HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

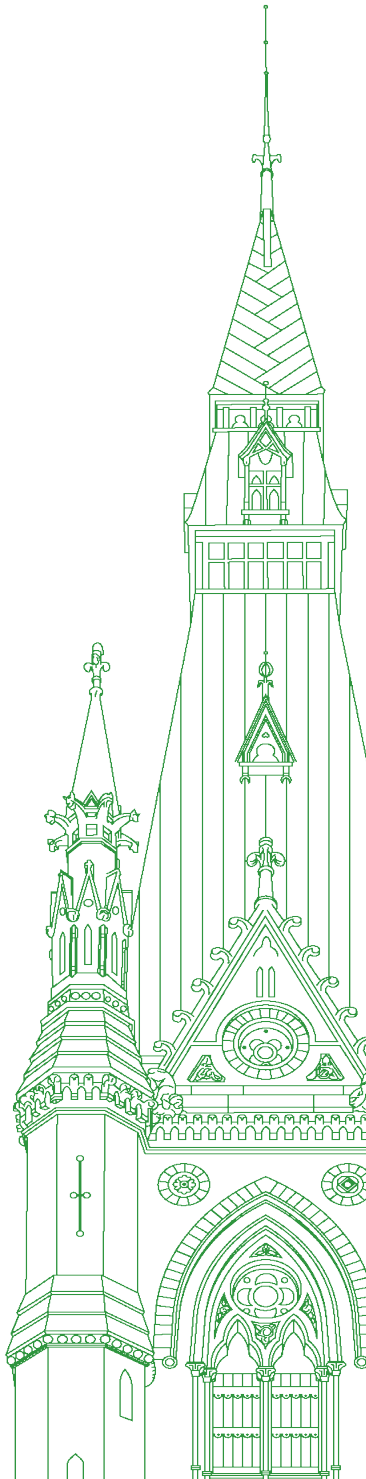
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 092

Monday, February 5, 2024



Chair: Mr. Heath MacDonald

Standing Committee on Public Safety and National Security

Monday, February 5, 2024

● (1555)

[*English*]

The Vice-Chair (Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC)): I call this meeting to order.

There has been some discussion since the last meeting about whether it was suspended or adjourned. The chair today—me—believes that we suspended last Thursday. There was a unanimous consent motion at the end of that meeting to continue the debate at the next meeting, so I'll continue with the UC motion on the floor and go to Mr. Motz.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): On a point of order, Mr. Chair, can you please pull up the ruling for a unanimous consent motion? That's number one.

Number two, through you to the clerk, in the minutes that he created, what does it say? Does it say that we suspended or adjourned the last meeting? What do the minutes say?

The Vice-Chair (Mr. Doug Shipley): The last meeting was adjourned, but our UC at the end of that, which we all voted on, was that we were going to continue with the discussion at our next meeting.

I see Mr. Julian has his hand up. Thank you for putting your hand up politely and asking for the floor. I appreciate that.

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

We have witnesses who are here, and I believe we need to hear from them. You'll recall that the last meeting was truncated and we weren't able to fully question the witnesses. We also have witnesses coming at 4:30, so I would suggest that we have that conversation off-line and proceed to questioning the witnesses.

The Vice-Chair (Mr. Doug Shipley): Do we have agreement that there was UC at the end of the last meeting to continue on?

You're shaking your heads. Did we not vote to continue debate? Does anyone want to debate whether we discussed and voted on that?

[*Translation*]

Ms. Kristina Michaud: I have a point of order, Mr. Chair.

I clearly remember hearing Mr. Motz say at the last meeting that he wanted us to adjourn debate on the motion he had introduced. That's my recollection. I may be wrong, but I don't recall a unanimous vote or unanimous consent to continue the discussion on this motion. In addition, we also had to question the witnesses who were here.

Today we have new witnesses. I think we could let them make their opening remarks.

The clerk could enlighten us on how the last meeting ended, but, as I recall, Mr. Motz himself asked to adjourn the debate on the motion he had moved.

[*English*]

The Vice-Chair (Mr. Doug Shipley): I think I see some other hands up on this point of order. I was definitely sitting in the room, and I definitely remember a UC motion that we all agreed on to let Mr. Motz carry on and to suspend to allow the witnesses....

Mr. Motz, you had your hand up.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): There are a couple of things. First, the original notice of meeting that came out for today on Friday afternoon was for committee business, resuming debate on my motion. An hour later—actually, 61 minutes later—a new notice of meeting came out. I don't know why the committee business was deleted. I suspect there must have been some pressure on the clerk, unfortunately, from somewhere to adjust it.

I'll take you back to the blues from the last meeting. Mr. Julian made an intervention about the witnesses, and I initially said to adjourn the motion. I then corrected myself to say to suspend the motion. That's where we were. The motion was not moved to adjourn. It was suspended. If you want to look at the blues, I encourage you to do so. That's where we are today, based on the history of the meeting last week.

The chair asked, “Is it the agreement of the committee?”, and the motion was agreed to. Then he said, “Okay. We'll go to our witnesses. We'll suspend for two minutes while our witnesses get in place.” That's what happened. That's all I can provide on the history of the last meeting.

● (1600)

The Vice-Chair (Mr. Doug Shipley): I have Mr. Lloyd next, and then Ms. O'Connell.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): I would just reiterate that Mr. Motz has the blues, and the blues were very clear. After Mr. Julian's suggestion that we suspend the meeting, there was unanimous consent to suspend it. That is my recollection of how the last meeting ended, and my full expectation is that we will resume exactly where we left off in the last meeting.

Thank you.

The Vice-Chair (Mr. Doug Shipley): We have Ms. O'Connell.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

Mr. Motz just made the point. He moved to suspend the debate. There was no clarification on when that debate would then continue. We moved on to Bill C-26. The meeting was not suspended; the meeting was adjourned.

There is a new notice of meeting. Therefore, if you would like to lift the suspended debate back to the floor, you would require a dilatory motion. It doesn't just continue, because the meeting was adjourned and the debate was suspended. However, there was no time and place given, and there was no agreement that it would start off at the beginning. If you can point that out in the blues, I'm happy for you to read that, but I know it doesn't exist.

Therefore, you require a motion to bring the suspended debate back to the floor. Otherwise the notice of meeting is here, and that's what we move forward on, because the meeting itself was adjourned.

Again, we have witnesses here. The Conservatives don't seem to care about safety. I find it interesting, Mr. Chair, on this point, that today we're seeing historic snowfalls in Atlantic Canada, where Canadians, the people there and in Cape Breton in particular, are worried about being able to get out, being able to access resources. In Bill C-26, actually part of this legislation deals with ensuring the sustainability of telecoms so that in the event of a natural disaster, like what we're seeing in Atlantic Canada right now, there are literal lifelines still available—

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell, we're still on the points of order, not debate.

Ms. Jennifer O'Connell: That's right, and I have the floor. I'm talking about—

The Vice-Chair (Mr. Doug Shipley): I know, but it sounded like debate. Can you make the point of order, please?

Ms. Jennifer O'Connell: Oh, I guess the chair and the Conservatives think it's debate to talk about the safety of Atlantic Canadians and the very legislation we're trying to deal with, which would actually create a system to ensure that in events like this their telecoms are protected.

Mr. Dane Lloyd: I have a point of order, Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): We're literally on a point of order right now.

Ms. Jennifer O'Connell: If you want to move a dilatory motion not to go to Bill C-26 and deal with that, then I think you can explain that to Atlantic Canadians today, too.

The Vice-Chair (Mr. Doug Shipley): We have a couple more hands up on this issue.

Maybe I can ask the clerk, because I got a little confused too. How were those two different meeting notifications given out so closely and yet they were so different? Could you please clarify that for us?

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Mr. Chair, on the same point of order—

The Vice-Chair (Mr. Doug Shipley): I'll get you on the list, Mr. McKinnon.

The Clerk of the Committee (Mr. Simon Larouche): The clerks follow the instructions of the chair unless there's any indication from the committee on what to put on the notice of meeting.

● (1605)

The Vice-Chair (Mr. Doug Shipley): Okay, so you were reinstructed to make a second one, to get that out.

The Clerk: Yes, I followed the chair's instructions for the notice of meeting.

The Vice-Chair (Mr. Doug Shipley): Mr. Motz, I have you next.

Mr. Glen Motz: Thank you, Chair.

I just want to clarify again in the blues. When we were talking about whether it was a suspension or an adjournment, I had the floor on the motion. I said, “I did not move a motion. I'm agreeing with him [Mr. Julian] to get to Bill C-26 for the remainder of our meeting today and I'll pick this up at the next meeting.” That's what I said. Then the chair said, “Is it the agreement of the committee?” Then the motion was agreed to.

As I understand the rules, that motion, the conversation about that motion and the debate on that motion were suspended from the last meeting, and we went on to the witnesses.

Now, today, in order to wrap up that motion, I have a couple of comments I wish to make that should take no longer than 15 minutes or so. Then we have other speakers on that list. If they wish to continue to speak, then that's certainly their choice. As I understand the situation from the last meeting, we were into a suspension on the motion, and because of Mr. Julian's intervention, I agreed to let those witnesses at that time.... I gave up the floor on a suspension to deal with that.

Thank you, Chair.

The Vice-Chair (Mr. Doug Shipley): Thank you.

If we had gone right into your comments, we'd probably be wrapping up right now and moving on.

Mr. McKinnon, you have the floor.

Mr. Ron McKinnon: I don't know what was in the mind of the chair as he made these preliminary schedules, but I think he had a hard think about what went on and decided this was more appropriate.

I think that whether or not we suspended or adjourned that motion or that discussion becomes moot if we realize that Mr. Motz or someone else could move the motion again when the time comes, but I wonder if we could have an agreement to hear from the witnesses first and have at least one round of questions for the witnesses before we do so.

That would be a suggestion to Mr. Motz.

The Vice-Chair (Mr. Doug Shipley): It sounds like probably a good compromise to me, but we'll see what Ms. O'Connell says.

Ms. Jennifer O'Connell: Mr. Chair, I move that we move to the business of Bill C-26.

The Vice-Chair (Mr. Doug Shipley): So you're not agreeing with Mr. McKinnon's compromise.

Ms. Jennifer O'Connell: I move my motion that we move to the business of Bill C-26.

The Vice-Chair (Mr. Doug Shipley): I'll ask the clerk for a recorded vote on that, please.

(Motion agreed to: yeas 6; nays 4)

The Vice-Chair (Mr. Doug Shipley): We will start with Bill C-26.

I have a nice preamble here to introduce everybody. To save some time and to give you folks a little bit more time, maybe you could—I know this is very informal—say your name at the beginning of your five minutes, and that will hopefully give you guys a little bit more time, because we've already lost some time going into this.

We will start with our witnesses.

Mr. Shipley, do you want to go first? It rolls off the tongue nicely, doesn't it, Mr. Shipley?

Mr. David Shipley (Chief Executive Officer, Beauceron Security): Good afternoon.

My name is David Shipley, and I'm the chief executive officer and co-founder of Beauceron Security Inc. I'm also the co-chair of the Canadian Chamber of Commerce's cyber council. I'm a proud Canadian Forces veteran, having served with the Canadian Army Reserve in the 8th Canadian Hussars.

I'm not a computer scientist. My expertise and perspective today are based on my experience as CEO and co-founder of Beauceron. I do not see cybersecurity as a technological issue. It's a people and business risk issue.

