HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

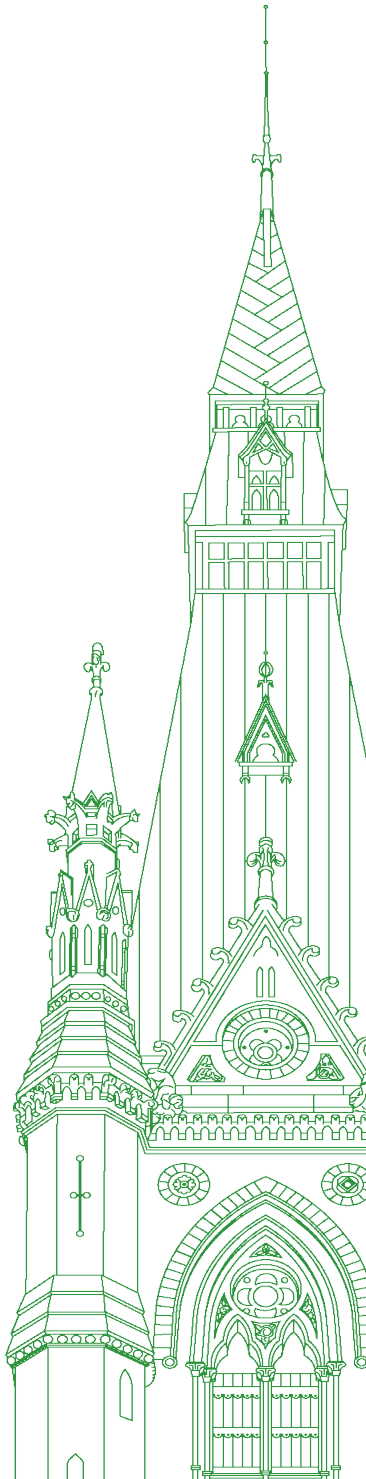
House of Commons Debates

Official Report

(Hansard)

Volume 151 No. 164

Monday, March 6, 2023



Speaker: The Honourable Anthony Rota

CONTENTS

(Table of Contents appears at back of this issue.)

HOUSE OF COMMONS

Monday, March 6, 2023

The House met at 11 a.m.

Prayer

● (1100)

[*English*]

VACANCY

PORTAGE—LISGAR

The Deputy Speaker: It is my duty to inform the House that a vacancy has occurred in the representation, namely Candice Bergen, member for the electoral district of Portage—Lisgar, by resignation effective Tuesday, February 28.

Pursuant to paragraph 25(1)(b) of the Parliament of Canada Act, the Speaker has addressed a warrant to the Chief Electoral Officer for the issue of a writ for the election of a member to fill this vacancy.

* * *

ADDRESS BY PRESIDENT OF THE EUROPEAN COMMISSION

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Mr. Speaker, there have been discussions among the parties and if you seek it, I believe you will find unanimous consent to adopt the following motion:

> That, notwithstanding any standing order, special order or usual practice of the House,
>
> (a) on Tuesday, March 7, 2023, at the expiry of the time provided for Oral Questions, the House shall adjourn to the next sitting day;
>
> (b) the address by the President of the European Commission to be delivered in the Chamber of the House of Commons on Tuesday, March 7, 2023, before members of the Senate and the House of Commons, together with all introductory and related remarks, be printed as an appendix to the House of Commons Debates for that day and form part of the records of this House; and
>
> (c) the media recording and transmission of such address, introductory and related remarks be authorized pursuant to established guidelines for such occasions; and
>
> (d) if a recorded division is requested in respect of a debatable motion after 2 p.m. on Monday, March 6, 2023, and before 2 p.m. Tuesday, March 7, 2023, it shall stand deferred to Wednesday, March 8, 2023, at the expiry of the time provided for Oral Questions.

[*Translation*]

The Deputy Speaker: All those opposed to the hon. member's moving the motion will please say nay.

[*English*]

The House has heard the terms of the motion. All those opposed to the motion will please say nay.

(Motion agreed to)

* * *

BUSINESS OF THE HOUSE

Hon. Mark Holland (Leader of the Government in the House of Commons, Lib.): Mr. Speaker, I would like to inform the House that the opposition day designated for Tuesday, March 7, has been undesignated.

PRIVATE MEMBERS' BUSINESS

[*English*]

FIGHTING AGAINST FORCED LABOUR AND CHILD LABOUR IN SUPPLY CHAINS ACT

The House proceeded to the consideration of Bill S-211, An Act to enact the Fighting Against Forced Labour and Child Labour in Supply Chains Act and to amend the Customs Tariff, as reported (without amendment) from the committee.

The Deputy Speaker: There being no motions at report stage, the House will now proceed, without debate, to the putting of the question on the motion to concur in the bill at report stage.

● (1105)

Hon. John McKay (Scarborough—Guildwood, Lib.) moved that the bill be concurred in.

The Deputy Speaker: If a member of a recognized party present in the House wishes that the motion be carried or carried on division or wishes to request a recorded division, I would invite them to rise and indicate it to the Chair.

Hon. John McKay: Mr. Speaker, I request that it be carried on division.

(Motion agreed to)

Hon. John McKay moved that the bill be read the third time and passed.

He said: Mr. Speaker, this has been quite a journey. We are close to the end of that four-year journey and hopefully we will move to a vote fairly quickly.

If I spent all my time thanking everyone who has helped us over the previous four years, I would use up all of my time, so let me confine my thanks to a select few who have helped us from Bill C-423 to Bill C-243, and from Bill S-216 to now Bill S-211.

We would not be here without Senator Julie Miville-Dechêne and her tireless efforts on Bill S-211 and Bill S-216, along with Jérôme Asselin-Lussier from her office and Shawn Boyle from my office, as well as the hon. member for Thunder Bay—Rainy River for his willingness to give up his preferred place in the Private Members' Business slot to me, for which I thank him.

I also want to recognize the very helpful contributions of two law firms, Dentons and Gowling, which have shepherded through the many iterations of this bill over the four years.

Finally I want to take note of World Vision, as it is aptly named. Over the past 10 years, World Vision has used its considerable resources to call attention to this international scourge, where Canadians play an unwitting role in enabling the distribution and consumption of slave products.

Before I turn to the bill itself, I want to offer a few comments on slavery in Canada.

As we know, prior to Confederation, Canada was really a collection of British colonies and as such was governed by the laws of Westminster.

In 1787, William Wilberforce, who, in my opinion, is the greatest member of parliament that the British Westminster system has ever produced, embarked on a mission to have the slave trade abolished, reasoning that if the slave trade was abolished, the abolition of slavery itself would surely follow. He was right.

To give us some context, 30% of the British Empire's GDP was dependent upon slave products. If ever an MP engaged in a formidable task, this was certainly it.

Twenty years later, the British Parliament passed the Slave Trade Act of 1807 and then 26 years after that slavery was formerly abolished in the British Empire on July 26. Wilberforce died three days later.

A committed evangelical Christian, Wilberforce was motivated by a deep conviction that the enslavement of another human being was a sin and an offence against God and mankind. As we know, deep moral convictions do not mean much in a parliament unless we can mobilize resources to push a bill to royal assent.

William Wilberforce showed his parliamentary and political genius in two ways. First, he was able to organize, rally and participate in probably the first citizens' movement that brought massive pressure on the Parliament of Westminster. Second, he was able to manipulate the legislative system to, over time, produce the desired outcome.

In fact, William Wilberforce gave a master class in British parliamentary procedures, strategies and tactics, which should be required reading for all parliamentarians.

The citizens' movement was pure genius. He took a ragtag group of quarrelsome evangelicals and attached to them some of the most committed abolitionists of the time. This was possibly the first time a group of deeply committed citizens confronted a deeply entrenched establishment and won.

For his efforts, William Wilberforce was branded as a traitor to his class. When he won, of course, we all won.

The laws of Great Britain applied to Canadian colonies. While some would argue that it is more complicated than that, and I might in another context agree, I would argue that it is a big improvement over the way the Americans handled the same issue.

● (1110)

Why a history lesson when we have an exceedingly modest Bill S-211 in front of us?

First, Bill S-211 is the product of a citizen's movement. World Vision and many others have pressured the parties to be proactive and commit to the legislation. Ultimately, this has resulted in both the Liberal and Conservative parties putting this kind of commitment into their platforms.

Second, getting worthwhile initiatives across the line is exceedingly difficult, especially from the weak position of a private member's bill in a minority Parliament.

I want to take this opportunity to thank the members for Thunder Bay—Rainy River, Sherwood Park—Fort Saskatchewan, Peace River—Westlock and Shefford, as well as Senator Julie Miville-Dechêne and the table officers of both houses for getting us here today.

With my remaining time, I want to talk about what Bill S-211 is, what it is not and what it could be.

Bill S-211 is a supply chain transparency bill. Companies of a certain size would be expected to examine their supply chains annually and certify that they are free of slave products, or if they are not, what are they going to do about it. Powers would be given to the Minister of Public Safety to examine the filing, and if not satisfied, cause an investigation to be made.

We expect that the mere existence of the bill will create a high level of compliance as companies worry about their reputational damage, government investigations, consumer disapproval and increased financial costs for non-compliance and additional financial risk.

Keeping it simple is the essence of this bill: examine our supply chains; certify there is no slavery; and if there is, tell us what they are going to do about it.

Why Bill S-211? The moral argument is blindingly obvious. No Canadian should be buying slave products, period.

