, “Cyber incidents cost Canada’s economy $5 billion annually, with Canadian businesses paying nearly $7 million per data breach.” Could you just roughly tell us why these data breaches cost companies so much? Are these attempts to pay customers because there have been privacy breaches? Why is it so large?

Kelly-Anne Gibson: There are a number of factors.

If you have a breach, a cyber-incident, your data can be compromised, so the first thing that happens is that you have to figure out what has been compromised. That can be incredibly expensive, because you have to bring in experts to understand what exactly is going on with your network. What's been compromised, and what's potentially been exfiltrated?

Then, you have to start putting in place remedies, and not only from the technical perspective. You also have to start looking at your regulatory responsibilities. Are you now not in compliance? There are privacy laws that are going to come into play, such as PIPEDA, the Privacy Act and all those types of things. There are notifications. There are lawyers and breach coaches who get involved. The costs mount.

The other piece, which is a little more intangible, is simply the reputational cost. Often, these will eventually become public, and you potentially begin losing customers. That's how the costs start multiplying very quickly.

Bridget Walshe: I might add to that a little bit.

From a technical perspective, it's the enormous expense that's paid, as my colleague pointed out, to remediate the situation immediately, but it's also the enormous cost of rebuilding and the losses in revenue that a business may have while that rebuilding occurs. We know that there's a huge cost incurred, not just in the immediate aftermath of the incident but also in rebuilding the technology to get back up and running.

The Chair: Thank you so much.

[*Translation*]

Witnesses, I want to thank all six of you for being here. We're grateful not only for your presence, but also for your preparation for this important meeting. We hope you have a great day.

I invite committee members to stay for a few moments while we finish this meeting.

Mr. Ramsay, the floor is yours.

[*English*]

Jacques Ramsay (La Prairie—Atateken, Lib.): I'd like to propose two motions.

The first one relates to Bill C-12:

> That, in relation to the study of Bill C-12:
>
> The committee invite members to submit witness lists to the clerk of the committee no later than October 29, 2025, at 5:00 p.m.;

That's tomorrow.

> That the committee schedule four meetings to hear from witnesses; invite the Minister of Public Safety to appear and invite relevant officials;
>
> And that the committee conduct clause-by-clause consideration of the bill after the conclusion of witness testimony on the fourth meeting, and that the committee does not adjourn until clause-by-clause has completed.

That's the first motion.

● (1300)

[*Translation*]

The Chair: Thank you, Mr. Ramsay.

Mr. Caputo, you have the floor.

[*English*]

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you, Chair, and thank you, MP Ramsay, as well.

There are a lot of moving parts here, so I'll attempt to summarize it all, because I think we have a general consensus. I just don't want to miss anything here.

With respect to the Bill C-12 motion that was just read, I'm not sure if he said a minimum of four meetings. That was my impression.

Was it a minimum of four meetings?

Jacques Ramsay: It was four meetings.

Frank Caputo: Okay. My understanding was that it was to be a minimum of four meetings.

One thing that should be noted—and we can have an agreement or an understanding of an agreement—is that we wouldn't move to clause-by-clause immediately. For instance, if the witnesses finish their testimony at one o'clock, we wouldn't be moving into clause-by-clause at 1:05. We would be taking two hours per meeting for clause-by-clause.

I think those were the two main issues.

Mr. Ramsay is saying four meetings. My understanding was that the agreement was for a minimum of four meetings, so I will just try to get some clarity on that.

I believe he's going to speak about Bill C-8, so while I have the floor—

The Chair: MP Caputo, would you mind reserving your comments until the motion regarding Bill C-8 is moved?

[*Translation*]

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Mr. Chair, I'd like to move an amendment to this motion, if I could. I will read the text as amended by the three changes I am proposing:

> That, in relation to the study of Bill C-12:
>
> The committee invite members to submit witness lists to the clerk of the committee no later than November 3, 2025 at 4:00 p.m.;
>
> That the committee schedule a minimum of four meetings to hear from witnesses; invite the Minister of Public Safety to appear and invite relevant officials;
>
> And that the committee conduct clause-by-clause consideration of the bill at a sitting specified by the committee, following the final meeting with witnesses, and that the committee dedicate the number of meetings required for clause-by-clause consideration to be completed.