I founded Beauceron Security in 2016. We now serve more than 750 organizations in Canada, the United States, Europe and Africa. We have helped more than 650,000 people learn how to spot, stop and report cyber-attacks. Beauceron Security has demonstrably reduced individual and organizational cyber risk. Our made-in-Canada solution is used by global banks, national telecommunications carriers, educational institutions, health care facilities, government and small business.

We live in a world where North Korean hackers steal billions of dollars of cryptocurrency to fund their nuclear weapons programs. Something that 25 years ago would have sounded too far-fetched to be even the plot of a James Bond movie is an all-too-real reality and is contributing to global instability today. It's also a world where a Canadian federal government IT worker by day becomes one of the most successful ransomware affiliates by night, making millions of dollars as a digital extortionist for an international criminal gang.

I share these real-life examples because they highlight the first point I want to make. When it comes to cyber, anything, even the bizarre, is not just possible but it is the norm. The challenge of managing cyber risk is to balance the incredible creativity of humans with the unpredictability of complex digital systems.

I know that for many this topic can be overwhelming. Many feel that they do not have the technical background to think about these issues. You may also feel, as legislators, that it is difficult to wrestle with this law.

However, please, this is not a technology issue. Throughout my career in cybersecurity and as a CEO of Beauceron, the root cause of every single cyber incident our customers and we have ever helped investigate has always been traced back to a combination of people, process, culture and technology. Cybersecurity has never been about technology alone, and it can never be solved by technology alone. The story is, has always been and will continue to be about the relationship between technology, people and control—which is, by the way, the actual meaning of the word “cyber”.

Reducing cyber risk to Canadians will require legislation and a regulatory regime tailored and developed collaboratively with industry. These regulations and directives must look at people, process, culture and technology-based risk controls.

I support the need for this legislation. We need this law now more than ever. We are far behind our allies, and we are risking the safety and prosperity of Canadians every day we delay. This legislation and the accompanying regulatory regime must ensure that a proactive, positive security culture is instilled and maintained within Canada's critical infrastructure firms. With some fine-tuning, I believe it can accomplish these goals.

I support the recommendations put forward by the Canadian Chamber of Commerce to improve the bill to ensure fairness, effectiveness and proportionality of the proposed legislation. In addition to their recommendation, I urge this committee to look at the following issues.

Number one, add due diligence defences to the proposed administrative monetary penalties. We need to create positive reasons to invest in security and compliance with legislation, and not just negative consequences for failure.

Number two, remove personal liability for individuals. At a time when the cybersecurity labour shortage is most acute, and when as many as 75% of the most senior cybersecurity leaders are considering a career change out of cybersecurity, adding a target on their heads will only make things worse and subvert the objectives of this legislation.

Number three, ensure regulators charged with creating industry-specific cybersecurity directives have the skills required to do so effectively. While regulators such as the Office of the Superintendent of Financial Institutions are experienced, others are being given responsibility for cyber for the first time. This legislation should require government collaboration with industry, such as what has already been done with the Canadian security telecommunications advisory committee.

● (1610)

Lastly, considering the recent news about Global Affairs, this legislation should limit the amount of sensitive data collected by regulators about cybersecurity defences of Canadian critical infrastructure, lest we inadvertently create a one-stop shop for hostile nation-states and criminals to learn how to cripple these vital sectors and firms.

The opportunity before you with Bill C-26 is to ensure that the Canadian people—

● (1615)

The Vice-Chair (Mr. Doug Shipley): Mr. Shipley, are you just about wrapped up?

Mr. David Shipley: I'm just about wrapped up.

It's to ensure that the Canadian people, through Parliament, are in control of the technologies they rely on for the functioning of our society—not the technology itself, not the technology companies, and certainly not our adversaries.

Thank you.

The Vice-Chair (Mr. Doug Shipley): Thank you.

We will now go to Ms. Bahr-Gedalia.

Thank you.

Ms. Ulrike Bahr-Gedalia (Senior Director, Digital Economy, Technology and Innovation, Canadian Chamber of Commerce): Mr. Chair and members of the committee, good afternoon. My name is Ulrike Bahr-Gedalia, and I'm the senior director of digital economy, technology and innovation at the Canadian Chamber of Commerce. I'm also the Canadian Chamber's architect and policy lead for the digital economy committee's future of artificial intelligence council and the “Cyber. Right. Now.” council.

As Canada's largest and most activated business network, representing over 400 chambers of commerce and boards of trade and more than 200,000 businesses of all sizes from all sectors of the economy and from every part of the country, the Canadian Chamber is pleased to have this opportunity to provide feedback on Bill C-26.

Our “Cyber. Right. Now.” council has been calling on government to prioritize cybersecurity and focus on a prevention-first approach and improved information sharing for close to three years. Today I'd like to share a few key recommendations and why cybersecurity is important to the Canadian Chamber and our members within the Canadian economy.

Over 98% of Canadian businesses are small or medium-sized enterprises. SMEs need greater cybersecurity threat awareness, protection and training to utilize the full suite of tools at their disposal and to keep Canadians safe from bad actors. Like other countries, Canada is facing an increasingly complex and risk-prone digital landscape. With a cybersecurity skills gap of some four million people globally, and an ever-increasing number of connected devices—at least 67 billion and counting—the challenges and costs associated with securing our digitally enabled world are increasing. But while every organization of every size and in every sector is at risk of a cyber breach, few carry the same real-world risk of a crippling cyber-attack as those in the critical infrastructure sector. This threat will only grow as our critical infrastructure increasingly relies on software and connected technology to power and support its operation.

We are pleased to see Bill C-26 proceed to committee study, and we support the bill overall. However, certain amendments are needed to ensure that the bill reaches its full potential. More specifically, our telecommunication members have expressed their concerns with respect to a few provisions in the Telecommunications Act, such as the lack of a due diligence defence for violations under section 15 in part 1, resulting in monetary penalties, and the extent of ministerial order-making powers. I will note that this defence is present elsewhere in Bill C-26, such as in relation to cyber directions in part 2, the CCSPA, as well as full due process for and parliamentary oversight of ministerial orders. I encourage the committee to reach out to the telecommunication providers, as it's important to hear from them first-hand.

With respect to the CCSPA, our members are seeking the following improvements.

The first is a clearer definition of a reportable cybersecurity incident. This will ensure that industry isn't forced to report events that do not pose a material threat to a vital system. Failure to clearly define the parameters for a reportable incident will undermine the purpose of Bill C-26 and overwhelm government authorities, who will have to process and assess each cyber incident reported.

The second is allowing for a 72-hour reporting period for cybersecurity incidents, as opposed to immediate reporting. Allowing for reporting within 72 hours provides organizations the time to investigate, and will harmonize with existing regimes, such as in the United States, one of our key trading partners.

Finally, two-way information sharing is crucial. As currently drafted, the CCSPA only contemplates one-way information sharing from designated operators to the government. We believe this is a missed opportunity and a potential weakness, and it underscores the prevention-first approach I noted earlier. The more information we have, the more we can work together and the better we can help prevent incidents.

Thank you for listening and for the opportunity to participate in the study of Bill C-26.

● (1620)

The Vice-Chair (Mr. Doug Shipley): Thank you for that.

Next we will go to IBM Canada. We have Ms. Daina Proctor and Mr. Tiéoulé Traoré.

Whoever wants to go, you have five minutes.

[*Translation*]

Mr. Tiéoulé Traoré (Government and Regulatory Affairs Executive, IBM Canada): Thank you, Mr. Chair.

[*English*]

I'm Tiéoulé Traoré. I'm the head of government and regulatory affairs for IBM Canada. On behalf of IBM Canada, I would like to thank this committee for the opportunity to testify on Bill C-26, and more specifically on part 2, the focus of our testimony.

The digitization of the global economy has increased the need for government and businesses to protect themselves from constantly evolving cyber-threats. Strong cybersecurity protocols should be viewed as digital foundations for all entities seeking to maximize the power of tools such as cloud, AI, and quantum computing.

[*Translation*]

IBM Canada fully supports the principles of Bill C-26.

Indeed, Canada must ensure that its critical infrastructure is properly protected from cyberthreats. The skyrocketing number of cyber-attacks is a global phenomenon that does not spare our country, so action is crucial.

However, to maximize the real impact of Bill C-26, we argue that it should be amended by this committee. The focus should be on three points: clarifying definitions, aligning the bill with international standards and avoiding potential excesses.

[*English*]

My colleague Daina Proctor will now go through each recommendation.

Ms. Daina Proctor (CyberSecurity Service Line Executive, IBM Canada): Thank you.

My name is Daina Proctor. I'm the Canadian cybersecurity executive with IBM Canada, and it's a pleasure to be with you today speaking on the topic of Bill C-26.

There are three items that I would like to talk about with you today.

The first one is clarifying the core definitions within Bill C-26. Currently, Bill C-26 leaves much of the scope of the legislation to regulations. We believe it's critical to clarify the scope and the definitions in the legislation itself rather than delegate to the regulatory processes. Key terms used in the proposed law, such as “designated operators”, “confidential information” and “security incident”, are either too broadly described or not adequately articulated. We believe this committee should aim to address these definitions as much as possible, as this will enable a common understanding, increase enforceability and speed up the review when it comes time to draft the ensuing regulations.

Second is alignment with international standards. Canada's strategy and approach should be inserted into the collective efforts of our international community. As drafted, Bill C-26 carries various provisions that are not aligned with other mature cybersecurity regimes. The legislation does not differentiate between security levels of breaches. Furthermore, it includes potential incidents within the scope of its incident-reporting obligations, which could serve to overwhelm regulators with unnecessary and unhelpful information and place an unnecessary burden on industry.

The legislation's “immediate” reporting of cyber incidents, without a formal definition as to what would constitute “immediate”, is also problematic. Most jurisdictions allow for a 72-hour reporting window to allow injured parties to understand what has transpired, which in turn ensures that regulators receive a comprehensive report about actual findings.

The court has unfettered and overly broad jurisdiction when, under an act, it can impose criminal conviction, imprisonment terms, uncapped fines and personal liability, with administrative monetary penalties in the amount of $15 million that can accrue. This represents an entirely new regime and significant penalties far above those under other comparable pieces of legislation. The severity of such penalties and the enforcement action that may be taken will invariably create a chilling effect. Respectfully, the enforcement action that may be taken against individuals should be removed, or to the extent that such liability is considered necessary and proportionate, at a minimum there should be a defined standard to demonstrate the objective and substantiated culpability.

Last is avoiding government overreach. While IBM recognizes the need for compliance oversight, we specifically suggest clarification and refinement of the authorized powers belonging to the regulatory authority or persons who have the ability to enforce the provisions: namely, the ability to attend facilities, examine documents and records, and mandate internal audits, as well as unilateral broad discretion to impose remedial actions—all of these. We strongly encourage that these regulatory authorities and government access rights be limited in their scope and limited to certain critical situations that meet specific non-compliance thresholds.

In conclusion, IBM believes that the clarity around key definitions, enhanced harmonization with international standards and clear safeguards from potential government overreach would strengthen Bill C-26's mandate.

Thank you for your time. We welcome and look forward to addressing your questions.

● (1625)

The Vice-Chair (Mr. Doug Shipley): Thank you for that.

You must have been practising a little bit because that was almost exactly five minutes. Good job.

We'll start off with questions.

Mr. Motz, I believe you're up first.

Mr. Glen Motz: Thank you very much.

Thank you to the witnesses for their testimony and for being here today.

One thing that you probably noticed at the front of this meeting is that we have been seized with the decision from the Federal Court, where the Federal Court found that the Trudeau government's use of the Emergencies Act was illegal and unconstitutional. As a result, we have been having that conversation here.