The economic argument is equally blindingly obvious. Canadian workers cannot compete with slaves. Not only are people beggaring their neighbours by depriving them of a job opportunity, but Canada creates its own supply chain vulnerabilities by becoming dependent upon slave nations to produce critical products.

This is dumb on dumb. In our feverish and immoral desire to get the cheapest product any time, any place, anywhere, we deprive ourselves of business labour and economic opportunities. Stupid is an inadequate description.

Bill S-211 is not a due diligence bill. Failure to comply will not expose a negligent company to a human rights lawsuit.

There are two examples of due diligence legislation, Germany and France. The German threshold is 3,000 employees. The French threshold is 5,000 employees. We estimate that instead of the thousands of companies that would be captured by Bill S-211 under our transparency bill, fewer than 100 companies would be captured by a due diligence bill.

Our reading of due diligence legislation is that it has a limited upside with a massive non-compliance on the downside, in effect trying to run before crawling or walking. It may be that the government will in time move in that direction, but Bill S-211, a transparency bill, is what is in front of us for a vote.

I do not want to be presumptuous, but I believe that Bill S-211 enjoys support in the House, as it did in the Senate. Looking ahead, and I know that is dangerous, I do not want this to be a Potemkin bill, a bill that looks good on paper, but is ineffective because the bureaucracy finds all kinds of reasons to not be ready for the implementation date.

We have enjoyed the support of the four ministers to date, and I want to applaud them for following through on the platform commitments made by both the Liberal and Conservative parties in the last election. It will now be up to them to ensure the compliance is as easy as it is effective. Lessons can be learned from the U.K. and Australia, both of which have similar legislation.

This bill would transform Canada from laggard to leader in this space. It would compel all governments to adhere to the same standards that we expect from Canadian businesses. We can hardly impose these standards on businesses, and yet give governments in Canada a free pass.

● (1115)

I know that businesses are gearing up. I can tell from both my emails and my telephone calls. I would hope that Canadian governments will be as diligent in their preparations for the implementation of this bill. As I have said, there is no need to reinvent the wheel. Models for the practicalities of this bill exist in other jurisdictions, and the minister can shape the demands of this bill to produce first-class data and first-class compliance.

In addition, I would encourage the Government of Canada to seek out other governments, in particular the governments of Australia and the United Kingdom, in order to maximize the collective opportunities. A three-nation web of mutually complementary reporting is far more effective than three nations operating individually.

As we can see, this bill is more carrot than stick. I hope that the stick of fines, investigations, naming and shaming will not have to be used too frequently. I am hoping that the carrot will create a high level of compliance deep into the business community to the benefit of us all.

While due diligence legislation may be ultimately the way to go, it is not what is on offer today. Properly executed at this time, I am prepared to trade a high level of compliance from a massively greater number of companies in exchange for a low level of compliance from very few companies.

Finally, this is what others have said about this legislation.

Matt Friedman, CEO of the Mekong Club, who has been in this business for around 30 years, stated, "The importance of this legislation is that it will educate Canadian companies/government agencies about this issue; help companies to look deeper into their supply chains to better understand their potential vulnerability; and ensure that those involved do what is needed to keep workers safe all over the world. It will also allow consumers to see which companies are stepping up to address this topic."

Michael Messenger, president of World Vision, stated, "Canadians don't want to be inadvertently contributing to the child labour crisis every time they shop. As child labour and risky imports continue to rise,—"

They have over the four years that we have been on this file.

"—supply chain laws are imperative to Canada's efforts to protect and promote the rights of boys and girls around the world. With supply chain laws in place, consumers, companies, and the federal government will be able to work together to ensure every purchase in Canada is an ethical one."

Stephen Pike, a partner with Gowling WLG, stated, "Bill S-211 has made outstanding progress to date through the legislative process. The House of Commons should take this unique opportunity right now to advance the interests of Canada and all Canadians in the fight against forced labour and child labour in supply chains."

Lastly, Chris Crewther, the MP for Mornington in the Parliament of Victoria in Australia, stated, "When I was a Federal Member of Parliament...I instigated, led and undertook the Inquiry into Australia establishing a Modern Slavery Act, produced the recommendations in 'Hidden in Plain Sight', and brought about Australia's *Modern Slavery Act....*"

"It has transformed the way Australian businesses, organizations and society looks at the crimes of modern slavery, resulting not only in entities paying attention to and reporting annually on modern slavery in their organizations...but working more deeply to actually look into, eliminate and remediate modern [supply chain] slavery...."

"...I've always adopted the saying: 'don't let the perfect get in the way of the good.' Thus, I encourage Canadian parliamentarians to see [this Bill] through...."

Madam Speaker, this bill is timely, it is broadly supported, it has ministerial buy-in and it puts our nation in a position of leadership. I recommend it to you and to our colleagues.

● (1120)

[*Translation*]

Mr. Yves Perron (Berthier—Maskinongé, BQ): Madam Speaker, I thank my colleague for his speech.

Clearly, there is an incredible amount of support for this bill in the House because it deals with an obvious issue. No one wants to encourage slavery or child labour. One has to wonder why Canada's current legislation and practices allow for the importation of such products. Now is the time to act, so let us do that.

One might also wonder whether the necessary resources will be allocated. It is all well and good to set out good intentions in a bill, but the government needs to put the necessary resources in place and ensure that it has the relevant information.

I had an opportunity recently to give a speech about the situation of the Uighurs and, at that time, I learned about forced labour in certain regions. That issue is also mentioned in this bill.

I would like my colleague to reassure me in that regard. Is his government prepared to allocate the necessary resources so that we have the information we need?

[*English*]

Hon. John McKay: Madam Speaker, those are excellent questions. I wish I could wave a magic wand and give the member the absolute assurance that the government would do that, hence it is the reason for devoting part of my speech to the implementation part of the bill.

The first question is on gaps. Yes, there are immense gaps. In a relevant period of time, the United States has stopped 1,400 container loads of products, which are suspected to have slave components in them. In a similar period of time, we stopped one. It went to a lawsuit and was released. There was none.

We have gaps. I am hoping that this bill would stimulate the government to be far more diligent and devote the resources that are needed.

The resources on this particular—

The Assistant Deputy Speaker (Mrs. Carol Hughes): I have to ask for other questions.

Questions and comments, the hon. member for Peace River—Westlock.

Mr. Arnold Viersen (Peace River—Westlock, CPC): Madam Speaker, I thank the hon. member for his hard work on this file.

Part of the challenge with whatever we are doing on this is that the problem is immense. Could the hon. member talk about some trends in human trafficking around the world, and what is the estimated grand total of enslaved people around the world?

Hon. John McKay: Madam Speaker, the hon. member points to an enormous problem that is ever growing. In fact, I would point to the weekend's newspapers talking about an issue of Mexican labourers in northern Toronto. The numbers are very difficult to come by. Whatever estimates we have are way below the reality. In that respect, it is very difficult.

I want to cover off the issue of resources. I do not think this bill is going to be resource heavy. What it really requires is getting the Aussie and U.K. legislation, looking at them, taking what we think is best for us, putting up a website and making some elements in the public safety ministry responsible for it.

Ms. Jenny Kwan (Vancouver East, NDP): Madam Speaker, Oxfam Canada, Amnesty International and Human Rights Watch want to hold companies accountable for their actions and to allow victims of human rights and environmental harm the statutory rights to bring a civil lawsuit against those companies.

This bill does not do that. The NDP tried to move six amendments at committee to make that change. The government members and the committee members voted against it. Some would argue that not ensuring there is action to hold companies accountable is more damaging than just pretending something is being done.

Why did the government members vote against the amendments that the NDP put forward to address the issues around child labour and modern-day slavery?

Hon. John McKay: Madam Speaker, I take issue with the member saying this would require companies to do nothing. This is a substantial change in practice. That is number one.

Number two is that I disagree profoundly with the analysis the hon. member made. The two places where due diligence legislation has been applied have been ineffective with massive non-compliance. I think it has resulted in one lawsuit over the course of time.

What is on offer here today is not a due diligence bill. It is a transparency bill. I would argue that the Australian, British and other experiences have shown that companies that operate in those jurisdictions are in fact cognizant of their supply chains, much more than in the absence of this legislation.

● (1125)

Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC): Madam Speaker, it is a pleasure to rise today and speak in support of Bill S-211. It is an important bill, and the Conservative caucus supports it. We have sought to advance it through the process, and we look forward to seeing it come into force at the beginning of next year, as per the coming-into-force timelines.

I was in the hon. member's neck of the woods this weekend, in Toronto, having meetings with some different communities that are concerned about various justice and human rights issues that our foreign affairs committee and others have been seized with. I was pleased to meet with the Pakistani Christian community, which continues, among others, to call for a repeal or reform of the blasphemy law in Pakistan.

I met with members of the Ethiopian community, the Tigrayan community specifically, who want to highlight the continuing need for the full implementation of the peace deal, for humanitarian access to Tigray and for support for processes around justice and accountability. I look forward to continuing to work on those important issues as well.

Bill S-211 would take a transparency or disclosure approach to combatting the issue of forced labour around the world. It would seek to encourage companies to take action to combat forced labour in their supply chains by having them report on the activities they are undertaking within those supply chains.

It is not a perfect bill, in that it would not solve every problem. Respectfully, I could probably say that about every piece of legislation that comes before the House. The question for us, at third reading, should not be whether the bill is the full realization of human perfection that is theoretically possibly, but rather would the bill be an improvement on the status quo. I think it very clearly is.