We felt that the October 29 date was rushed to provide the list of witnesses, so by saying “no later than November 3”, that gives the clerk some leeway to contact witnesses and prepare for the business meeting.

I agree with my Conservative colleague that a minimum of four meetings would be much wiser. However, I don't agree at all with the idea of burying the clause-by-clause study of the bill after hearing from witnesses, at the fourth meeting, until it's over. I think it makes more sense to start clause-by-clause on the bill after we finish hearing from witnesses at a later meeting.

The Chair: Okay.

[*English*]

Three things have been said: first, a minimum of four meetings; second, witness lists by November 3; and third, an implicit understanding that we would suspend, not adjourn, after the fourth meeting, which means that the next meeting would be a continuation of the meeting that was not adjourned. That's the understanding, those three things.

Is there a unanimous view on this?

Go ahead, Madame DeBellefeuille.

[*Translation*]

Claude DeBellefeuille: You've summarized the spirit of my amendment. That's my understanding, Mr. Chair.

The Chair: I did, yes.

Claude DeBellefeuille: Okay.

I want us to understand each other. We don't want to find ourselves in a situation where, at the fourth meeting—assuming there will be four—if there are still a few minutes left after hearing from the witnesses, we continue with clause-by-clause consideration of the bill late into the evening. Is that what you understand from my amendment?

I want to remind you that the Standing Committee on Citizenship and Immigration, or CIMM, will be studying the part of the bill that deals with amendments to the Immigration and Refugee Protection Act, and it will be hearing testimony. Since it will be up to our committee to do the clause-by-clause consideration of the bill, I think it's important for the analysts to be able to give us a summary of what was heard at the CIMM committee, since we'll have to read its recommendations. As a result, it seems to me that we should have a minimum of four meetings.

● (1305)

The Chair: Okay.

The clerk would like to clarify a few things.

The Clerk of the Committee (Andrew Wilson): I spoke to the clerk of the CIMM committee, who told me that his committee would submit its recommendations to the chair of our committee once his committee had finished hearing the testimony. Those recommendations will then be distributed to the members of our committee as soon as we receive them.

The Chair: Very good.

[*English*]

Is there consensus, possibly even unanimity, on these three changes to the motion being produced? First, there's the minimum of four meetings. Second, there is the November 3 date by which to submit a list of witnesses. Third, there is an understanding that the fourth meeting will be followed by other meetings to have the clause-by-clause discussion, and the fourth meeting will not be extended, possibly, to very late in the day.

[*Translation*]

It seems to me we're coming to a consensus.

Ms. Dandurand, the floor is yours.

Marianne Dandurand: I'm fine with the last two proposed changes, but I think we should stick to four meetings, without mentioning “a minimum of”. We won't give our consent to this proposal of “a minimum of” four meetings.

The Chair: Okay. I believe there have been preliminary discussions on this among the leaders' offices and that a preliminary agreement has been reached. We can't reopen these discussions once such an agreement has been reached. We need to avoid going around in circles.

[*English*]

I would like to remind everyone that these discussions are best taking place outside of such a meeting. My understanding is that there was an agreement to such a motion before it was tabled by MP Ramsay, so perhaps we shouldn't invest our time again in relitigating all of that.

MP Lloyd.

Dane Lloyd: Thank you.

I think there might have been some wires crossed here. I do like November 3 and the implicit understanding. To assuage your concerns, I'm fine with the four meetings and not saying “a minimum of four”. If there is a really compelling reason to have a fifth meeting, we can discuss that at a different time, but I think four is fine for the motion right now.

The Chair: Thank you, MP Lloyd.

Now, what about the date? Is November 3 a reasonable date? Okay.

Madame DeBellefeuille.

[*Translation*]

Claude DeBellefeuille: Mr. Chair, when you summarized the three changes I proposed in my amendment—I think we're discussing this amendment in a friendly manner—you did so in English. I just want to make sure I understood correctly.

As for replacing the words “October 29”, the words “November 3”, that's fine. If everyone agrees to hold four meetings instead of a minimum of four, that's fine with me, too.

However, I'd like to understand one thing regarding my last change. We may need one or two meetings for clause-by-clause. You understand that, after the testimonies, we would begin clause-by-clause consideration and that we can't say how many meetings it will take.