I know this might derail the questions to the witnesses, but I'd like to move a motion, Mr. Chair, please, that is duly on record and presented to the committee.

I move:

> That, in light of the recent Federal Court ruling which found that the government's use of the Emergencies Act in February 2022 to have been illegal and that the special criminal laws subsequently created by the Liberal Cabinet to have been an unconstitutional breach of Canadians' Charter rights, the Committee undertake a study of 7 meetings, pursuant to Standing Order 108(2), of the Department of Justice's role in supporting the government's illegal and unconstitutional decisions concerning the Emergencies Act, together with the consequences which follow the Court's decision, provided that
>
> (a) the Committee invite the following to appear, separately, as witnesses, for at least one hour each:
>
> (i) the Honourable David Lametti, the Minister of Justice and Attorney General of Canada at the time,
>
> (ii) the Honourable Marco Mendicino, the Minister of Public Safety at the time,
>
> (iii) the Honourable Arif Virani, the Minister of Justice and Attorney General of Canada,
>
> (iv) representatives of the Canadian Civil Liberties Association, and
>
> (v) representatives of the Canadian Constitution Foundation; and
>
> (b) an order do issue for all legal opinions which the government relied upon in determining that
>
> (i) the threshold of "threats to security of Canada", as defined by section 2 of the Canadian Security Intelligence Service Act, required by section 16 of the Emergencies Act, had been met;
>
> (ii) the thresholds required by paragraphs 3(a) or (b) of the Emergencies Act, concerning a "national emergency" had been met;
>
> (iii) the situation could not "be effectively dealt with under any other law of Canada", as required by section 3 of the Emergencies Act;
>
> (iv) the Emergency Measures Regulations were compliant with the Canadian Charter of Rights and Freedoms, including the analysis relied upon by the Minister of Justice in discharging his responsibilities under section 4.1 of the Department of Justice Act, and
>
> (v) the Emergency Economic Measures Order was compliant with the Canadian Charter of Rights and Freedoms, including the analysis relied upon by the Minister of Justice in discharging his responsibilities under section 4.1 of the Department of Justice Act,
>
> provided that these documents shall be deposited with the Clerk of the Committee, without redaction and in both official languages, within seven days of the adoption of this order.

Mr. Chair, I think it's important that Canadians at least have a brief summary—

Mr. Ron McKinnon: I have a point of order, Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): Yes, Mr. McKinnon.

Mr. Ron McKinnon: With apologies to Mr. Motz, I would renew my concern, as expressed when this was last moved, that this exceeds the powers of this committee. I understand that this matter was taken under advisement and will be reported back at some time once wiser heads have been able to wrestle with it.

I would like to put that on the record.

The Vice-Chair (Mr. Doug Shipley): Since we have different chairs today, I'm not sure where he is on that decision.

We'll let Mr. Motz continue now.

Thank you.

Mr. Glen Motz: Thank you, Mr. Chair.

As I was saying, I think it's important that Canadians at least have a brief overview of this particular order—

Ms. Jennifer O'Connell: I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell.

Ms. Jennifer O'Connell: Thanks.

Can I get a clarification on what motion Mr. Motz is moving? Is this the same as the other day, or is this a new one?

If so, can you point to which motion it is? There were, like, six motions tabled.

The Vice-Chair (Mr. Doug Shipley): The clerk is indicating to me that it's the notice of motion from Mr. Motz dated Tuesday, January 30, the 1.1 Emergencies Act motion.

Ms. Jennifer O'Connell: Is it the same one that Mr. Motz moved at the last meeting?

The Vice-Chair (Mr. Doug Shipley): No, it is a different motion.

Ms. Jennifer O'Connell: Okay. That's what I wanted to clarify.

Thank you.

The Vice-Chair (Mr. Doug Shipley): Go ahead, Mr. Motz.

Mr. Glen Motz: Thank you, Chair.

As I was saying, maybe the third time is the charm. Canadians need to understand and deserve to understand a summary of the decision, at least for today: what the decision was and how the Mosley decision impacts the government.

As we know, on January 23 of this year, the Federal Court of Canada released its historic decision from the judicial review of the Trudeau government's invocation of the Emergencies Act and the regulations made under it in response to the 2022 "freedom convoy".

We all know that the Emergencies Act is extraordinary legislation that upends our normal constitutional order and grants sweeping powers to the Prime Minister and cabinet, including the power to create new criminal laws at the stroke of a pen. The Emergencies Act had never been invoked before February 14, 2022, and its use against mostly non-violent protesters concerned about the federal COVID-19 policies and mandates was disturbing and is disturbing.

Many Canadians, myself included, believed all along that the decision was illegal. We believed that the high threshold to invoke the act, which is a tool of last resort, was not met. We believed that the new criminal laws created by cabinet under this act, which prohibited attending convoy protests and even froze bank accounts without reason to suspect a crime had been committed, were unconstitutional.

Justice Mosley found that the high threshold to invoke the act was not met, because there was no national emergency and there was no threat to the security of Canada as defined by the legislation. The regulations violated the charter rights and freedoms of expression and security against unreasonable search and seizure, and those limits were not justified.

I'll go through a few of the points that Justice Mosley spoke about. The bottom line is that his opinion, his decision was that cabinet was not owed extraordinary deference when interpreting the act. One of the more galling claims by the government was that cabinet is owed near total deference when it comes to anything to do with an emergency. Justice Mosley rejected the government's proposition, finding that, while cabinet is owed deference because it needs to respond to fluid situations quickly, there is no untrammelled discretion, and cabinet is nonetheless constrained by the objective thresholds written into the statute.

Second, there was no national emergency within the meaning of the act. To invoke the act, there must be a national emergency. If the effects of the emergency do not extend to the whole of Canada, the area to which they do extend must be specified. The Trudeau government claimed that the emergency existed throughout Canada. Justice Mosley called this “an overstatement” and found that the provinces were able to deal with the situation using existing laws such as the Criminal Code.

In paragraph 248 of his decision, Justice Mosley says, “the Proclamation stated that it 'exists throughout Canada'. This was, in my view, an overstatement of the situation known to the Government at that time.” He also says that “the majority of the provinces were able to deal with the situation using other federal law, such as the Criminal Code, and their own legislation.”

He goes on to talk about the Emergencies Act as a tool of last resort. Justice Mosley affirmed the Federal Court decision that the Emergencies Act is a tool of last resort. In paragraph 253 of his decision, he states:

> Due to its nature and to the broad powers it grants the Federal Executive, the Emergencies Act is a tool of last resort. The GIC cannot invoke the Emergencies Act because it is convenient, or because it may work better than other tools at their disposal.... And in this instance, the evidence is clear that the majority of the provinces were able to deal with the situation using other federal law, such as the Criminal Code, and their own legislation.

● (1630)

The next area that he talks about is that there were no “threats to the security of Canada” within the meaning of the Emergencies Act. Justice Mosley found that there was no threat to the security of Canada within the meaning of the act. The act says those words have the same meaning as in the CSIS Act, which includes the threat of “serious violence against persons or property”. Justice Mosley noted that the head of CSIS did not believe that definition was met. The only specific example of threats of serious violence provided was about weapons uncovered at Coutts, but that situation had already been dealt with by the RCMP using the Criminal Code before any of the extraordinary regulations were created.

Justice Mosley moves on to the economic harm. He suggests that the economic harm was not part of the threshold to invoke the act. The government claimed during the Rouleau commission, during the Federal Court hearings and in press conferences following their loss that a threat to the security of Canada can include economic harm, like damage to supply chains. Justice Mosley found that the harm being caused to Canada's economy, trade and commerce, although concerning, did not constitute threats or the use of serious violence to persons or property, as required by the CSIS Act's definition.

He goes on to say, in paragraph 296 of his decision:

> the test for declaring a public order emergency under the EA requires that each element be satisfied including the definition imported from the CSIS Act. The harm being caused to Canada's economy, trade and commerce, was very real and concerning but it did not constitute threats or the use of serious violence to persons or property.

Justice Mosley goes on to talk about the attendance and the issues that are illegal not only by the act but also by the Constitution. Banning mere attendance at protests violates the freedom of expression under the charter. Justice Mosley suggested that the regulations limited the right to freedom of expression guaranteed by paragraph 2(b) of the charter by banning anyone attending an assembly “that may reasonably be expected to lead to a breach of the peace”, rather than simply prohibiting conduct like blockades and excessive honking.

The violation of expression, Justice Mosley found, was not a reasonable limit. Justice Mosley ruled that the measures that infringed upon paragraph 2(b) could not be upheld under section 1 of the charter—

● (1635)

[*Translation*]

Ms. Kristina Michaud: I have a point of order, Mr. Chair.

[*English*]

The Vice-Chair (Mr. Doug Shipley): Mr. Motz, wait just one moment, please.

Ms. Michaud, you have a point of order.

[*Translation*]

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

Mr. Motz seems to want to read the entire text of the judge's decision. At our last meeting, he didn't give his colleagues an opportunity to speak to his motion. I don't know if he intends to do the same thing today. I guess we won't have time to ask the witnesses questions.

I'm wondering if he can tell the committee how long he intends to speak on this. We must not waste the witness' time. They made the effort to come here to give us their comments on Bill C-26.

If not, I will move that we vote on Mr. Motz's motion so that we can get back to studying the bill. That said, I don't know if he agrees with my proposal.

[*English*]

The Vice-Chair (Mr. Doug Shipley): Thank you for that point of order.

I'll ask Mr. Motz.

Mr. Motz, do you have any idea how much longer you will be?

Mr. Glen Motz: I will probably be five to eight minutes at the most.

The Vice-Chair (Mr. Doug Shipley): Okay, we'll let you continue.

Mr. Peter Julian: Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): Yes, Mr. Julian.

Mr. Peter Julian: On a point of order, I think the way this committee has dealt with issues in the past is to have discussions offline and come back to committee. I have amendments I'd like to offer to the motion, possibly. I think this is something we could have a full committee meeting on.

I am conscious of the fact that we have costs that have gone to the Canadian taxpayer and witnesses who are offering important testimony on a bill that is vitally important and that has languished now for almost two years. It is, I believe, our responsibility to question the witnesses. I would ask if Mr. Motz would just suspend his discussions so that we can have some talks off-line and question the witnesses, which was really the intent of this meeting today.

I think we could probably come to a consensus in the coming days, prior to the next meeting.

The Vice-Chair (Mr. Doug Shipley): Mr. Julian, thank you very much for that.

Unfortunately, Mr. Motz does have the floor. I will reiterate that Mr. McKinnon did bring up a nice concession earlier that was not agreed to.

Mr. Motz, I can't direct you in this, but if you could wrap it up within five minutes or so, it would be nice to get back to the witnesses. It's up to you, and the floor is yours.

● (1640)

Mr. Glen Motz: Thank you very much.

To Mr. Julian's point, I thought I had a gentleman's agreement with the committee the last time that was proposed, and that certainly got tossed. I will finish within five to seven minutes, Chair, and thank you.

As I said, the violation of the freedom of expression was not a “reasonable” limit, as Justice Mosley ruled. Those measures infringing on paragraph 2(b) could not be upheld under section 1 of the charter, which allows for “reasonable limits...as can be demonstrably justified in a free and democratic society.”

He found that the measures were “not minimally impairing” in two ways. First, they were applied throughout Canada when they could have been limited to Ontario, and possibly Alberta. Second, there were less-impairing alternatives available that the government was constitutionally required to select over the measures they chose.