The bill would push companies to be engaged in the process of being accountable about the efforts they are undertaking to combat slave labour. It would seek to also bring further awareness to the reality that many of the products we buy may be tainted by the ongoing scourge of slavery that still continues in the 21st century.

One of the areas where we need to go further, and this is a matter for subsequent legislation, is to take a targeted approach to those very specific hot spots in the world where we know there is a high level of slave labour and the government is complicit in it. We have discussed before in the House the issues of the Uighur genocide, the slave labour and the forced labour that are associated with the repression of the Uighur people.

In the United States, on a bipartisan basis, they have passed something called the Uyghur Forced Labor Prevention Act, which effectively creates a reverse onus for the region of Xinjiang or East Turkestan. The reverse onus is that goods coming out of that region are presumed to have involved slave labour, unless someone can prove otherwise.

This recognizes the reality that many products coming out of that region are tainted by slave labour. As much as one might try, on faith, to say we are banning products made by slave labour, then we are not paying attention to what is going on. In every case, if we require CBSA or other countries' border services agencies to conduct a thorough investigation to know for sure that a product had a problem before it was imported, then we are not going to have an effective approach.

Recognizing the prevalence of slave labour, the government's complicity in that and imposing particular import restrictions, as the United States has done, makes sense. This is the reverse onus presumption that came in through the Uyghur Forced Labor Prevention Act in the United States.

We have seen how efforts to combat forced labour in the United States have led to many shipments being blocked. In Canada, they have not led to a single shipment being blocked. The member across the way said there was one shipment blocked, but my understanding is that shipment was stopped and then subsequently released.

● (1130)

The worst possible consequence so far in Canada, if one is complicit in forced labour, is that one would face a delay. I think that many members on all sides of the House would agree, certainly privately and in many cases publicly, that this is an unacceptable situation.

In general, when it comes to combatting forced labour, we should be thinking more about aligning our approaches with those of other like-minded countries and collaborating on enforcement. Part of our commitment in our free trade deal, the USMCA with our partners in the U.S. and Mexico, is to stop forced labour from coming in. Why, therefore, would we not have common standards, such that if a ship carrying supplies is not able to bring those supplies into the United States on the basis of concerns of forced labour, then that same ship should not be able to shift course and travel to Canada?

We should have a common approach among allies, in which we are sharing information and intelligence as well as working together to enforce these kinds of standards. This would make it a lot easier from a resource-investigation perspective for our country and would help to have that united front to combat the problem of forced labour and modern-day slavery.

These are some of the areas where I think we should be doing more. One is to recognize these hot spots and to acknowledge the need for a specific, targeted approach in the case of these hot spots. Another is to ramp up the enforcement around our existing rules and to try to collaborate more on enforcement.

A couple of weeks ago, I was in Japan for an IPAC conference ahead of the upcoming G7, which is going to be hosted in Japan. I can share that there was a great deal of interest among Japanese legislators for a common approach to these kinds of challenges, including human rights approximated from forced labour. The G7 summit coming up in Japan will be a great opportunity to discuss these things, for these issues to be on the agenda and for the G7 to talk about leading a global approach where like-minded countries share standards, share information and collaborate to prevent products made from forced labour from coming into their countries.

Those are a few of the additional areas, but again, I do not expect one private member's bill to cover everything.

There was some debate at the committee stage of Bill S-211 on whether we should have amendments, and I think I signalled in my second-reading speech that there were some amendments I wanted to propose around the bill. It would have been nice if we had treated the bill earlier in the committee process. However, because of time and the fact that we are in a minority Parliament, if we had passed the bill with amendments, it would have gone back to the Senate and we would have gotten into a sort of ping-pong match that I think would have caused further delay and risked us not passing any legislation.

Recognizing that Canada has been way behind until now on this issue of recognizing the gaps, it makes much more sense to support legislation; move it forward; and then also continue to talk about the problems, the need for further action and what the areas are in which we can strengthen the framework, which we are gradually building.

As well, I know that there were commitments from all of the major parties, including the governing party, to take legislative action on this particular issue. I do not think that Bill S-211 exhausts the obligation to take legislative action. I am still hoping that we see government legislation that would address some of the specific issues I have raised as well as have government engage with our partners and allies. Therefore, I hope that nobody is planning on saying, after the bill before us is passed, that our work is done, because it is not done. However, this is a good bill. Conservatives are pleased to support it and we look forward to seeing it pass into law.

● (1135)

[*Translation*]

Mr. Stéphane Bergeron (Montarville, BQ): Madam Speaker, I first want to address what our Conservative colleague just said. By his own admission, the bill is clearly flawed, but the Conservatives have decided to support it anyway simply to ensure that we do not take more time to get to the bottom of things. To me, that does not seem like the right or appropriate approach to take.

By way of introduction, I want to make three comments, which I hope will be rather brief, before I get into the substance of the matter and explain why we will be voting against this bill at report stage. Here is my first comment.

When he asked his question, my colleague from Berthier—Maskinongé did a great job explaining why we are voting against this bill at report stage. We voted in favour of this bill in principle because we support the idea of having tighter controls on imports coming in from forced labour, slavery and child labour. However, as my Conservative colleague noted, as we listened to some of the witnesses we realized that this bill has major flaws. As the member who introduced it admitted, this is a bill that simply encourages transparency, essentially relies on corporate goodwill, and does not provide for the necessary checks or for what we call due diligence. As my colleague from Berthier—Maskinongé noted, the government will not necessarily follow up to ensure that goods produced from forced labour or child labour are indeed not imported into Canada. I think that is a major flaw of this bill.

As my NDP colleague stated a little earlier, we tried to make some amendments to the bill in committee in light of the testimony we heard. However, the government had absolutely no intention of compromising. Considering the circumstances, we voted against the bill in committee. Consequently, and understandably, we will be voting against the bill given what has been reported today about what happened in committee.

My second introductory comment is simple: I believe that the sponsors of this bill, Senator Miville-Dechêne and the member for Scarborough—Guildwood have very good intentions. I believe that their reasons for introducing this bill are honourable. They put their heart and soul into the bill and worked very hard on it. I believe they deserve our utmost respect for the work that has been done to date, but it is unfortunately not enough for us to vote in favour of this bill.

Third, I simply want to say that there is time before third reading to do something that would allow us to vote for this bill.

With that in mind, I would like to explain why we went from voting in favour of the bill in principle to voting against it in committee and today. As some of my colleagues have pointed out, the bill does not go far enough. It does nothing to ensure that the necessary checks will be performed to confirm that the spirit of the bill is being respected, in other words, to prevent the importation into Canada of goods made with forced labour, slavery or child labour. Beyond the principle, beyond the intentions, there is no follow-up. That is a fundamental flaw in this bill. Several witnesses who appeared before the committee told us that international experience has shown that once legislatures have passed legislation that simply calls for transparency, they stop there and do not go any further. If we want to go further than that, we should not pass a bill that does nothing beyond suggesting transparency.

● (1140)

Some might feel that this bill does nothing more than ease our conscience. It targets transparency and leans on corporate goodwill, but that is all.

My colleague from Edmonton Strathcona put forward amendments to make the bill more hard-hitting, to give it real teeth so we do not have to just cross our fingers and hope companies will get on board. The government and the Conservative Party rejected every single one of her proposed amendments.

Indeed, some people were in a big rush to shut down the committee's work, supposedly to avoid yet more delays, as my Conservative colleague said. Again, I do not think that rushing legislation is the right thing to do, especially when everyone knows the bill has some major flaws.

I asked that the Minister of Labour appear before the committee because there were rumours that the government had prepared a whole slew of amendments to improve the bill. To my surprise, when we studied the bill in committee, there was not a single amendment from the government, although we had been assured that the government had at least 20 amendments. Not a single one was introduced. What happened behind closed doors? I have absolutely no idea.

From what I understood, the Minister of Labour was persuaded by a number of people, including probably one of the sponsors of the bill, to withdraw the government's amendments and propose a more robust bill instead. I thought that was great, and I wanted the minister to come tell us about it publicly in committee. We invited him, but he declined.

I ran into the minister by chance at an event. He told me that he did not want to appear before the committee to say he had nothing to say because there were no amendments. That being said, he did tell me he intended to introduce a more robust bill along the same lines as Bill S-211.

I told him that that was great and asked him why he would not appear before the committee to tell us about it. He told me that he did not yet have the bill in his hands and he did not want to appear before the committee to say that the bill was not ready yet. I replied that, in that case, he needed to find a way to make public the government's intention in order to allay the concerns of some non-governmental organizations, or NGOs, that the bill would provide only for the transparency measure and would not go any further to ensure the necessary due diligence.

Since then, the minister has not made any public commitment to that effect, so the message he has been sending thus far is not very encouraging. There is still time, however, because we are approaching third reading stage.

In his speech, my colleague referred to a letter he sent to all members on February 28. That letter said this bill will transform Canada from laggard to leader on this issue.

I am sorry, but it takes more than just passing a bill on transparency to be a leader. If the government's position is that transparency would make Canada a leader, then I have concerns. That says to me that the Liberals do not have any real intentions of going further.

Accordingly, I have no choice today than to be consistent with the decision we made in committee and say that at report stage, the stage where we report on what happened in committee, we are voting against this bill. However, I want to assure my colleague, as I did in committee, that we are still open to the possibility of voting in favour of the bill at third reading provided we get a commitment from the government that it is ready and willing to go further than just passing a bill on transparency.