The Chair: I understand, but we're going to have to be disciplined, because we have a lot of other work to do afterwards. Many of you are waiting to conduct or complete other studies, so we're aware of the fact that the time available to all members is limited.

[*English*]

We have to be reasonable in our expectations, because time is the scarcest resource around.

MP Caputo.

Frank Caputo: Thank you.

I apologize. I was communicating throughout Madame DeBellefeuille's intervention.

My understanding is that there was an agreement for four meetings. I'm only talking about the Conservatives and the Liberals. This happened above my level.

If there is a concern, I would hope that we, as a committee, would be nimble and honour Madame DeBellefeuille's concerns. If we need another meeting, I would hope that this is something we would address, if need be, to allay any of her concerns. I believe that right now we're debating between four and a minimum of four. If it is four, then it's with an understanding that if there have to be more meetings, we would readdress that. Is that okay?

● (1310)

The Chair: I think there is indeed some consensus. Is everyone fine with that?

Madame Dandurand.

[*Translation*]

Marianne Dandurand: I'd like to make sure of one thing, Mr. Chair.

I think I misunderstood the last change proposed by my colleague's amendment. As I understand it, there would be only one meeting for clause-by-clause consideration and we would continue it until it is completed. Only one meeting would be held, without adjournment.

Claude DeBellefeuille: It would be a subamendment.

The Chair: Okay.

In that case, one meeting would be added after the fourth meeting on Bill C-8, but during that meeting, we would have to complete the clause-by-clause consideration of the bill. Did I understand correctly?

Jacques Ramsay: It's Bill C-12, Mr. Chair.

The Chair: I stand corrected. We are indeed talking about Bill C-12. Otherwise, have I understood correctly?

Marianne Dandurand: Mr. Chair, it isn't a subamendment. That's exactly how Mr. Ramsay's motion was written. Only one meeting would be held after the four meetings, which would be adjourned only after the end of clause-by-clause consideration.

The Chair: Okay.

I'm summarizing in a more informal way. If Mr. Ramsay's motion is accepted, with very specific amendments, four meetings will be held to consider Bill C-12. After the fourth meeting, there will be another meeting immediately following that to deal with clause-by-clause on Bill C-12. It will take as long as it takes to go through the clauses.

In addition, the list of witnesses would be submitted by November 3.

Claude DeBellefeuille: I'm opposed to it, because the change I proposed was intended to avoid that. I think this committee is quite rigorous. We have no intention of dragging out the study of Bill C-12, but I also don't want us to limit ourselves to a single meeting for clause-by-clause consideration, a meeting that may last two, three, four or five hours. That's the spirit of the change I proposed.

We don't have a steering committee, and that's why we always have a full committee meeting to organize our work. However, I'm really starting to question this approach because we had almost reached an agreement, but time is running out. It's 1:15 p.m. and this is the third meeting we've ended this way. If the Conservatives and the Liberals agree, let them call the vote, and I'll oppose it. I don't want to restrict clause-by-clause consideration, and I don't want to spend three, four, five, six, seven or 10 hours on it. I'll cooperate, and I know we'll work rigorously. It would be great if we could finish in less time, but I don't want a motion to restrict us.

I don't know how you're going to manage, Mr. Chair, but I have put forward an amendment. If it's rejected, another one can be moved and voted on. Then we'll decide how to proceed with our work.

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

[*English*]

Frank Caputo: Thank you, Mr. Chair.

I echo Madame DeBellefeuille's sentiment. We are all hearing from our various parties. I thought we had an agreement in principle, and I don't think consensus is that far away on all of these issues.

Typically, though, this would go to the subcommittee, and then the subcommittee can work it out behind closed doors, so to speak, where we all come very prepared to deal with that. I'm not sure.... It would be me, Madame DeBellefeuille, Mr. Ramsay and the chair. I believe we are on the subcommittee. I'm not sure if we can do something like that very quickly in the interim, because it appears we're not getting anywhere here.

The Chair: Yes, a lot of work needs to take place outside of this room and outside of subcommittee work. My understanding—and I was obviously not informed of everything—was that there was an agreement, as Mr. Caputo said earlier, above our pay grade, which is the right thing to do, because other considerations would have needed to be taken into account in those conversations. There was an agreement between the parties that this motion would be supported.