He got into the freezing of bank accounts, and he ruled that it violated the right to be free of unreasonable search and seizure. Justice Mosley also ruled that the measures ordering banks to disclose banking information of persons designated by the RCMP and freezing their accounts violated the right to be secure against unreasonable searches and seizures under section 8 of the charter.

The searches of bank records were not reasonable because they required banks to inform the RCMP if they had any reason to believe someone was materially assisting the protest, when a search normally requires that police prove to a third party on an objective standard, like reasonable suspicion or reasonable grounds to believe, that a crime had been committed before the search takes place.

In paragraph 337 of his decision, Justice Mosley says, “The absence of any objective standard was confirmed by Superintendent Beaudoin, who...acknowledged in cross-examination that the RCMP did not apply a standard of either reasonable grounds or a standard of reasonable suspicion, and all they required was 'bare belief'.” In paragraph 341, Justice Mosley goes on, “I find that the failure to require that some objective standard be satisfied before the accounts were frozen breached s. 8” of the charter.

Lastly, I would note in a brief overview that the search and seizure violation could not be justified under section 1 of the charter either. Justice Mosley found that there was no threat to the security of Canada within the meaning of the act. The act says those words have the same meaning as in the CSIS Act, which includes the threat of “serious violence against persons or property”. Justice Mosley noted that the head of CSIS did not believe that the definition was met. The only specific example of threats of serious violence, as I said previously, was provided through weapons uncovered at Coutts, but that situation was already dealt with by the RCMP using the Criminal Code before any of the extraordinary measures were created.

I wrap up by saying this, Chair. I think it's important that Canadians recognize that this government—although many Canadians felt the same way—had extended beyond lawful authority. They can't change the law to suit their own purpose that's convenient for them. Finally, now a Federal Court has ruled that they did, in fact, extend beyond the confines of the law and they did, in fact, breach the charter.

I think it behooves this committee to look at this issue or come to some agreement on how it would be best dealt with, moving forward.

With that, Chair, I will cede the floor to the next speaker.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Motz.

I have Ms. O'Connell next on the speakers list.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

I move that we adjourn debate.

The Vice-Chair (Mr. Doug Shipley): Okay.

Would you like a recorded division, Ms. O'Connell?

Ms. Jennifer O'Connell: Yes.

The Vice-Chair (Mr. Doug Shipley): I would ask the clerk to take a recorded division, please.

(Motion agreed to: yeas 6; nays 4)

The Vice-Chair (Mr. Doug Shipley): We will move on and get back to Bill C-26.

We'll start with six minutes for questions.

I believe Mr. McKinnon is first.

● (1645)

Mr. Ron McKinnon: Thank you, Mr. Chair.

I would like to welcome our witnesses here. Thank you for being here, and for all the time and effort you have put into this bill so far.

I'm going to start with Mr. Traoré and Ms. Proctor. You indicated that this legislation should align with international standards. Is there a specific international standard that you can specify?

Ms. Daina Proctor: Thank you, Mr. McKinnon. I appreciate the question.

There are a number of international standards that we would rely upon. If I dare say, I would look forward to and welcome the opportunity to share with you what those international standards are during a more working session. For this debate and this discussion right now, the points I would draw out are certainly the definitions, the response times and the punitive nature of the responses.

The 72 hours on a specific incident being responded to—but a set severity of incident—would be a particular item of interest. Then there are the punitive aspects. The punishment of an individual for the infractions is a stretch too far, which I have not seen any other international regulations go towards; they go towards corporations. The accrual aspect is equally far.

Mr. Ron McKinnon: Do these comments pertain to the international standards, or are they part of your other...? You mentioned them already. Is this a matter of adhering to those standards to clarify those definitions and obligations?

Ms. Daina Proctor: I'm sorry. Can you repeat the question, Mr. McKinnon?

Mr. Ron McKinnon: At some point we'll have to submit amendments to this bill. You indicated that we should adhere to international standards. It would be helpful if we had specific standards that we should adhere to. Are those standards sufficiently encompassing, or do they go too far? If you could clarify both of those aspects, it would be helpful.

Mr. Tiéoulé Traoré: We will make sure to get back to you with proposed amendments and examples of what we see as frameworks to achieve.

Mr. Ron McKinnon: You're concerned about definitions. Would that be assuaged with adherence to these standards?

Ms. Daina Proctor: Perhaps I can clarify that as well. My apologies if, during my opening statement, I indicated otherwise. Adherence isn't necessarily the encouragement that we would be offering. It's more that a number of aspects of Bill C-26 are much more far-reaching than established international standards for mature cybersecurity regimes, of our allies in particular.

It's not necessarily adherence to them, but more a recognition that we don't necessarily need to go beyond what they're already working towards in their private and public partnership and enablement of the industry.

I hope that gives a little bit of clarification. It's not necessarily an alignment to international standards, but a “not going farther than”, as we try to work together to bolster our critical infrastructure.

Mr. Ron McKinnon: These standards basically establish a border within which we ought to operate.

Ms. Daina Proctor: That's a good way to put it.

Mr. Ron McKinnon: Could we clarify what the risks are that we leave ourselves open to if this legislation does not pass?

I open this to everyone.

Go ahead, Mr. Shipley.

Mr. David Shipley: I draw your attention to April 2023, when a Russian-linked hacking group successfully penetrated a Canadian natural gas pipeline provider and was “able to increase valve pressure, disable alarms, and make emergency shutdowns.” By the way, this Russian hacking team wasn't even their best, so that's what we're risking when we fiddle while Rome burns on cyber-legislation.

I'm not saying we're going to have a Hollywoodesque total society shutdown. I'm saying people could get killed. I'm saying businesses could be negatively impacted economically. I'm saying there are people who want to throw a punch and hit us right in the nose. We are sticking our face up, without an ability to defend ourselves, and it's going to hurt.

Mr. Ron McKinnon: How would this legislation stop that kind of attack?

Mr. David Shipley: First, we have to walk before we can run. Let me put this into very clear terms: Canada is not even crawling when it comes to defending itself. If you want to look at a leader right now, look at Australia. We are lagging, and it's not going to be business that pays the price. It's going to be everyday Canadians.

Every time there's a cyber incident, it contributes to the cost of living crisis in this country. We need to get moving on this, and we need to get it right. The flaws in this legislation that have been pointed out are significant. They will set us back. Instead of making things better, we're going to make them worse.

● (1650)

Mr. Ron McKinnon: I'm not sure how much time I have left.

The Vice-Chair (Mr. Doug Shipley): You have just a little over a minute.

Mr. Ron McKinnon: We'll chance for two minutes, Ms. Bahr-Gedalia, if you'd like to weigh in on these questions as well.

Ms. Ulrike Bahr-Gedalia: Mr. Shipley started with one example.

If you think about cyber incidents and threats, I don't think we can even keep up with any records and reporting in terms of how many there are a day. MP O'Connell, you mentioned Atlantic Canada, the Newfoundland health care infrastructure that was impacted as well. It's a snowball effect. If one portion of critical infrastructure gets impacted, it impacts our economy and society, and it also impacts how foreign direct investment will happen in the future. How do foreign entities see us? Do they want to settle in Canada? Do they want to build a future here as businesses, as communities and as talent?

I see it as a two-way.... While we have trouble in front of our own door, within the country, it is also on a global level. How do we get perceived and how do we best align ourselves and ensure that we are...? This is the cyber tag line right now: Lead the global cybersecurity future and be the most secure country on the planet. Canada can be that, and I think Bill C-26 is a step forward, but we need to speed it up a little, as it has already been in discussion for quite some time.

Thank you.

Mr. Ron McKinnon: Parliament proceeds at its own pace.

I think I'm out of time.

Thank you.

The Vice-Chair (Mr. Doug Shipley): Ms. Michaud, you're up next for six minutes.

[*Translation*]

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

I'd like to thank the witnesses for being here and for their patience.

Ms. Proctor and Mr. Traoré, you mentioned three important elements that seem essential to you in the context of this bill. Mr. McKinnon talked a little bit about the need to align with international standards, and I'd like to hear more about that as well. This is going to take a little bit of a longer discussion.

You also talked about the need to clarify the definitions in the bill, because there's a lot of room for regulations at the moment. That's more or less my understanding of the bill: it gives a lot of power to the Minister of Industry and the Governor in Council to make orders, and when I read it in its current form, I get the impression that it could go all over the map. It gives a lot of powers, but it's not really clear what the ministers could invoke, or what they could ask companies to do or force them to do.

So you're proposing that certain definitions be clarified, which could help to provide a framework for the government's actions later. I'd like to hear more about this.

Mr. Tiéoulé Traoré: There are two aspects to this. The first is the implementation of the bill and the regulatory framework. We all want the bill to be applied in the best way possible, of course. However, we find that some definitions leave room for interpretation. In cases where it's a major issue, we would prefer that the framework be much clearer so that people can comply with it more easily. Terms like “major incident” or “cybersecurity breach” are quite broad and generic. We find ourselves at an impasse. We think it's much simpler to clarify these terms now than to wait until the regulatory stage to establish definitions and end up in a bit of a mess when it comes to determining what to do. It's always better to clarify things right from the start.

The second aspect concerns government intervention. To be clear, we are committed to seeing the essence of the bill come to fruition, since cybersecurity breaches are a major issue. At IBM, we produce an annual report, and we've determined that the cost of a cybersecurity breach is $7 million per affected company, which increases to $12 million when the financial sector is involved. As a result, it's important to take action, and the government must show leadership in this regard. Its actions must also be well regulated, codified and predictable for the players in the system.

● (1655)

Ms. Kristina Michaud: Thank you.

Mr. Shipley, you talked about creating positive reasons for companies to implement a cybersecurity framework and inform the government. The government wants to force companies to do so under threat of monetary penalties.

Last week, a witness told us that tax incentives were needed. I asked him if we should switch things up, that instead of imposing monetary penalties, we should introduce tax incentives. He said no, that it was worth keeping the penalties for companies that didn't comply with the government's demands. Some companies may be concerned that this will create a lot of paperwork. So there's not a lack of willingness on the part of these companies to comply with these requests, but they are concerned about the delays and the costs that setting up such a framework could entail.

I imagine you consulted companies. What did you hear from them? Could a tax incentive be of interest to them?

Mr. David Shipley: Thank you for the question.

I apologize, my French isn't very good, so I'll answer in English.

[*English*]

The due diligence defence to the administrative monetary penalties is the first thing that becomes a positive thing. If I showed that we were in the spirit, trying to defend our organization, that we were doing what we should, that's a positive step that encourages me to invest, so I can show that. That's why it's so important that this gets addressed in the Telecommunications Act.

To be very clear, the Canadian private sector already spends $9 billion a year on cybersecurity, so we're not coming to Parliament and looking for a handout, for government to solve all problems. However, what's interesting is that this legislation deals specifically with very large enterprises and critical infrastructure. It does not deal with 98% of Canadian businesses, which are small businesses, 50% of which spend nothing on cybersecurity today, so they absolutely need help. As parliamentarians, you've heard the story of the impact of COVID-19 on small businesses, the debt load and more. They cannot afford yet another thing. Let's be very clear: The bill for cybersecurity for small businesses and large enterprises is because, at a national level, we fail to protect them from other countries and from criminals, so yes, I highly encourage other measures.

My point about the speed with which we need to move this legislation.... This is just the first step for laws you need to consider, and we need to get it right.