If my colleague can convince the minister to follow through on the informal commitment he made in my presence, he can be assured that we will vote in favour of the bill at third reading stage.

● (1145)

[*English*]

Ms. Jenny Kwan (Vancouver East, NDP): Madam Speaker, today we are debating Bill S-211, which claims to fight against forced labour and child labour in supply chains. There is no question that global supply chains continue to be tainted with forced labour and child labour. Millions of people around the world experience conditions of modern slavery. Horrifically, this includes young children who, too often, harvest the food we eat and manufacture the clothes we wear.

Sadly, progress toward eradicating child and forced labour has stalled and even reversed during the COVID-19 pandemic. In 2020, the report from the International Labour Organization warned that child labour was increasing for the first time in two decades. Between 2016 and 2020, the number of children in child labour increased to 160 million worldwide; 79 million of these children, some as young as five years old, are working in conditions considered to be hazardous, which means that the work is likely to harm their health, safety and morals.

Economic impacts of the pandemic, leading to school closures and income loss among low-income families globally, have pushed more children into these dangerous working conditions to try to earn a living. The reality is that forced labour conditions exist in nearly every country. Canada is deeply implicated in perpetuating these human rights abuses. Under the current legislative framework, there is no corporate accountability for companies that profit from the exploitation in their supply chains.

According to a report from World Vision in 2016, it is estimated that over 1,200 companies operating in Canada are importing over 34 billion dollars' worth of goods at high risk of being produced by child or forced labour every year. The agricultural and grocery industry is one of the worst offenders for forced labour and child labour: 71% of all child labour takes place in the agricultural sector, and many of these items end up on Canadian grocery store shelves.

In 2019, more than 3.7 billion dollars' worth of risky food products were imported into Canada, a 63% increase from 10 years ago. During the same pandemic period when Canada's major grocery chains raked in record profits, the use of child and forced labour in agricultural supply chains increased. As Canadians get gouged with greedflation at the grocery checkout, corporate giants fail to take action on ending forced and child labour in their supply chains. World Vision reported that corporate social responsibility reports from Loblaws, Metro and Sobeys, Canada's three largest grocers, yield "little meaningful information about what they are doing to address the risk of child labour in their supply chains." There are record profits, yet zero accountability to respect human rights. This is egregiously wrong.

Unfortunately, we know that these issues extend far beyond the agricultural sector. In 2021, CBC reported that Canadian clothing brands sold items manufactured by North Korean forced labour at a Chinese factory. Recently, I spoke about the genocide against Uighurs and other Turkic Muslims. This is again relevant to raise, because these issues are connected. Many products sold in Canada are manufactured with Uighur forced labour. Between 2017 to 2019, it is estimated that more than 80,000 Uighurs were forcibly transferred out of the Uighur region to work in factories across China. In 2020 alone, reports reveal that 83 global companies were indirectly or directly involved in employing Uighur workers under conditions of forced labour. From food products, clothing and textiles to the supply chains of major auto manufacturers, the use of Uighur forced labour is widespread.

Canada can and must do more to uphold human rights and work to eradicate child and forced labour. The NDP wants to ensure that products imported into Canada are not produced with forced labour or child labour. New Democrats believe that Canada has a responsibility to ensure that supply chains of products sold in Canada are free from these egregious human rights violations.

The government has an international human rights obligation to do this, but due to the inaction of successive Liberal and Conservative governments, Canada is lagging behind other jurisdictions. European countries such as France have already passed due diligence legislation, which requires that companies take action to address child labour and forced labour. Importantly, this also provides legal recourse if efforts are shown to be inadequate.

● (1150)

The Canadian Network on Corporate Accountability has been calling for human rights and environmental due diligence legislation in Canada. The organization has even drafted model legislation, providing a blueprint for writing into Canadian law the corporate duty to respect human rights and the environment.

For over a decade, the CNCA has also been calling for an independent ombudsperson office with the power to investigate human rights complaints related to Canadian corporate activity abroad. The Liberals announced that they would create this independent ombudsperson office in 2018, yet today this is just another empty promise from the government. Instead, the government has created a powerless advisory post.

It is clear that there is much work to be done. That is why NDP members, in working with policy experts on these issues, have put forward two critical pieces of legislation. Bill C-262, the corporate responsibility to protect human rights act, would implement the human rights and environmental due diligence that is needed. It would hold companies accountable for their actions and allow victims of human rights and environmental harm the statutory right to bring a lawsuit against that company. Bill C-263 would give the Office of the Canadian Ombudsperson for Responsible Enterprise the powers needed to actually do its job and investigate and hold companies accountable.

The CNCA, which includes member groups such as Oxfam Canada, Amnesty International Canada and Human Rights Watch Canada, supports these steps, but it is yet to be seen whether other parties will do the right thing.

Today, we are here debating Bill S-211. From the outset, the NDP recognized that this bill was deeply flawed. New Democrats agree with the view that CNCA shares: that, unamended, this bill is damaging because it creates the appearance of action to end modern slavery without actually having that effect. As currently drafted, Bill S-211 advances none of the essential elements of an effective supply chain law.

According to the CNCA:

> Bill S-211 would require companies to report on what steps, if any, they have taken to prevent and reduce the risk of forced or child labour in their supply chains. It would only apply to a small minority of companies; it does not require these companies to stop using child or forced labour or to conduct human rights due diligence; and it is silent on other egregious human rights abuses (such as mass rape, murder and torture), as its focus is limited to child or forced labour.

Recognizing the flaws of this bill, the NDP proposed six amendments at committee stage to improve the legislation based on expert testimony, yet the government rejected all of them.

Canada needs to do much more to fight forced labour and child labour. The Minister of Labour's own mandate letter instructs him to "introduce legislation to eradicate forced labour from Canadian supply chains and ensure that Canadian businesses operating abroad do not contribute to human rights abuses."

Bill S-211 fails to do that. Therefore, the NDP will be voting against this legislation. We will continue to advocate for legislation that actually addresses the issue and commit to eradicating forced labour and child labour. Having the appearance under this bill to be doing something is not good enough.

Mr. Sameer Zuberi (Pierrefonds—Dollard, Lib.): Madam Speaker, I would like to thank all the members who have expressed themselves thus far on this extremely important piece of legislation, Bill S-211.

We need to take a step back and look at the path this bill has taken. First off, the very notion of forced labour being enacted into legislation has been something that this Parliament has been discussing for several years. Thankfully, we are on the cusp of actually passing something: from the vantage point of where we are currently of having nothing in terms of a piece of legislation that directly deals with forced labour to having a piece of legislation that will address forced labour head-on.

We can just take a step back and look at how procedure works. We know that it would be great to strengthen this legislation, but if we were to do so, it would require us to go back to the Senate to have those amendments approved within the Senate, and then it would have to wind its way back over here to the House, which would create a significant delay for us to actually pass something. That is why this is a moment that we actually must seize to pass this legislation.

In terms of Bill S-211, I would like to thank Senator Miville-Dechêne and the member for Scarborough—Guildwood for their advocacy on this issue and for shepherding this and bringing it to the point where we see it right now.

This legislation requires that large companies and the federal government examine supply chains and identify forced labour, so they have to go through their supply chains, which is a lot of work. It also has a compliance mechanism. Therefore, it has teeth. It would levy significant fines on companies that do not comply with the legislation, for up to $250,000. That is important, not only in terms of the monetary amount, but also in terms of the naming and shaming of those companies, which I will get to later on. The naming and shaming of companies, if they do not comply with this legislation, is quite powerful. It also requires that companies provide reports in terms of how their supply chains are operating and whether there is forced labour or child labour within those supply chains.

There is an added component in terms of teeth with this legislation, which gives the minister the authority to ban imports of products if this legislation is not respected by companies. It also gives power to the minister to have warrants to seize information within companies to ensure that there is compliance with the legislation. This is not just a value statement or an airy-fairy piece of legislation. It actually has teeth and mechanisms to force compliance.

Thus far, several of our allies, such as the United Kingdom and Australia, have similar legislation to this. This is critical so that we can send a signal to companies that forced labour is unacceptable. The Canadian government thus far has addressed this issue of forced labour and child labour through trade agreements that it has with other countries, but Bill S-211 will make it more robust.

A lot has been said about the Uighur region within the debate on Bill S-211. It has been highlighted that America has an interesting piece of legislation around a rebuttable presumption, where everything coming in from the Xinjiang Uighur Autonomous Region is assumed to be produced with forced labour. This chamber has discussed the condition of the Uighur people, that at least one million are in camps where they are forced into labour. This chamber has heard that 48% of polysilicon, which is the base product of solar panels, is produced within the Uighur region. We have heard that 20% of cotton is produced within the Uighur region, and 35% of tomato products, which are the base material of pizza, pasta sauce, etc., are also produced within the Uighur region.

This is an issue that we have been seized by. This legislation would help us address that concern, to ensure that Canadians are not unwittingly importing forced labour products. While I would love to see and do hope that there will be more robust legislation in the future, I think this legislation, as it is currently, is an important mechanism and an important addition to what is already out there. As some have said, having something is better than having nothing, and we are going to do something important by passing this.

● (1155)

I would like us to take a step back and think about what happened several years ago in Bangladesh, when we learned about the garment industry and the factories that were destroyed. That caused us, as Canadians, to reflect upon where our goods are produced and the conditions in which our clothing is manufactured and created, and to be mindful about forced labour.