There is, however, an opening to have a change in the date, which would be November 3. Apart from that, my understanding is that an agreement was achieved.

Monsieur Ramsay.

● (1315)

Jacques Ramsay: The information I'm getting is that we have an agreement that if things break down, if the clause-by-clause becomes too difficult, we can always suspend the meeting and take it up later on.

[*Translation*]

I don't know if Mrs. DeBellefeuille will like this option, but we can adjourn the meeting. That's not what we want. We want to move forward quickly, but if that's not possible, we will be reasonable, of course. We agree not to begin clause-by-clause consideration at the fourth meeting, but rather at the fifth meeting.

The Chair: Okay, so that's what I propose to do. We'll see how it goes, but if the schedule doesn't allow us to deal with clause-by-clause consideration in a single meeting, we'll discuss how to adjust the schedule.

[*English*]

I would seek consent for the amendment, which is replacing “October 29” with “November 3”.

(Amendment agreed to)

(Motion as amended agreed to [*See Minutes of Proceedings*])

The Chair: Good.

This leads us to the second motion that you alluded to, MP Ramsay.

[*Translation*]

Claude DeBellefeuille: Mr. Chair, I would like to speak.

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

Claude DeBellefeuille: I'm sorry, but I rarely give my consent when I don't understand.

Have you disposed of my amendment?

The Chair: Yes, your change about November 3 was taken into account.

Claude DeBellefeuille: My amendment proposed “November 3” and “four meetings”, as well as the change proposed in the last paragraph of my amendment. Have you disposed of my amendment?

The Chair: Look, we can also vote on your…. In fact, to try to—

Claude DeBellefeuille: I don't mind. We can work it out, Mr. Chair. The idea is that it needs to be clear for everyone, especially the clerk. At the end of the meeting, what exactly have we agreed on? I think there's consensus on the date of November 3.

The Chair: Absolutely.

Claude DeBellefeuille: Did we also keep the proposal to hold “a minimum of four meetings”?

Jacques Ramsay: No.

Claude DeBellefeuille: Did we keep the proposal to hold only four meetings?

The Chair: Yes, that's correct.

Claude DeBellefeuille: Okay. That's perfect.

Jacques Ramsay: There's a possibility that we could negotiate adding a fifth meeting.

Claude DeBellefeuille: We're dealing with the amendment that I proposed, Mr. Ramsay, and we can't amend it. Is that correct? I agree with holding “four meetings” and amending my amendment by removing “a minimum of”, as I had indicated.

As for the last change put forward by my amendment, it proposes to amend the text of the motion so that clause-by-clause consideration begins at the fifth meeting, without limiting the number of meetings. Is that proposal being accepted?

The Chair: That's what was retained.

Claude DeBellefeuille: Perfect.

The Chair: Procedurally, we should have actually voted on your amendment, debated it, moved another amendment—

Claude DeBellefeuille: Yes, but at the moment, we're dealing with this amicably.

The Chair: —or a subamendment as a result of your amendment. It might have been more complete, but it would also have been more complicated procedurally.

We agreed on the amendment to Mr. Ramsay's motion to change the date from “October 29” to “November 3”. We agreed to maintain the proposal to hold “four meetings”, while taking into account Mr. Caputo's wish that the committee remain open to adding meetings based on the witnesses who will appear before the committee. It's also proposed that we hold a meeting two or four days after the fourth meeting to proceed with clause-by-clause consideration. Then we'll see how it goes, and the committee will decide if it wants to schedule more meetings for this clause-by-clause.

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

The Chair: Thank you.

Mr. Ramsay, the floor is yours.

Jacques Ramsay: I propose that we deal with Bill C-8 at our next meeting, if that's okay.

The Chair: Okay, if that's your wish.

Mrs. DeBellefeuille. The floor is yours.

Claude DeBellefeuille: Can the clerk send us the wording of the motion we agreed on to avoid confusion at the next meeting?

The Chair: Yes.

The Clerk: The text of the motion will appear in the minutes of the meeting.

Claude DeBellefeuille: Okay. Thank you.

The Clerk: I've just circulated the text of Mr. Ramsay's notice of motion for the next meeting on Bill C-8.

Claude DeBellefeuille: Perfect. Thank you very much.

The Chair: Okay.

Thank you very much, everyone, and good afternoon.