I'll be honest. Where Canadians are being hurt, and hurt badly, right now is in health care. You have five hospitals in Ontario right now that are still recovering from an ransomware attack. We still don't know what happened in Newfoundland and why it happened, nor have we learned from it. We know, from non-peer-reviewed research study in the U.S.—

The Vice-Chair (Mr. Doug Shipley): Excuse me, but I have to ask you to wrap it up, please.

Mr. David Shipley: —that 40 to 60 Americans have died because of ransomware attacks against hospitals there, so yes, we need help. We need to get this law done first, and the first thing to make it better, from a positive side, is to have a due diligence defence.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Shipley.

Thank you, Ms. Michaud.

Mr. Julian, you have six minutes.

Mr. Peter Julian: Thanks very much, Mr. Chair.

I will start with Mr. Shipley and Ms. Bahr-Gedalia.

We have had this legislation basically sitting now for 20 months. It was introduced in June 2022. We're coming up to the second-year anniversary and we're only beginning, really, the hearings about the legislation.

How important is it that we move forward quickly on this, given the problems all of our witnesses have enumerated? What would you suggest, in terms of a time frame, given the length of time it has taken to get the bill this far?

Mr. David Shipley: I'll go first.

In the time that we have languished, Australia has published a comprehensive cyber strategy in relation to some horrific attacks on their citizens and their personal medical information, Europe has moved forward with legislation, and the United States has moved forward with bold executive and legislative action. We are the easy target left in the west, so we are going to continue to attract an unhealthy amount of attention that is going to steal prosperity from Canadians and risk safety.

So, I would say, soon, because the reality is this: We'll get this legislation passed, and then we're going to end up in at least a year, if not two years, of battling over regulation. That goes back in particular to Ms. Proctor's point about the importance of getting the definitions as clear as possible in legislation so we can get moving on this stuff.

We are way behind. I know Parliament has many issues in front of it, but we live in a digital world and we're acting like we're in the 20th century.

● (1700)

Mr. Peter Julian: Before I go to Ms. Bahr-Gedalia, would it be fair to assume that, given the fact that other countries have moved forward, the longer we delay getting this bill right and getting it back to the House and then to the Senate, the more likely it is that we'll have serious incidents because we have that vulnerability?

Mr. David Shipley: Absolutely.

Mr. Peter Julian: Thank you.

Ms. Bahr-Gedalia, on the same question, how critical is it for us to act?

Ms. Ulrike Bahr-Gedalia: It is very critical. That's a definite “yes” that we should act in a timely manner.

I would also like to emphasize that we need to get it right and not rush through it in a way that.... I'm a little hesitant to name a time frame because the focus should be on all the challenges we pointed out and addressing these properly.

Comments were made as well on national cybersecurity strategies and plans in other countries and so forth. We don't have our national cybersecurity strategy yet launched. We greatly look forward to what the Canadian Chamber has fed into the submission, because for me and our members it would provide the broader, overarching picture of cybersecurity per se. Bill C-26 would be one part of that strategy. It's a holistic view and a comprehensive approach there.

Lastly, I wanted to make one comment in terms of time and I lost my train of thought there. You had another follow-up question to Mr. Shipley, I think. Could you please remind me what it was?

Mr. Peter Julian: It was on the vulnerability that this creates with Canada not moving forward while other countries put in place legislation.

Ms. Ulrike Bahr-Gedalia: Yes, I wanted to make one more point that members had mentioned to me.

We had this experience with another bill. If we wait too long, provinces might go ahead and start their own legislation. A few members have mentioned that there is a concern that while we are internationally lagging and maybe also not harmonizing right now in many ways, this could happen on a domestic or provincial level as well. A patchwork always works to the disadvantage of businesses.

Mr. Peter Julian: Thank you for that.

Ms. Proctor and Monsieur Traoré, you've spoken about the issue of regulation and also having in place a reporting period that is less onerous. Is getting the legislation right responding on those two areas?

I would ask all the witnesses whether they have specific amendments to offer that would take improvements to the bill out of the regulatory format and put it into discussions that we can have around this table for adoption in Parliament.

Ms. Daina Proctor: Thank you for the question.

To bring both of your questions together, wherein you were asking about the risk of not acting, in IBM we operate with, partner with and strategically advise over 1,700 organizations. Admittedly, they're not all in the direct scope of this, but they would be impacted through the passing of Bill C-26. Many of those organizations struggle. Many of those organizations are focused on Canada. Many of them are focused on multinational. By not acting within Canada, we are, in effect, encouraging those organizations to pause on Canada.

We don't have the regulations. We don't have the definitions. We don't have the laws in place for them to understand the arena they're playing in within Canada. This bill languishing is causing that pause to get larger.

From a collective individual perspective, it also shifts into the mindset of our resources, our teams and our neighbours. Our graduates—our children coming up through education —challenge what Canada's position is on cyber risk and cybersecurity, not just for the critical infrastructure that we need to run and operate, but for the employment opportunities that we have and that our organizations have.

The Vice-Chair (Mr. Doug Shipley): Thank you.

Ms. Daina Proctor: I hope that gives you a bit more perspective on that, so when we lean into the reporting time period, it equally speaks to the risk. One of the best things we do—

● (1705)

The Vice-Chair (Mr. Doug Shipley): Ms. Proctor, I'm going to have to ask you to wrap it up. We're out of time. I'm sorry.

Committee, we have the room resources until 6 p.m. I think there's some very interesting information coming out here, so I'm going to give everybody one more—

Mr. Ron McKinnon: I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Yes, sir.

Mr. Ron McKinnon: I'd like to suggest that, rather than do that, we go to the next panel. I may have misunderstood—

The Vice-Chair (Mr. Doug Shipley): You were reading my mind. I was going to give two minutes to each side—

Mr. Ron McKinnon: Two minutes for each party is eight minutes. We are going to be cutting into the time for the next panel. I'd love to hear more from these guys, but we also need to hear from the next panel.

The Vice-Chair (Mr. Doug Shipley): Maybe someone wants to put forward a UC motion.

Mr. Julian, I don't know what the will of the committee is. We can talk like this, but we're wasting time.

Mr. Peter Julian: Mr. Chair, I thought your suggestion was a good one, doing one more round for two or three minutes for each party. I think that makes sense.

The Vice-Chair (Mr. Doug Shipley): We don't have UC on that, so we'll make it very quick. I will hold everyone to two minutes. If you want to pass your time, then we can move on.

That's two minutes, starting with Mr. Lloyd.

Mr. Dane Lloyd: Thank you, Mr. Chair.

I'd like to start by offering my thoughts and prayers, and hopefully the committee's, on the terrible news about the cancer diagnosis of His Majesty, the King of Canada, King Charles III. I know our thoughts are with his family, and also with the families in Atlantic Canada, including, I believe, our chair's, who are undergoing a massive snowfall right now. I wanted to share our committee's thoughts and prayers with those families.

I also want to put a motion on notice. I'm not going to be moving the motion, but I want to put on notice a motion regarding car thefts. As we know, in the past eight years, car thefts have exploded in this country. Particularly in the last three years, we've seen a massive explosion in the number of insurance claims that have been paid out. In 2022—

[*Translation*]

Ms. Kristina Michaud: I have a point of order, Mr. Chair.

[*English*]

The Vice-Chair (Mr. Doug Shipley): Yes, go ahead, Ms. Michaud.

[*Translation*]

Ms. Kristina Michaud: Thank you.

I find it hard to understand why the Conservative Party wants to table a notice of motion on auto theft in the Standing Committee on Public Safety and National Security, when the committee has already voted in favour of a motion on auto theft that I tabled a few weeks ago. I don't understand that. In addition, we are supposed to study this subject in a few weeks, possibly after the study of Bill C-26. So I'm wondering about the need to table a new notice of motion on the same subject.

Thank you.

[*English*]

The Vice-Chair (Mr. Doug Shipley): Thank you, Ms. Michaud.

I can't really speak to the need. Mr. Lloyd does have two minutes on the floor. He'd probably be done by now, but it is in order, so I'll have to let Mr. Lloyd proceed.

Mr. Ron McKinnon: On the same point of order, I would observe that, just two meetings back, we had a debate on a car theft motion. It seems excessive and redundant to me.

The Vice-Chair (Mr. Doug Shipley): It is in order.

Mr. Lloyd, go ahead.

Mr. Dane Lloyd: Thank you, Mr. Chair.

I have a minute left.

There's been an explosion in car theft, especially in the last three years. My notice of motion will be calling on the government to take immediate action—

Mr. Peter Julian: I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Go ahead, Mr. Julian.

Mr. Peter Julian: Mr. Chair, I'm quite disturbed by this. We have a good-faith move to do a final round of questions. I have a ton of questions for the witnesses.

The Conservatives are spending their entire opposition day tomorrow on auto theft. As Madame Michaud has already mentioned, she's already brought a motion that has been adopted by this committee.

I don't see this as a legitimate motion being brought forward in good faith. I see this as a filibuster tactic, which I do not believe is appropriate, given that we have witnesses who've spent their time, and Canadian taxpayers who've spent their resources to have these hearings about legislation that we've just heard is absolutely critical to adopt.

I don't believe it's appropriate. It's redundant to bring forward this motion at this time. If the member persists in trying to filibuster this committee, I will have to challenge your decision to allow the motion to come forward, Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Julian.

I'm going to take Mr. Lloyd in good faith. He said he has only 30 seconds left. That's not filibustering. He had two minutes, and it was his time. Quite frankly, we have spent more time outside of that discussing it.

Mr. Lloyd, we'll hold you to your word, and we'll wrap this up.

Mr. Dane Lloyd: Thank you, Mr. Chair.

I'm disturbed that I've been blocked so many times from bringing forward this common-sense motion. This is an immediate problem. I've had my vehicle stolen. It was attempted to be stolen. I stopped a vehicle theft in Alberta over the Christmas break that occurred right in front of my house. This is an immediate problem. These repeat offenders need to be held accountable.

We can have a study on this, but Canadians want action now. We need to get tough on these repeat offenders. This is costing every Canadian family $500 a year in increased insurance premiums. I'm appalled that I've been stopped so many times from bringing forward a common-sense motion so that we can debate this in the House and take real action on this issue.

Thank you, Mr. Chair.

● (1710)

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Lloyd.

We'll go to Ms. O'Connell for two minutes.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

Once again, it's fake outrage for the Conservatives while the cameras are rolling. Once we get through Bill C-26, auto theft is the very next study, which Madame Michaud brought forward, that we would be dealing with. I also find it incredibly ironic that—

Mr. Dane Lloyd: I have a point of order, Mr. Chair.

Ms. Jennifer O'Connell: It's my time.

The Vice-Chair (Mr. Doug Shipley): It's a point of order, just like we had when he was speaking.

Go ahead, Mr. Lloyd.

Mr. Dane Lloyd: We have witnesses here. I think it's very important that we hear from them, Mr. Chair.

Thank you.

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell, the floor is yours still.

You have a minute and a half left.

Ms. Jennifer O'Connell: I'm actually really pleased that my colleague did that, because it just goes to show the immaturity the Conservatives are showing every day that we have been studying Bill C-26. They haven't asked a single question.

I overheard Mr. Brock, after his filibuster the other day, ask what we were studying and whether this was the first day we were on it.

They don't care about security or safety.

Mr. Larry Brock (Brantford—Brant, CPC): I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Go ahead, Mr. Brock, on a point of order.

Mr. Larry Brock: I didn't comment at all at the last meeting. I don't know what Ms. O'Connell is talking about.