That really made us think about the products we are purchasing and ask a serious question: Are our products being produced by labour in terrible conditions, through forced labour or child labour? At that point in time, some companies were named and shamed. Canadians asked for a much higher standard with respect to the products that were being produced in these garment factories.

That is exactly what this legislation will do. It will give a chance for companies to be held accountable. If they do not reach the standard required or if we look at their supply chains and see that their products are produced from forced labour, they will be named and shamed. That is the power of this legislation. Similar to how several years ago the garment industry in Bangladesh was looked at critically and examined carefully, companies in the future would be given the same scrutiny.

I would also like to highlight that certain companies have actually stepped up and taken a hit in dealing with forced labour. H&M is one of those companies. It has pulled out of the Xinjiang Uighur Autonomous Region and ensured that it is not taking goods and content produced within that region. We need to highlight the positive examples.

I will conclude by saying that it is important for Canadians, and not only legislators and those in government, to highlight this issue and pass laws around it. However, it is also important for Canadians to demand that their companies not take goods that are produced from forced labour and child labour. It is through this call that companies will change their behaviour. Canadians have asked that companies go green, that we produce goods that are respectful of the environment. This same call needs to be made when it comes to respecting labour and the workforce.

I will leave it at that. I am happy that members of the loyal opposition are supporting this legislation. I would ask that all parties in this House do the same, the reason being that we need to have something on the books that holds companies to account. This legislation not only puts out important values but also has teeth.

● (1200)

The Assistant Deputy Speaker (Mrs. Carol Hughes): The time provided for the consideration of Private Members' Business has now expired, and the order is dropped to the bottom of the order of precedence on the Order Paper.

GOVERNMENT ORDERS

[*English*]

TELECOMMUNICATIONS ACT

The House resumed from December 1, 2022, consideration of the motion that Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, be read the second time and referred to a committee.

Mr. Gerald Soroka (Yellowhead, CPC): Madam Speaker, I will be splitting my time with the member for Kootenay—Columbia.

I am pleased to rise in the House today to speak to Bill C-26, the critical cyber systems protection act, introduced in June 2022 and split into parts 1 and 2. The former aims to amend the Telecommunications Act to include:

> the promotion of the security of the Canadian telecommunications system as an objective of the Canadian telecommunications policy and to authorize the Governor in Council and the Minister of Industry to direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system.

The latter outlines the introduction of the critical cyber systems protection act, which would create a new regulatory regime requiring designated critical infrastructure providers to protect their cyber systems.

I would like to emphasize that the safety and security of our telecom industry, with particular reference to foreign adversaries such as the Beijing Communist Party, has been a broad theme in communications lately. This is especially concerning the controversial Bill C-11, the online streaming act, or, should I say, government censorship, and new revelations from the Canadian Security Intelligence Service, CSIS, flagging election interference from those involved with the Beijing Communist Party.

We Conservatives believe it is of paramount importance to defend the rights and interests of Canadians from coast to coast to coast. Thus, Canada's national security should be strongly well equipped to be prepared for cyberwarfare threats that could be presented by emerging digital technologies, intelligent adversaries or authoritarian artificial intelligence.

The NDP-Liberal government has had a long record of denying Canadians the truth. Instead of protecting their rights and freedoms, the government uses deflection tactics to divide Canadians, pitting them against one another to distract from the real issue: that the NDP-Liberal government has been too slow to address cyberthreats. For this critical lack of action, Canada has seen several serious incidents occur with no substantive legislative response for over seven years. After years of chronic mismanagement and utter failure, it is time for the government to step aside and let the Conservatives turn Canadians' hurt into hope.

We support the stringent and thorough examination of this legislation. We will always defend and secure the security of Canadians, especially with regard to cybersecurity in an increasingly digitized world. There is a pressing demand to ensure the security of Canada's critical cyber-infrastructure against cyber-threats. Let us not forget that these very systems lay the foundation of the country as a whole. It is these cyber systems that run our health care, banking and energy systems, all of which should be guarded against the cybercriminals, hackers and foreign adversaries who want to infiltrate them.

Akin to several other Liberal ideas, a number of aspects of this bill require further review, and it should thus be sent straight to committee where it can be further dissected and refined to ensure that all flaws are addressed. One can only imagine the disaster that a hospital system crash would add to the already horrible wait times in emergency rooms and shortages of medical professionals thanks to the NDP-Liberal government. The results would be disastrous. Furthermore, disruption of critical cyber-infrastructure in health care can bring severe consequences, such as enabling cybercriminals to access confidential patient health care information.

While we understand that it is imperative to provide the resources necessary to effectively defend against cyber-threats, it is still equally important to ensure that the government does not overreach on its specified mandate through Bill C-26. A research report written by Christopher Parsons called "Cybersecurity Will Not Thrive in Darkness" highlights some recommendations to improve Bill C-26. Among these recommendations is an emphasis on drafting legislation to correct accountability deficiencies, while highlighting amendments that would impose some restrictions on the range of powers that the government would be able to wield. These restrictions are critical, especially concerning the sweeping nature of Bill C-26, the critical cyber systems protection act, as outlined in parts 1 and 2, which I have explained in my opening statement.

● (1205)

The sweeping nature of this legislation is not new, particularly for the Liberal government. It even goes back to Bill C-11, the online streaming act, which essentially placed the Liberal government as the online content regulator controlling what Canadians see or listen to online. If members ask me, the government policing what Canadians view online is a cyber-threat in its own way, but I will not get into that right now.

There are other flaws in Bill C-26 that I would like to highlight, which brings us back to having Bill C-26 closely reviewed in committee.

In terms of civil liberties and privacy, some civil liberties groups have flagged serious concerns regarding the scope and lack of oversight around the powers that may be granted to the government under Bill C-26. In September last year, the Canadian Civil Liberties Association, along with other groups, released a joint letter of concern regarding Bill C-26, highlighting that the bill is "deeply problematic", like several other questionable Liberal policies. They went on to further explain that Bill C-26 "risks undermining our privacy rights, and the principles of accountable governance and judicial due process".

From an economic perspective, the bill lacks recognition of foreseeable impacted enterprises, such as small and medium-sized businesses, which will undoubtedly bring forth unintended consequences. According to the Business Council of Canada, some concerns include the lack of transparency seen through the one-way sharing of information. This brings about serious concerns. Operators are required to provide information to the NDP-Liberal government, yet those same operators are not entitled to receive any information back from the government or other cyber-operators. This whole information-sharing regime is lacking and, simply put, completely misses an opportunity to implement a transparent information-sharing system that would benefit all parties involved.

There is also concern regarding government overreach. Considering what powers would be granted to the government to order what a telecommunications provider has to do under Bill C-26, I would have expected to see sufficient evidence to support this overreach. However, that was not addressed at all, if not vaguely, in this bill. This, on top of blatant disregard for the recognition of privacy and other charter-protected rights, proves how the government only cares about granting itself more and more power, even in the face of blatant transparency and accountability concerns like election interference or the Bill C-11 censorship bill.

I only highlighted a few of the several highly valid concerns regarding this critically flawed bill. Obviously, it is important to defend national cybersecurity and defend against cybercriminals or foreign threats. However, there is a fine line between upholding the best interests of Canadians and just using another faulty bill as a power grab for the NDP-Liberal government, despite concerns regarding cyber systems, privacy and security infrastructure.

We Conservatives believe that it is of paramount importance to truly defend the rights and interests of Canadians from coast to coast to coast. One of the best ways this can be done is by securing Canada's cyber-infrastructure from attacks. While we welcome the idea of protecting the interests of Canadians in terms of cybersecurity, we want to flag that Bill C-26 has some highly concerning content that should be closely reviewed and discussed in committee to correct flaws and prevent potential overreach from the NDP-Liberal government. In the interest of protecting Canada's cyber-infrastructure, we must also guard against the sweeping government powers outlined in the critical cyber systems protection act.

● (1210)

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, on the one hand, the member says that he is really concerned about cybersecurity, and then on the other hand, the member is saying that the government is doing too much and that he is concerned about overreach and is very skeptical. Then he uses examples of health care and talks about waiting lists and so forth. I am a bit confused about exactly where the Conservative Party is with respect to the legislation.

Would the member not agree that, at the very least, many of the issues or concerns he raised might be somewhat irrelevant to the debate and that parts of his comments would probably be better served if the bill went to committee? He seems to give me the impression in his comments that the Conservative Party supports the principles of the legislation. Does the member believe that he will be voting in favour of the bill so that it can go to committee?

● (1215)

Mr. Gerald Soroka: Madam Speaker, yes, I think we will be voting in favour of the bill. The problem is that although the bill would address the fact of cybersecurity as a very important thing we need to deal with, it seems like every type of legislation the Liberal government puts forward would also take away our rights and freedoms as Canadians. The Liberals always try to make sure the government is in charge, controlling what we can or cannot do. I think that is quite evident in this legislation when they start talking about one-way sharing of information.

[*Translation*]

Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ): Madam Speaker, I agree somewhat with my colleague. Sometimes, the Conservatives want their bread buttered on both sides, especially when it comes to cybersecurity or Internet bills. They support the principle, but oppose the intervention. It is difficult for them to find the right balance.

My colleague did not address the concerns. He spoke instead about Bill C-11, which is a very important bill for the promotion of French content on the Internet, but which was blocked by my Conservative friends.