Ms. Jennifer O'Connell: No, I overheard—

Mr. Larry Brock: The record will show—

The Vice-Chair (Mr. Doug Shipley): Thank you.

Ms. O'Connell.

Ms. Jennifer O'Connell: Thank you.

Sure, let the record show, Mr. Prosecutor, that I overheard him speaking to Mr. Lloyd about not knowing what was being discussed.

Mr. Larry Brock: I have a point of order, Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): Go ahead.

Mr. Larry Brock: I heard all kinds of backroom chat between Ms. O'Connell, Mr. Bittle and their team. If we want to talk about dirty laundry, let's get it all out on the table.

The Vice-Chair (Mr. Doug Shipley): Thank you. I'm not sure that's a point of order.

Go ahead, Ms. O'Connell.

Mr. Ron McKinnon: I have a point of order.

I just want to know—

The Vice-Chair (Mr. Doug Shipley): Folks, I'm going to speak up here.

Everybody's complaining about not having enough time. We are wasting more time on points of order.

Mr. Ron McKinnon: I understand. However, points of order need to be done.

The Vice-Chair (Mr. Doug Shipley): I have the floor right now, Mr. McKinnon. The chair is speaking right now. I'll address you in a moment.

Mr. Ron McKinnon: I'm sorry.

The Vice-Chair (Mr. Doug Shipley): Thank you.

Folks, if we do want to wrap this up.... We have the time stalled right now.

Ms. O'Connell, you have just over a minute left.

We will proceed with Mr. McKinnon, who has a point of order.

Go ahead.

Mr. Ron McKinnon: I was just wondering which of our four Conservative colleagues are members of this committee and which are substitutes.

I would ask for clarification as to whether people who are not members of this committee can move points of order.

The Vice-Chair (Mr. Doug Shipley): Right now, the clerk has informed me that Mr. Lloyd, Mr. Motz and Mr. Brock are in this committee today.

Go ahead, Ms. O'Connell.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

Once again, the Conservatives talk tough on crime. Mr. Brock can raise whatever supposed conversation he claims to have heard, because I guarantee it didn't exist, but I heard him talk about not even knowing what committee he was coming in to filibuster or what issues it was on.

It's been demonstrated very clearly that the Conservatives had time to ask questions and didn't bother.

I'll move to the witnesses on Bill C-26.

Mr. Shipley, you talked about the importance of this legislation. You raised examples of a natural gas pipeline that was hacked and what that does for critical infrastructure, including workers who might work in the energy industry. What happens if Canada is not prepared for a cyber-attack in our energy industry?

Mr. David Shipley: We got lucky with this last attack. That's everything I have been told publicly. We only know about this attack because an American soldier leaked it. Otherwise, the Canadian public wouldn't know about it—

The Vice-Chair (Mr. Doug Shipley): Mr. Shipley, I'll have to ask you to wrap this up quickly, please. I said I was going to keep it tight to two minutes.

Go ahead.

Mr. David Shipley: I do want to get to something that was raised about cars.

Modern cars right now are software. The reason they're being stolen so easily is that they're easily hackable. If you want to talk about something that should keep you awake at night, it's the fact that Elon Musk at Tesla does over-the-air updates and every single Tesla in this country could get bricked. There's not a law on the books holding them accountable in this country, either for the cybersecurity of it to prevent theft or, more broadly, to prevent the actual cause of a major accident.

We need to move.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Shipley.

I hate to cut people off, but we are very tight on time.

Ms. Michaud, you have two minutes, please.

[*Translation*]

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

Ms. Bahr-Gedalia, you spoke earlier about introducing a 72-hour deadline to give companies time to report an incident to the government.

In the current version of Bill C-26, it says that incidents must be reported as soon as they occur. You believe that the deadline you are proposing could give businesses a boost. I also think that 72 hours would be a good time frame, particularly to manage the additional paperwork that this bill will create.

As a chamber of commerce representative, you surely talk to companies and must know their opinion on this bill. What are you hearing from them?

What are the arguments behind the proposal to give them a little more time?

● (1715)

[*English*]

Ms. Ulrike Bahr-Gedalia: Thank you for the question.

First of all, when an attack happens, you need time to figure out the nature and scope of the attack. That can't happen immediately. That 72 hours that the members were looking at is actually from the time you become aware of it.

It is based on recommendations by the United States, in their Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA, which is from 2022. It has been in practice. We like to learn from those who have actually applied best practices.

I hope this answers your question.

[*Translation*]

Ms. Kristina Michaud: Yes, thank you very much.

Mr. Shipley, earlier you gave the example of Australia. IBM Canada also talked about international standards.

Can you give us an example of a cybersecurity law that has been passed by a country that we should read? In my opinion, everyone agrees that Canada is lagging behind a bit when it comes to cybersecurity.

[*English*]

The Vice-Chair (Mr. Doug Shipley): Ms. Michaud, you've had your two minutes. I'm sorry.

Perhaps the witnesses could supply that answer in writing or contact Ms. Michaud after.

Mr. Julian, you have two minutes.

[*Translation*]

Mr. Peter Julian: I'm going to go back to Ms. Michaud's question about countries that have adopted models. What models should we be looking at?

My second question is for Mr. Traoré and concerns the protection of the confidential information of merchants. How important is it that the bill protect that information?

Mr. Tiéoulé Traoré: This is extremely important in a number of respects.

Socio-economic considerations come to mind. We know the importance of data; we know its value. This is obviously data that needs to be protected. We do not want them to end up in the hands of people who are not authorized to have access to them.

It is indeed something that we support, as a company and as an entity of Canada. It's very important.

Mr. Peter Julian: Thank you very much.

[*English*]

I'll start with Ms. Proctor.

What are the best countries in terms of the models we should be looking to?

Ms. Daina Proctor: There are a number of countries that we can emulate based on some of their responses to various activities, being mindful that cyber is a global issue. While there are jurisdictions within individual countries, many of the corporations that are headquartered and operate out of Canada certainly are multinational, so I think it's great to be looking at additional countries. I would encourage you to start with all of our Five Eyes allies.

Mr. Peter Julian: Thank you.

Ms. Bahr-Gedalia, what is your opinion?

Ms. Ulrike Bahr-Gedalia: I can only echo those sentiments, because everything pretty much has been pointed out and said in that regard. I always like to remind everybody as well, though, to put it into a Canadian context while looking for alignment and harmonization with other jurisdictions.

Thank you.

Mr. Peter Julian: Go ahead, Mr. Shipley.

Mr. David Shipley: Our business is with the United States, in terms of the amount of trade we do. We'd best make sure that we're aligned with our largest trading partner.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Shipley.

We are out of time.

Thank you to the witnesses. Thank you for enduring today.

Folks, we are limited on time. Let's take a short, five-minute recess, and we'll get set up for the second part.

Thank you, everyone.

● (1715)

_____(Pause)_____

● (1720)

The Vice-Chair (Mr. Doug Shipley): I think we're good to start again.

I just want to remind everybody that we have resources until 6:00. I also want to mention that that clock is not the clock we go by. As Mr. McKinnon would know, it's never accurate. It's 5:24 right now, but we do have a hard stop at 6:00, so we have about 35 minutes.

Thank you to the witnesses for being here today. From Bruce Power, we have Todd Warnell, chief information security officer. From Citizen Lab, we have Kate Robertson, senior research associate, Munk School of Global Affairs and Public Policy, University of Toronto. By video conference, we have, from OpenMedia, Matthew Hatfield, executive director.

Thank you, all, for being here. We'll give you five minutes each.

We'll start with Mr. Warnell.

● (1725)

Mr. Todd Warnell (Chief Information Security Officer, Bruce Power): Thank you, Mr. Chair and members of the committee.

My name is Todd Warnell and I am the chief information security officer at Bruce Power.

Established in 2001, Bruce Power is Canada's only private sector nuclear generator, annually producing about one-third of Ontario's power, as well as life-saving medical isotopes used around the globe to fight cancer and sterilize medical equipment.

I'm grateful for the invitation to participate in your review of Bill C-26. Today, I will focus my comments on part 2 of the bill, namely, the critical cyber systems protection act.

I'm here before the committee to provide a perspective that proceeding with the implementation of Bill C-26 is of vital importance to the safety and security of all Canadians. Canada has prospered over the last four decades through a period of relatively stable and predictable global relations. However, that period of stability and predictability is changing amidst a backdrop of global geopolitical tensions and changing global dynamics. Ensuring the safe and reliable delivery of critical services that Canadians depend upon every day is not, and cannot be, a political issue.

Within Canada's nuclear industry, we have seen and demonstrated that through collaboration with governments, regulators, industry, academia, and individual Canadians, we can be successful in establishing and regulating cyber systems that are important to the safe and reliable operation of critical services.

The critical cyber systems protection act would introduce a broad framework from which all critical sectors, in collaboration with government and regulators, can develop and implement risk-informed and performance-based regulation to enhance the reliability and resilience of critical services. The committee should consider ways of ensuring that appropriate checks and balances are in place for any directives issued to address a risk or threat to Canada's critical cyber systems.

Harmonizing Canada's cybersecurity framework across critical sectors through Bill C-26 would also align our approach with our closest allies and avoid our being left behind as our allies move forward with enhancing their respective national cyber resilience programs and driving innovation that can enhance our collective capabilities in protecting ourselves and detecting and responding to a changing threat landscape.

In conjunction with Bill C-26, we urge lawmakers to review and consider the amendments to the CSIS Act, to enable Canada's intelligence community to exchange and co-operate on cyber-threat intelligence with Canada's public and private sector operators in both a proactive and preventative manner.

Thank you for the opportunity to address the committee today.

I look forward to your questions.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Warnell.

Up next, we have Ms. Robertson, please.

Ms. Kate Robertson (Senior Research Associate, Munk School of Global Affairs and Public Policy, University of Toronto, Citizen Lab): Good afternoon.

My name is Kate Robertson. I am a researcher at the Citizen Lab, which is based at the University of Toronto's Munk School.

My comments today draw on the Citizen Lab's research on cybersecurity and telecommunications policy, data security, and transparency and accountability mechanisms that are applicable to the relationship between governments and telecommunications providers. My brief, which was submitted to this committee, was written with Lina Li of McGill Law and provides a charter analysis of Bill C-26. Part three of our brief sets out our recommended amendments, building on a report on Bill C-26 written by my former colleague Dr. Christopher Parsons.

There are key recommended amendments that would act as constitutional safeguards in the legislation. This is not to state that they're exhaustively read here.

To protect the rule of law and free expression, orders issued under the legislation must be published in the Canada Gazette. Any exceptional circumstances that might justify confidentiality of those orders should be expressly and strictly defined in the legislation, and should be time-limited.

For privacy rights, the legislation needs explicit protections for personal information, notice requirements, and tighter controls surrounding the sharing and use of personal and confidential information. You'll find proposed terms for those amendments under recommendations 13, 14, 16, 19, 28 and 29 in our brief.

We also reiterate, as others have, that orders issued must be proportionate and reasonable. In particular, the legislation should make explicit that an order compelling the adoption of particular standards cannot be used to compromise the integrity of a telecommunications service, such as by compromising encryption standards. The terms for those amendments are in recommendations one and five of our brief.

It is notable that these amendments are compatible with the government's objective to play an assertive role in protecting Canada's networks. This is not a tug-of-war between competing public interests. This is important, because the courts do not tend to find it reasonable if constitutional rights are infringed upon in a way that is unnecessary. The desire for expediency through Parliament is understandable, but if these issues aren't fixed now by legislators, then the legislation may well be held up in court litigation for years, which ultimately requires additional legislative time to fix.

Amendments to limit secrecy and to require proportionality also reinforce the government's objective of protecting our networks. I agree that, as was said last week, cybersecurity is a team sport, and I agree with Mr. Warnell's comments on the same subject. Effective cybersecurity integrates expertise from across a range of sources, including regulators, industry, civil society, academic and security researchers, and data journalists.

Dr. Parsons' report on Bill C-26 last year, as well as this committee process itself, illustrates how industry and independent expertise can provide a path forward for improving the legislation without detracting from the bill's core mandate. Public transparency will be an effective way to garner expertise from these sources as the legislation is implemented over time.

The Citizen Lab's recent report, “Finding You”, which is appendix C to our brief, underscores how secrecy at the regulatory level has led to serious “geolocation-related threats associated with contemporary networks”. The report documents persistent vulnerabilities at the heart of the world's mobile communications networks. It notes, “The failure of effective regulation, accountability, and transparency has been a boon for network-based geolocation surveillance.” In other words, when network standards and regulations are shrouded in unnecessary secrecy, this enables network insecurity to fester.

Similarly, without proportionality and transparency, Bill C-26, unamended, could enable successive governments to actually undermine network security, and ultimately human security, through orders that would drill holes in encryption standards in telecommunications networks.

● (1730)

The Vice-Chair (Mr. Doug Shipley): Ms. Robertson, can I ask you to wrap this up? Your time is up.

Do you have much more to go, or are you just about done?

Ms. Kate Robertson: My clock is slower than yours. I had 20 seconds, but I will leave the remainder of my comments for questions.

The Vice-Chair (Mr. Doug Shipley): I'm sorry about that. Thank you.

Up next, we have Mr. Hatfield, by video conference.

Mr. Matthew Hatfield (Executive Director, OpenMedia): Hi there. I'm Matt Hatfield, and I'm the executive director of OpenMedia, a grassroots community of 230,000 people in Canada who work together for an open, accessible and surveillance-free Internet. I'm joining you from the unceded territory of the Sto:lo, Tsleil-Waututh, Squamish and Musqueam nations.

I’d like to ask us all a question: What does cybersecurity mean to you as an individual, as a family member and as a citizen? For me, and for many people across Canada, our cybersecurity is inseparable from our privacy, as so much of our everyday lives is conducted online—much more so since COVID—and none of us feel secure with the thought of being spied on in our everyday lives, whether by hackers, hostile states or our own government. For most Canadians, our cybersecurity is very much about that sense of personal security.

The draft of Bill C-26 you have in front of you threatens that security. It poses enormous risks to our personal privacy, without basic accountability and oversight to ensure that the people given these powers don't abuse them against us. You must fix this.

Exhibit A is proposed section 15.2 of the Telecommunications Act, which grants the government the power to order telcos “to do anything or refrain from doing anything”. There are no limits here, no tests for necessity, proportionality and reasonableness, and no requirement for consultation. The government could use these powers to order telcos to break the encryption we need to keep ourselves safe from hackers, fraudsters and thieves. They could even use these powers to disconnect ordinary people indefinitely from the Internet, maybe because our smart toaster or an old phone we gave our kids gets hijacked by a hostile botnet. Without a requirement that these orders be proportional or time-limited, these are real risks.

It gets worse. The government would be allowed to keep even the existence of these orders—never mind their content—top secret indefinitely, and even if these orders are challenged by judicial review, the minister could bring secret evidence before secret hearings, which flies in the face of basic judicial transparency.

There's no excuse for this. Our close allies in Australia and the U.K. have shown how cybersecurity can be strengthened without compromising fundamental rights. Why do Canadians deserve lesser protections?

All this comes when Parliament is working on strengthening our privacy laws through Bill C-27. I have to ask, does one hand of our government even know what the other is working on?

We recognize that there are very real problems, though, that Bill C-26 is trying to solve. When we read the government's stated objectives, we're on board. Should we protect the digital infrastructure? Sure. Should we remove risky equipment from hostile states? Of course. Should we force big banks and telcos to better protect their customers? Of course. However, we can fulfill these objectives without sacrificing our rights or balanced, effective governance. Let's talk about how.

First, the government's new powers must be constrained. Robust necessity, proportionality and reasonableness tests are an absolute must. An unbreakable encryption is the fundamental baseline that all of our personal privacy depends on, so there must be an absolute prohibition on the government using these powers to break encryption.

Second, privacy rights must be entrenched. Personal information must be clearly defined as confidential and forbidden from being shared with foreign states, which are not subject to Bill C-26's checks and balances.

Third, the government must not be allowed to conceal the use of its new powers under a permanent veil of secrecy.

Fourth, when the use of those powers is challenged in court, there must be no secret evidence. Special advocates should be appointed to ensure all evidence is duly tested.

Fifth, any information the Canadian Security Establishment obtains about Canadians under Bill C-26 should be used exclusively for the defensive cybersecurity part of their mandate. I hope you all remember that NSIRA, the body explicitly established by Parliament to oversee CSE, has complained for years about CSE not being accountable to them. Knowing how difficult it's proved to keep them accountable for their existing powers, please don't grant them broad new powers without tight and clear use and reporting mechanisms.

As other people have said, when cybersecurity works, it's a team sport. It requires buy-in from all of us. We all have to be on team Canada, and we all have to trust in the regulatory framework that governs it. There's zero chance of that happening with Bill C-26 as is. Adequate transparency, proportionality and independent verification are the necessary baseline that this bill has to earn for it to work.

We're going to be delivering a petition signed by nearly 10,000 Canadians to you shortly, folks who are calling for that baseline protection. We urge you to listen to these voters and adopt the amendments package that civil society has suggested to you to get this legislation where it needs to be.

Thanks. I look forward to your questions.

● (1735)

The Vice-Chair (Mr. Doug Shipley): Thank you to all the witnesses.

We will start for six minutes with Mr. Lloyd.

Mr. Dane Lloyd: Thank you, Mr. Chair.

Thank you to all the witnesses for being here today.

My line of questioning will be mostly for Ms. Robertson and Mr. Hatfield.

I'm very concerned by the testimony you've shared with me today, in light of the fact that the government itself certainly has been victim of hacking. I recall that Global Affairs was the victim of a recent hack.

I think this is one of the dilemmas of increasing centralization of information, as Bill C-26 purports to do in collecting information on the cybersecurity plans of the designated operators. Is there any guarantee that, when government collects all of this very confidential and powerful information, it is better equipped than some of the best companies in the world to protect that information from hackers?

Ms. Kate Robertson: The amassing of data in any database brings with it attendant security risks. The extent of them I cannot comment on.

I would indicate that your concerns are connected to amendments that we have raised in our brief regarding the handling of data. Right now, the information-sharing powers within the Canadian government that would be enabled by Bill C-26, if passed unamended, are extremely broad.

One limit that we recommended, for example, is that the use of the information being shared should be constrained to cybersecurity objectives, and not piggybacked objectives that are layered on after the fact. Retention limits should be strictly defined to address the very concern that you're raising.

In that way, while there is understandably a need for some examination of critical information to enable that mandate to be fulfilled, it should be very strictly defined within the legislation itself.

Mr. Dane Lloyd: Mr. Hatfield, did you have comments on that?

Mr. Matthew Hatfield: I would reinforce what Ms. Robertson said.

I think transparency is actually the ally of effective cybersecurity. A lot of mistakes get made when things are stored in the dark. Rather than allowing our security establishments to hoover up the maximum possible amount of information and sit on all of it, I think putting some limits in terms of retaining only information that is strictly necessary and deleting other information at a certain point helps minimize the risk of that information transfer.

● (1740)

Mr. Dane Lloyd: Are you confident that the legislation as written, coming before this committee unamended, will protect the privacy of Canadians and the safety of our cybersecurity sector?

Mr. Matthew Hatfield: I think this legislation makes our privacy much worse, actually.

Mr. Dane Lloyd: That's very concerning.

Of course, you listed some amendments that you've put forward. What do you think would be the most powerful amendments to ensure that Canadians' privacy rights and the security of all this information that the government is purporting to gather are protected?

Mr. Matthew Hatfield: I think the necessity and proportionality tests that we've applied are a really important piece here to make sure information is being collected only for appropriate purposes. I think getting those kinds of fixes, which are similar to what Australia has done, will greatly mitigate some of the potential harms of the legislation.

Mr. Dane Lloyd: Thank you, Mr. Hatfield.

Ms. Robertson.

Ms. Kate Robertson: Ultimately, under the Constitution, the courts look to an effective mechanism of accountability and review. In this case, it's hard to pinpoint one particular amendment when what the courts look for when protecting privacy is an interlocking system that enables effective review.

I identified in my opening remarks a number of amendments that would assist that review mechanism, not one of which could be functional on its own. For example, we've identified notice requirements as an important mechanism. This is a way to enable individuals whose personal and confidential information has been shared to know that this has happened, so it could be effectively challenged in court.

That's just one example of the amendments we have identified in the report for that reason.

Mr. Dane Lloyd: Thank you.

Mr. Hatfield, something you said in your remarks also greatly disturbed me.

In response to cybersecurity incidents, we've seen the government putting forward legislation to give itself massive new powers. We have seen recent examples of government using the legislative powers at its disposal to freeze people's bank accounts.

I have deep concerns that if we don't put in the necessary checks and balances that you are talking about, we can be giving the government extraordinary powers to shut people out of the Internet, which, as we know, has become so essential in the 21st century to participating in our democratic society and in our economy, to be connected with loved ones, and to work. I have serious concerns. I want to pass along that we share your concerns and we'll be looking into this further.

Mr. Chair, I would like to split my time with my colleague, Mr. Motz.

Thank you.

Mr. Glen Motz: Thank you, Chair.

I know the committee is going to be annoyed, but Canadians are more annoyed with the fact that we have an issue with the Emergencies Act. It was spoken about before.

I would like to move the following motion, Chair:

> That, in light of the recent Federal Court ruling which found that the government's use of the Emergencies Act in February 2022 to have been illegal and that the special criminal laws subsequently created by the Liberal Cabinet to have been an unconstitutional breach of Canadians' Charter rights—

Mr. Ron McKinnon: I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Mr. Motz, wait just one moment, please. We have a point of order.

Mr. McKinnon, go ahead, sir.

Mr. Ron McKinnon: Just at the outset, it seems to be pretty much exactly what Mr. Motz just moved. That motion was moved, and we voted to adjourn the debate.

I don't think enough time has passed since that transpired. I think this is repetitive and redundant, and should be out of order.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. McKinnon.

I haven't even read it, so I can't comment on that yet.

Mr. Brock, do you have a comment?

Mr. Larry Brock: Perhaps Mr. McKinnon can allow the member to actually read out the motion before he opines on it.

The Vice-Chair (Mr. Doug Shipley): Yes. We don't know how different it is, Mr. McKinnon.

Go ahead, Mr. Motz.

Mr. Glen Motz: Thank you.