Over the past two break weeks, I spoke with many Quebec artists. The Union des artistes fervently hopes that Bill C-11 will pass so that French content will be promoted on line. It is extremely important. However, the Conservatives are stonewalling. They did so in committee, and even now, they are delaying the work in this place.

How does my colleague feel about the fact that all Quebec and francophone artists across Canada are against his party?

[*English*]

Mr. Gerald Soroka: Madam Speaker, I think there is some confusion as to what we do and do not stand for. I believe there are a lot of opportunities in Canada when it comes to online streaming and how we can get our products out to market. However, when we start talking about Bill C-11, we start talking about censorship and what can or cannot happen here in Canada. Everyone talks about how we are going to protect the rights of our artists, but I am very concerned about the time when the censorship starts taking place and Canadians actually start understanding there is going to be content that would not be allowed to be viewed. I sure hope the member is right that there will not be such censorship, but I am afraid he could be mistaken.

Mr. Kevin Lamoureux: Madam Speaker, I am pleased the member is going to vote in favour of the legislation. Could he provide a specific example within the legislation that he would say is government overreach?

Mr. Gerald Soroka: Madam Speaker, that was probably the briefest time I have ever heard the member speak in the House; it is shocking. I will do my best as well.

When we start talking about information sharing, all these companies have to provide information as to what they are doing to make cybersecurity safe in Canada. However, the government is not reaching out to the same companies and people to say what it is hearing about and what it is understanding. That is one of the biggest problems; it would not be a two-way sharing system but only a one-way sharing system. Once again, the government is trying to control what Canadians can or cannot do.

Mr. Rob Morrison (Kootenay—Columbia, CPC): Madam Speaker, it is always an honour to rise in the House, especially when I can talk about safety and security.

I always try to enhance safety and security for Canadians at home and abroad, for our corporations that are major contributors to our economic base, and of course, for government institutions. Today, discussing cybersecurity in Canada is an opportunity to enhance our country's ability to protect us from cyber-threats.

Security is a significant concern for all Canadians. Lately, with the rise in organized crime and gang offences to the tune of a 92% increase in gang crime, I have to wonder when the government will be led by evidence, or in other words, provide evidence-based action. It is extremely important for our country to have cybersecurity to protect itself from threats, and I welcome Bill C-26. However, I am apprehensive about how successful this bill may be since accountability is a question that the opposition brings up every day in this House.

Bill C-26 is basically divided into two parts. The first part aims to amend the Telecommunications Act to promote the security of the Canadian telecommunications system. It aims to do this by adding security as a policy objective to bring the telecommunications sector into line with other infrastructure sectors.

By amending the Telecommunications Act to secure Canada's telecommunications systems and prohibit the use of products and services provided by specific telecommunications service providers, the amendment would enforce the ban on Huawei Technologies and ZTE from Canada's 5G infrastructure, as well as the removal and termination of related 4G equipment by 2027. Of concern is the time it took the government to react to enforce the ban on Huawei.

The second part aims to enact the critical cyber systems protection act, the CCSPA, which is designed to protect critical cybersecurity and systems that are vital to national security or public safety or are delivered or operated within the legislative authority of Parliament. The purpose of the CCSPA is to ensure the identification and effective management of any cybersecurity risks, including risks associated with supply chains and using third party products and services; protect critical cyber systems from being compromised; ensure the proper detection of cybersecurity incidents; and minimize the impacts of any cybersecurity incidents on our critical cyber systems.

The effects of this bill will be far-reaching, and there are some points to consider: The government would have the power to review, receive, assess and even intervene in cyber-compliance and operational situations within critical industries in Canada. There would also be mandatory cybersecurity programs for critical industries, as well as the enforcement of regulations through regulatory and law enforcement with potential financial penalties.

Under both provisions, the Governor in Council and the Minister of Industry would be afforded additional powers.

If any cybersecurity risks associated with the operator's supply chain or its use of third party products and services are identified, the operator must take reasonable steps to mitigate these risks. While the bill does not indicate what steps would be required from the operators, such steps may be prescribed by the regulations during a committee review.

The act also addresses cybersecurity incidents; a cybersecurity incident is defined as an:

> incident, including an act, omission or circumstance, that interferes or may interfere with
>
> (a) the continuity or security of a vital service or vital system; or
>
> (b) the confidentiality, integrity or availability of the critical cyber system
>
> touching upon these vital services. It does not indicate what would constitute interference under the act.

In the event of a cybersecurity incident, a designated operator must immediately report the incident to the CSE and the appropriate regulator. At present, the act does not prescribe any timeline or indicate how "immediately" should be interpreted. Again, there is an opportunity to address this at committee.

There are some concerns with Bill C-26 as it is presently drafted. What the government might order a telecommunications provider to do is not clearly identified. Moreover, the secrecy and confidentiality provisions of the telecommunications providers to establish law and regulations are not clearly defined.

● (1220)

As has been brought up today, potential exists for information sharing with other federal governments and international partners, but it is just not defined. Costs associated with compliance with reforms may endanger the viability of small providers. Drafting language needs to be in the full contours of legislation, and that could be discussed at committee as well. In addition, there should be recognition that privacy or other charter-protected rights exist as a counterbalance to proposed security requirements, which will ensure that the government is accountable.

Some recommendations, or ones derived from them, should not be taken up, such as that the government should create legislation requiring the public and telecommunication providers to simply trust that the government knows what it is doing. Of course, this is a challenge. Telecommunications networks and the government must enact legislation to ensure its activities support Canada's democratic values and norms of transparency and accountability.

If the government is truly focused on security for Canadians, should we not be reviewing our gang and organized crime evidence? Our present policies have failed. Should we not look at the safety and security of our bail reform in an effort to prevent innocent Canadians from becoming victims?

Bill C-26 is a step in protecting Canada from cybersecurity threats. What is the review process to ensure compliance and effectiveness, as well as that goals are met?

In terms of bail reform, even though the evidence clearly shows that Bill C-75 has failed, we see that the NDP-Liberal government is not interested in reviewing bail reform. Cybersecurity is important to our country's security; so are victims of crime after their safety and security has been violated.

I am concerned that the government is struggling with evidence-based information to review Bill C-26, as it has with Bill C-75 and Bill C-5. These bills are not supported by evidence. In fact, offenders and criminals have a higher priority than victims do. My concern is as follows: If Bill C-26 requires amendments and review, will the government follow up? It is so important to be flexible and to be able to address changes, especially in a cybersecurity world, which changes so rapidly.

Bill C-26 proposes compliance measures intended to protect cybersecurity in sectors that are deemed vital to Canadian security. Therefore, although late out of the gate, Bill C-26 is a start. However, since this bill proposes compliance measures intended to protect cybersecurity in sectors that are deemed vital to Canadian security, I would like to see individuals, corporations, and most importantly, the government held accountable. There should also be measures to ensure that the objectives of the bill are met and that there is a proper review process.

As I have stated, government accountability has not been a priority. For the proposed bill to succeed, there have to be processes for review and for updating the critical cyber systems protection act.

The failure of Bill C-75 on bail reform is clear with recent violent acts by murderers and individuals who should never have been out on bail. Today we are debating Bill C-26, and I would hope that there are lessons learned from our failure to review Bill C-75. In addition, we can learn from the failure of Bill C-5, as gang violence and organized crime rates are up 92%. Surely the government will open a door for review and making required changes to Bill C-26 on cybersecurity.

I am thankful for the time to speak on the responsibilities related to cybersecurity.

● (1225)

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, we have seen an explosion in the impact of the digital world around the globe. Here in Canada, our systems are very complex, and we have some that are absolutely critical, which need to have the proposed protection.

We have a progressive government that is looking at this in a very serious manner. This is why we are bringing forward this legislation and recognizing the impact of cybersecurity threats. The opposition seems to support the principle of the legislation.

The member has recognized a number of areas in which he would like to see better definition and more details. I would suggest to the member that much of what he is looking for could best be had at the committee stage. If we get the bill to committee, could we look at what he is talking about in more detail? What are his thoughts on that?

Mr. Rob Morrison: Madam Speaker, the member is right. When we get to committee, we can iron out some of the flaws that we have seen in Bill C-26. It is going to be important to focus on accountability and the member did not address that. That is where this bill can either succeed or fail. We need to ensure there is an accountability process for the government, so when it follows through with Bill C-26, we have a process and we can go back and say we need to tweak or change something because cybersecurity changes so fast.

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Madam Speaker, we have been hearing details about the impact this bill could have. I would like to hear my colleague's thoughts on the following question. Why are we always in reaction mode?

In 2019, the Standing Committee on Access to Information, Privacy and Ethics was looking at how to separate information pertaining to social insurance numbers in order to protect citizens' privacy.

What message does this bill send? Yes, a structure exists. Yes, there are correspondents, organizations and individuals who will have more power and potential accountability, but what is behind all of this? Are the Liberals trying to clear their conscience for all the scandals of the past few years?

I would like to hear my colleague's thoughts on that.

● (1230)

[*English*]

Mr. Rob Morrison: Madam Speaker, I am not too sure what the specific scandals were, but this bill certainly opens the door for information sharing and, as was brought up, intelligence sharing, and, through accountability, we can cover those. We can actually be accountable in how we share information safely and we can protect the rights of Canadians.

Mr. Terry Dowdall (Simcoe—Grey, CPC): Madam Speaker, I want to thank the hon. member for his speech today and for his many years in law enforcement. He certainly knows a lot about this file. Throughout the member's speech, the number one word he used, and we can check Hansard, was "accountability", and also the frustration with the Liberal government on a lot of the bills that have been passed.

How does he feel on this particular bill on accountability?

Mr. Rob Morrison: Madam Speaker, in the last several months, we have seen accountability raise its head here in Parliament with Bill C-5, Bill C-75 and Bill C-11. Without accountability, it is as though the government does not actually care what we are doing because with a majority government, the NDP and Liberals can make decisions based on what they think is right and there is no accountability.

With Bill C-5, the evidence is not there. Bill C-21, taking legal guns from legal gun owners, is another non-evidence-based process. With Bill C-26, which we are talking about today, it is time that we start building in some processes for accountability so the government is actually accountable for what it is doing.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Madam Speaker, I am very pleased to be joining the debate today to offer some of my thoughts and perspective on Bill C-26, a much awaited bill on a cybersecurity infrastructure.

Bill C-26 is a good reminder to members that the Department of Public Safety and its subject matter is so much bigger than just firearms, because, of course, firearms and Bill C-21 have been dominating the news cycle for the last couple of months. That bill, in particular at the public safety committee, has occupied so much time and wasted so many resources. Bill C-26 is a good reminder that with cybersecurity we have so many other agencies that are dedicated to national security under the umbrella of public safety. Cybersecurity is a big subject matter. We also have Bill C-20, which is an important bill on oversight and accountability for both the CBSA and RCMP.

Today, we would not find many members in the House of Commons who are arguing against the need for better cybersecurity. All of the evidence out there points to this being a new and evolving threat. Artificial intelligence systems offer some interesting advantages, but with those advantages come threats and with those threats come actors who are determined to use them in nefarious ways that will harm and have harmed Canada's interests. We need a whole host of options to counter this threat. We need our national security agencies to take these threats with increased importance. We also need legislation to fill in the gaps and make sure that all of Canada's laws are up to date.

I have spent a lot of time on the public safety committee. We did a couple of reports that directly touched on this area. One of our first reports identified violent extremism. Our most recent study looked at the threat posed by Russia. We know that since Russia conducted its invasion of Ukraine, which has recently passed the one-year anniversary, it has also increased the threats that it offers to Canada and to like-minded countries. One of those areas is cybersecurity.

Our committee has not yet tabled its report, which should be tabled in the House of Commons soon so that members of the House and the public can not only see the results of the deliberations, but also see the important recommendations that the committee is going to make. However, we heard a lot of testimony during those committee hearings on the cyber-related threats from Russia. Many witnesses identified that those are among the most serious and relevant for Canada's public safety and national security, particularly in relation to critical infrastructure.

I want to set this table before I get into the nuts and bolts of what Bill C-26 is offering, but also set some of the problems that are in evidence with this first version of the bill.

We have to understand a few basic terms. The Government of Canada refers to critical infrastructure as the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government", whether that is the federal government, the provincial governments or our municipal governments. Because so many of those pieces of critical infrastructure are now tied into computer systems that are vulnerable to attack, a bill like this becomes quite necessary.

I could go on and on about all of the critical systems in our modern society and the range of sectors, from our energy production to our food distribution systems to our electricity grid and transportation networks and how our ports and our banking system work. If one were to interrupt any one of those services, it could create absolute havoc within any Canadian community or countrywide.

● (1235)

One of the witnesses we had during our public safety meetings on the topic of the threats posed from Russia, and this was just talking about the cyber-threat more broadly, was Jennifer Quaid, Executive Director of the Canadian Cyber Threat Exchange. She reminded our committee that there are nation-states that are conducting espionage and statecraft through the Internet, but there are also criminals who are engaging in cybercrime for financial gain.

In some cases, those criminal groups and the nation-states are working together. There is evidence of this not only in Russia but in places like North Korea and China, where it is almost like the policy that was in place back in the 1700s and 1600s, where privateers would go out and do a nation-state's bidding. In this modern-day version of that policy, there are criminal organizations that are working hand in glove with some nation-states to give them some plausible deniability, but the systems they are using do pose a very real threat to Canada.

One of our key witnesses during the study was Caroline Xavier, Chief of the Communications Security Establishment. She was not able to go into much detail or specifics, given the very sensitive nature of the topic, but she was able to assure the committee that cybercrime is absolutely the most prevalent and most pervasive threat to Canadians and Canadian businesses. She observed that the state-sponsored cyber programs of China, North Korea, Iran and Russia posed the greatest strategic threat to Canada, and that foreign cyber-threat activities have included attempts to target Canadian critical infrastructure operators, as well as their operational and information technology.

Leaving aside the government, it is important for members to realize that most of Canada's critical infrastructure is, by and large, in the hands of the private sector. This is going to underline some of the important elements of Bill C-26.

We also had testimony from David Shipley, Chief Executive Officer of Beauceron Security. He was relaying the same stuff about Russian criminal organizations working in tandem with the government, and saying that criminal gangs have crippled Canadian municipalities. They have gone after health care organizations. The range of malicious cyber-activity has absolutely extended to many small and medium-sized enterprises.

When we look at the reporting requirements of Bill C-26, one of the biggest gaps that we have in our system is the fact that many businesses, private enterprises, are loath to report the fact that their systems have experienced a cyber-attack. They may be threatened to not do so. There is also a very real concern about the institutional harm that could come from the public release of said information. A large corporation that relays to its customers that it has experienced a cyber-attack may find people are loath to do business with it if they are unsure that its systems are up to par.

I also want to highlight a recent example from 2021, where the Government of Newfoundland and Labrador experienced a health records cyber-attack on October 30. The investigation revealed that over 200,000 files were taken that contained confidential patient information.

One can just imagine that in a province the size of Newfoundland and Labrador the fact that over 200,000 files were taken, that is a shocking theft of personal and confidential information. It really underlines just how important addressing this is.

I also want to touch briefly on the topic of artificial intelligence. I want to read a quote from a recent *Hill Times* article. This is from Jérémie Harris who is one of the co-founders of Gladstone AI, which is an artificial intelligence safety committee. He says:

> But perhaps more concerning are the national security implications of these impressive capabilities. ChatGPT has been used to generate highly effective and unprecedented forms of malware, and the technology behind it can be used to power hyperscaled election interference operations and phishing attacks. These applications—and countless other, equally concerning ones also enabled by new advances in AI—would have been the stuff of science fiction just two years ago.

● (1240)

He goes on to say:

> ...ChatGPT is a harbinger of an era in which AI will be the single most important source of public safety risk facing Canada. As AI advances at a breakneck pace, the destructive footprint of malicious actors who use it will increase just as fast. Likewise, AI accidents—now widely viewed by AI safety specialists as a source of global catastrophic risk—will take more significant and exotic forms.

Something all members of the House really have to be aware of is how, just in the last two years, AI has advanced so quickly. We can think about what AI will be capable of two years or a decade from now. Just as Mr. Harris said, what it is doing right now was inconceivable just two years ago. The fact that AI is now being used to generate unique code for malware indicates there is no telling what it can be used to do and how it could be used to wreak havoc. That underlies just how important this issue is and how seriously we, as parliamentarians, have to take it as we serve our constituents and do the important work of equipping our nation with the tools it needs to keep Canadians, and the critical infrastructure they depend upon, safe.

When I was a member of the public safety committee, I had a chance to speak with Mr. Harris. I actually put a motion on notice that the committee should be undertaking a study on the range of threats posed to Canada's public safety, national security and critical infrastructure, specifically by AI systems. I hope one day the committee can take that study up, but it is a committee with a very heavy workload. It is still trying to find its way through Bill C-21. It is waiting for Bill C-20 to arrive on its door and, of course, this bill, Bill C-26, would also keep committee members quite busy.

I would like now to turn to the specifics of Bill C-26 and what it is attempting to do. It is separated into two main parts. According to the summary of the bill:

> Part 1 amends the Telecommunications Act to add the promotion of the security of the Canadian telecommunications system as an objective of the Canadian telecommunications policy and to authorize the Governor in Council and the Minister of Industry to direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system.

There are a number of orders that the Minister of Industry could issue. For example, he or she could prohibit a TSP from using any specified product or service in its networks or facilities; direct a TSP to remove a specified product from its networks or facilities; impose conditions on a TSP's use of any product or service; subject a TSP's networks or facilities, as well as its procurement plans for those networks or facilities, to a specified review process. Those are just a few examples of how the minister's orders could be issued. The bill does require the Governor in Council or the Minister of Industry to publish these orders in the Canada Gazette, but there is an allowance in the bill to allow these provisions to be prohibited, so the government can prevent the disclosure of these orders within the Gazette if they feel they need to be kept secret.

Part 2 would enact a brand new statute of Canada, a critical cyber systems protection act, which would "provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety". In schedule 1 of the government's bill there is a brief list. Vital systems and services can include telecommunication services, interprovincial or international pipelines and power line systems, and nuclear energy systems. Those are a few examples. A really important point is that the Governor in Council, through this bill, would be able to establish classes of operators and require designated operators to establish and implement cybersecurity programs.

● (1245)

This is where the bill would affect the private sector and make sure those cybersecurity programs are in place, especially when that private sector is involved in critical infrastructure. As a brief outline, with those cybersecurity programs, the expected outcomes would be that they could identify and manage any cyber-risk to the organization, including supply chain risks; prevent their critical cyber systems from being compromised; detect cybersecurity incidents; and limit the damage in the event a cybersecurity incident did occur.