I'll continue:

> ...created by the Liberal Cabinet to have been an unconstitutional breach of Canadians' Charter rights, the Committee undertake a study of 6 meetings, pursuant to Standing Order 108(2), of the Department of Justice's role in supporting the government's illegal and unconstitutional decisions concerning the Emergencies Act, together with the consequences which follow the Court's decision, provided that
>
> (a) the Committee invite the following to appear, separately, as witnesses, for at least one hour each:
>
> (i) the Honourable David Lametti, the Minister of Justice and Attorney General of Canada at the time,
>
> (ii) the Honourable Marco Mendicino, the Minister of Public Safety at the time,
>
> (iii) the Honourable Arif Virani, the Minister of Justice and Attorney General of Canada,
>
> (iv) representatives of the Canadian Civil Liberties Association, and
>
> (v) representatives of the Canadian Constitution Foundation; and
>
> (b) an order do issue for all legal opinions which the government relied upon in determining that
>
> (i) the threshold of "threats to security of Canada", as defined by section 2 of the Canadian Security Intelligence Service Act, required by section 16 of the Emergencies Act, had been met;
>
> (ii) the thresholds required by paragraphs 3(a) or (b) of the Emergencies Act, concerning a "national emergency" had been met;
>
> (iii) the situation could not "be effectively dealt with under any other law of Canada", as required by section 3 of the Emergencies Act;
>
> (iv) the Emergency Measures Regulations were compliant with the Canadian Charter of Rights and Freedoms, including the analysis relied upon by the Minister of Justice in discharging his responsibilities under section 4.1 of the Department of Justice Act, and

(v) the Emergency Economic Measures Order was compliant with the Canadian Charter of Rights and Freedoms, including the analysis relied upon by the Minister of Justice in discharging his responsibilities under section 4.1 of the Department of Justice Act,

provided that these documents shall be deposited with the Clerk of the Committee, without redaction and in both official languages, within seven days of the adoption of this order.

As I have indicated before, Chair—

● (1745)

Ms. Jennifer O'Connell: I have a point of order.

The Vice-Chair (Mr. Doug Shipley): Mr. Motz, we have a point of order. Just one moment, please.

Ms. O'Connell, go ahead.

Ms. Jennifer O'Connell: Now that we have heard the full motion, I would argue Mr. McKinnon's point that even if it is a different motion that he submitted, the only difference is the timing. Therefore, it is too similar to a motion that we have already dealt with and it should be out of order.

The Vice-Chair (Mr. Doug Shipley): Thank you, Ms. O'Connell.

Could you just give us a moment? The clerk is trying to.... Which motion was it?

Ms. O'Connell, I don't think we need snide remarks or comments.

Ms. Jennifer O'Connell: I laughed because you don't know which motions you're moving.

The Vice-Chair (Mr. Doug Shipley): I'm not moving anything. I'm the chair.

The clerk is looking it up because he doesn't know, Ms. O'Connell, so what's so funny?

Ms. Jennifer O'Connell: I find it funny that you guys are that disorganized in your own filibuster.

Mr. Glen Motz: Are we disorganized, or are you just trying to cover up?

Ms. Jennifer O'Connell: Cover up what? You don't want to talk about cyber—

The Vice-Chair (Mr. Doug Shipley): Order.

Mr. Glen Motz: You don't want to inform the Canadian public on the Emergencies Act.

Ms. Jennifer O'Connell: Do you want me to read from your mayor—

The Vice-Chair (Mr. Doug Shipley): Order, please.

Everybody, it has been a long day. Let's have order, please.

Mr. Motz, is the new one 1.2?

Mr. Glen Motz: I don't have that on mine, but yes, it's the one with the study of six meetings.

The Vice-Chair (Mr. Doug Shipley): And your last one was—

Mr. Glen Motz: It was 1.1.

The Vice-Chair (Mr. Doug Shipley): Significantly, you're asking for a different number of meetings.

Mr. Glen Motz: Yes.

The Vice-Chair (Mr. Doug Shipley): Okay. I think that's significant enough.

Carry on, Mr. Motz.

Ms. Jennifer O'Connell: I have a point of order.

I challenge the chair and I ask for a recorded division.

The Vice-Chair (Mr. Doug Shipley): We'll have a recorded vote.

Ms. Jennifer O'Connell: Mr. Chair, before you start, can you please remind everybody that, if I'm correct, a “no” vote means you don't sustain the chair's ruling?

The Vice-Chair (Mr. Doug Shipley): I'll ask the clerk to clarify.

I ruled the motion in order.

The Clerk: The question is, shall the decision of the chair be sustained?

(Ruling of the chair overturned: nays 7; yeas 3)

The Vice-Chair (Mr. Doug Shipley): Mr. Julian.

Mr. Peter Julian: I have a point of order, Mr. Chair.

We only have 11 minutes left. I know it's a hard stop at 6 p.m. It's certainly a hard stop for most members. I would suggest that we divide the time among the three parties that haven't yet had questions, perhaps three minutes each.

● (1750)

The Vice-Chair (Mr. Doug Shipley): Okay, I have 10 minutes left. I have 5:50 p.m., so we'll do five minutes each.

Is that fair, Mr. Julian?

Mr. Peter Julian: Well, that takes us to 6:05 p.m.—

The Vice-Chair (Mr. Doug Shipley): Oh, I'm sorry. That's good Conservative math.

We'll do two and a half or three minutes each.

Ms. O'Connell, you're up first.

Ms. Jennifer O'Connell: Thank you, Mr. Chair, and thank you to the witnesses for being here.

Once again, unfortunately, we see how unserious the Conservatives are when it comes to cyber safety—

Mr. Glen Motz: I have a point of order, Mr. Chair.

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell, hold on just a moment, please.

Mr. Motz.

Mr. Glen Motz: You know, it's really quite interesting to hear from the other side—

Mr. Chris Bittle (St. Catharines, Lib.): [*Inaudible—Editor*]

Mr. Glen Motz: Mr. Bittle, you can have your turn.

Mr. Larry Brock: Mr. Bittle, you don't have the floor.

Mr. Chris Bittle: Neither do you.

The Vice-Chair (Mr. Doug Shipley): Gentlemen, order, please. We're almost through this.

Let's get through this.

Mr. Glen Motz: If you want to have the floor, you can ask for it.

On my point of order, Mr. Chair, it's really surprising that we have the narrative from Ms. O'Connell about our concern about cybersecurity. In fact, I think nothing can be further from the truth. The fact is—

Ms. Jennifer O'Connell: This is debate, Mr. Chair.

Mr. Glen Motz: It's not debate at all. I'm making a comment. Please—

Ms. Jennifer O'Connell: That's literally debate.

The Vice-Chair (Mr. Doug Shipley): Mr. Motz, let's maintain order, please. Let's quickly get to your point.

Do you have a point?

Mr. Glen Motz: Yes, I do actually.

The fact that Ms. O'Connell speaks for us is an embarrassment to the Conservative Party of Canada. She doesn't speak for us. We do take this matter very seriously, and we'll see—

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Motz.

Ms. O'Connell.

Ms. Jennifer O'Connell: Thank you.

I'm only 12 seconds in. I'm keeping track.

Through the chair to the witnesses, again, apologies—

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell, just one moment, please. We did have an agreement that our last nine minutes would be broken up evenly, so we will keep breaking them up as we go.

How many minutes are left now?

Ms. Jennifer O'Connell: I'm 22 seconds in. My time has been interrupted for points of order, so I have three minutes.

The Vice-Chair (Mr. Doug Shipley): For clarification, do you want to take the Bloc's and the NDP's time, or do you want to divvy up what's left now?

Ms. Jennifer O'Connell: I have three minutes, which is what was agreed to. If your side would like to keep interrupting to shut me down—

The Vice-Chair (Mr. Doug Shipley): I'm the chair, Ms. O'Connell. I'm not on a side.

Ms. Jennifer O'Connell: —then it demonstrates exactly my point of how unserious you are about cybersecurity and anything dealing with crime and safety in this country.

Go ahead. Cut my time. Cut me off. Silence me.

The Vice-Chair (Mr. Doug Shipley): You're actually eating into your time. I'm not silencing you at all. I'm letting you speak freely right now. Everybody's listening.

Ms. Jennifer O'Connell: So I will continue. I've spoken for 22 seconds out of my three minutes. If you're going to try to silence me—

The Vice-Chair (Mr. Doug Shipley): Does anybody here think she's silenced right now?

Ms. Jennifer O'Connell: Nobody cares about your poll, Mr. Chair. I would ask that you run a meeting as a proper chair. I was given three minutes—

Mr. Larry Brock: I have a point of order, Chair.

The Vice-Chair (Mr. Doug Shipley): Mr. Brock.

Mr. Larry Brock: This is absolutely disgusting and unparliamentary on so many levels. The ad hominem attacks against our chair and members of the Conservative side are deplorable, and Canadians are watching this behaviour of Ms. O'Connell and Mr. Bittle. The only person we have respect for right now is Mr. McKinnon. He's actually taking this seriously.

The Vice-Chair (Mr. Doug Shipley): Thank you, Mr. Brock.

Go ahead, Ms. O'Connell. Continue, please.

Ms. Jennifer O'Connell: Thank you. I'll continue.

The Conservatives are doing the work for me in showing how unserious they are.

Mr. Warnell, I'm going to try to at least get a question on the record. To all our witnesses, we're very interested in amendments. Comments have been made that there are things that can be done to improve this bill, but overall we need a cybersecurity plan to deal with critical infrastructure. We're very open to amendments and having those conversations about where we can strengthen this. However, unless we hear testimony, unless we go through this process, unless there are questions and amendments suggested, we can't propose those amendments to the government. This little demonstration here, this fake outrage, is really disappointing to see, because critical infrastructure is at risk.

Mr. Warnell, I come from a host nuclear community myself, and my residents share the concerns around the risk to critical infrastructure, nuclear, and supply chains. You brought up at the very beginning the risk to cancer patients for the critical isotopes that are produced. Can you perhaps speak to not only critical infrastructure but the upstream of the supply chain, if the immaturity of certain members can't get us through this process to allow amendments and testimony.

● (1755)

The Vice-Chair (Mr. Doug Shipley): Ms. O'Connell, could we please keep it professional and stop personal attacks on anybody in this room?

Ms. Jennifer O'Connell: Mr. Chair, you're not the arbiter of what I say. It is parliamentary.

The Vice-Chair (Mr. Doug Shipley): I think, actually, that it is my job.

Ms. Jennifer O'Connell: I still have a minute, and I would like the witness to answer.

The Vice-Chair (Mr. Doug Shipley): No, you have 18 seconds, according the clerk. He's keeping time.

Ms. Jennifer O'Connell: No, I have spoken for two minutes. You're counting interruptions from the Conservatives against my time.

I'd like Mr. Warnell, who has sat here for the duration of this meeting, to answer my question about the safety and security of critical infrastructure in nuclear communities.

The Vice-Chair (Mr. Doug Shipley): Let's keep it civil among all people, please.

Ms. Jennifer O'Connell: Oh, my gosh, I'm so not interested in your opinion of my comments to get to a question about critical infrastructure in nuclear communities.

The Vice-Chair (Mr. Doug Shipley): I was speaking to everybody, Ms. O'Connell. If you think that it's directed towards you, perhaps there's something going on there, but I was talking to our whole committee to keep it on a—

Ms. Jennifer O'Connell: Perhaps you have an issue in particular with me.

The Vice-Chair (Mr. Doug Shipley): Would you stop interrupting me, Ms. O'Connell, please?

Ms. Jennifer O'Connell: You've interrupted my time.

The Vice-Chair (Mr. Doug Shipley): Order.

Ms. Jennifer O'Connell: You have interrupted my time, Chair, time and time again.

The Vice-Chair (Mr. Doug Shipley): Order.

Ms. Jennifer O'Connell: It's funny that you don't interrupt the male Conservatives, but the one woman asking questions on this side—

The Vice-Chair (Mr. Doug Shipley): Okay, this meeting has gotten just ridiculous.

I declare this meeting adjourned.