I want to talk about concerns with the bill, because there are a lot of concerns. I have had the chance to speak with a number of organizations, but first and foremost was OpenMedia. I had a great conversation with the people there. There is a section on its website that specifically deals with Bill C-26. OpenMedia absolutely realizes that new cybersecurity protections are needed to protect Canada's infrastructure, but it believes they have to be balanced by appropriate safeguards, and this is to prevent their abuse and misuse.

We rely on these essential services, and their protection is important, but Bill C-26, as it is currently written, would give the executive branch huge sweeping powers. In my reading of the bill, there would not be enough accountability and oversight; there would not be enough review mechanisms for Parliament to check the power of the executive, and I think this is a critical point. I think, in principle, we have a good idea with the bill, but a lot of work will be needed at committee to ensure that this executive power would be checked and that it would fit within the parameters of the law. We absolutely must have that kind of parliamentary oversight.

I also know of the Canadian Civil Liberties Association, which said:

> The problems with the Bill lie in the fact that the new and discretionary powers introduced by C-26 are largely unconstrained by safeguards to ensure those powers are used, when necessary, in ways that are proportionate, with due consideration for privacy and other rights. The lack of provisions around accountability and transparency make it all more troubling still.

I think, at this stage, we want to ensure, with the minister's powers to order or direct service providers, and the requirement to comply with these orders, that these powers are being subjected to the appropriate safeguard mechanisms. They are quite broad, as currently written.

In conclusion, I want to see a bill that protects vulnerable groups from cyber-attacks. So many Canadians rely on these critical systems, and we know so many have been targeted and are being targeted as we speak, and we know these dangers are going to multiply and get worse the longer we go on. We want to make sure they are protected, but we want to make sure that we do not have broad unchecked ministerial powers with no public oversight. That is the balance that must be achieved.

I must express, in my closing minute, my personal frustration with how the Liberals draft their bills. The idea behind Bill C-26 is a good one, but the problem with how the Liberals drafted the bill is that it would give huge sweeping amount of power to the executive branch. I just wish they would have had the foresight to understand that, of course, these provisions would be met with opposition. It seems the Liberals are putting the work on committee members to fix the bill for them, rather than having had the foresight and intuition to understand that these are problematic elements of the bill.

I think a lot more work could have been done on the government's side to have presented a better first draft. I guess we have what we have to work with, but a lot of work is going to be needed to be done at committee, and I look forward to seeing members do that work.

I also look forward to voting for the bill at second reading and sending it to committee. I welcome any questions or comments from my colleagues.

● (1250)

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, Bill C-26 would assist in empowering our laws and legislators to ensure there is a higher sense of Canadian confidence in the digital world, given the importance of the critical systems that are at work. Whether they are in health care services or consumer purchases, we have witnessed a great deal of advancement over the last number of years in cyberspace.

I am wondering if the member could provide his thoughts on why it is so important that legislation is brought forward to support Canadian confidence and protect privacy at the same time, and deal with the issue of the security of our Internet.

Mr. Alistair MacGregor: Madam Speaker, it is quite clear that legislative gaps exist. Many of my remarks were focused on detailing the threat landscape out there.

The good people who work at CSIS, CSE and Public Safety Canada are dedicated professionals who treat this threat very seriously. Every day they go to work, they are determined to keep Canadians safe. The problem lies in the fact that so much of our critical infrastructure, those systems that our society relies on every single day, lies in the private realm. We want to ensure that the government is there as a partner to help them beef up their cyber systems so that, if any one of them is attacked, we can pool resources, address the threat and also learn from it to prevent ones in the future.

There is a need there, but again the crux of my comments is that we have a good idea in this bill. There is a need. It is just the details and specifics that need to be hammered out.

● (1255)

Mr. Alex Ruff (Bruce—Grey—Owen Sound, CPC): Madam Speaker, I am going to build a little on the last question to the member. I know he sat on the public safety committee for a while. From his viewpoint, what does he think is the greatest cyber-threat to Canadians?

I would ask him to speak again to why getting this legislation right is so important, but I am interested in his take on what he perceives to be the greatest cyber-threat to Canadians.

Mr. Alistair MacGregor: Madam Speaker, in my opinion, based on what I have heard, it is artificial intelligence and its capabilities in the hands of nefarious actors.

We heard from Caroline Xavier, the chief of the Communications Security Establishment, at committee. She identified China, Russia, Iran and North Korea as countries that are actively trying to undermine Canada's national security. If we combine that with what Mr. Jérémie Harris has identified as what AI is capable of now and what it could be capable of, I am very concerned that those countries that are actively trying to undermine Canada's national security interests will use this emerging technology to construct malware, the likes of which we have never seen.

That is why a bill such as Bill C-26 is important, but it is important that we get it right. We absolutely must make sure that our critical systems are beefed up and secured against not only those particular nation states, but also others that are actively trying to undermine our interests.

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Madam Speaker, I heard loud and clear what the bill is missing. It lacks teeth and, of course, accountability mechanisms.

I heard my colleague opposite talk about the purpose of this bill, which could restore some degree of public trust. It is safe to say that trust is being undermined at the moment. My colleague is concerned not only about the fact that people's safety must not be compromised, but also about the impact on democracy and the need to ensure that it is not undermined.

Does my colleague agree that this bill has been crafted well enough to deal with the serious problems we are facing in terms of cyber-attacks and interference in our elections?

[*English*]

Mr. Alistair MacGregor: Madam Speaker, the hon. member has a point. I would identify the system that deals with our democratic process, including all of the actors involved, as being a critical system. It is probably the most critical system. However, while I do acknowledge there are definitely state actors who are trying to undermine our system, they are trying to undermine democratic systems all over the world. We see evidence of that.

I have a lot of confidence in the public servants who work at Elections Canada and who work for the office of the Commissioner of Canada Elections. They are doing their utmost to protect the sanctity of our democratic system. That being said, we cannot rest on our laurels, and it is up to us, as parliamentarians, to acknowledge these evolving threats and to equip our dedicated public servants with the tools they need to counteract these threats actively.

I would agree with the member's saying that these threats are real. They do need to be acknowledged. We owe it to ourselves to get Bill C-26 right so our public servants have the tools to counteract those threats.

Ms. Lori Idlout (Nunavut, NDP): *Uqaqtittiji*, given that there are concerns about our privacy rights being infringed upon and that Bill C-26 is not doing enough to protect our privacy rights, I would like to hear what the member thinks needs to happen to make sure this bill is improved.

Mr. Alistair MacGregor: Madam Speaker, a 20-minute speech does not give a lot of time to go over the multitude of concerns with Bill C-26. Yes, there are a lot of privacy concerns with this bill. We have had those concerns outlined not only by the Canadian Civil Liberties Association, but also by OpenMedia.

The way we allay those concerns is that we empower committee members on the public safety committee to give this bill a thorough going-over, and to make sure those expert witnesses are brought forward so they can identify the specific clauses of this bill that are problematic. We need to give members of the committee enough time to draft the amendments.

What I ultimately want to see when this bill is reported back to the House is an acknowledgement that there is a very real threat; that the bill would empower the government to counteract that threat; and that the bill would also provide a very important layer of parliamentary oversight and accountability, which I think should include some of our dedicated public servants, like the Privacy Commissioner and others.

● (1300)

Mr. Mike Morrice (Kitchener Centre, GP): Madam Speaker, the member for Cowichan—Malahat—Langford shared some concerns in his speech. I am sure he saw the open letter from eight groups, including the Canadian Civil Liberties Association, the National Council of Canadian Muslims and OpenMedia. One of their concerns is power without accountability for the CSE, or Communications Security Establishment, our cybersecurity agency.

Can he share more about what could be done to address this concern in Bill C-26?

Mr. Alistair MacGregor: Madam Speaker, there have been serious concerns about how, within the telecommunications infrastructure, Bill C-26 would allow Canada's national security and spy agencies to permanently implant themselves within that infrastructure, have access to all kinds of sensitive data and possibly share it.

I do not know what the specifics are at this point. I think the committee will be empowered to look at that. I want to make sure that, everywhere in Bill C-26 where ministers are able to issue these types of orders, or if they are kept secret, there would be accountability mechanisms built into the bill.

Can we give the standing joint committee on regulations the ability to review those orders, since they could be prevented from being published in the Canada Gazette? That is one particular example, but there are many others.

I agree with the premise of the member's question in that there is a lot of work that needs to be done with Bill C-26 at committee.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Madam Speaker, I am pleased to be able to rise in this place today and speak to Bill C-26, a bill that we as Conservatives are supporting to get to committee.

I have a lot of concerns around the bill itself, in terms of making sure that the government did not make a number of errors in judgment in putting it together. These concerns are based on the feedback we have received from Canadians and from organizations, especially on the issues surrounding privacy and the costs that have been offloaded to the private sector.

I also have to raise my concerns. Here we are, eight long years under the Liberal government, and we know that, when it has come down to cybersecurity, it has been slow in responding. A good case in point was banning Huawei from our critical infrastructure, our 5G network. We know that the Liberals sat on their hands and tried to do nothing for most of the past seven years, before they were finally forced to act after a great deal of pressure was brought upon them by our allies, especially within the Five Eyes.

Cybersecurity and national defence go hand in hand. When we talk about our national defence and national security, we know that hybrid warfare has evolved.

It is now about more than just targeting military assets; it is about targeting the entire government as it is at play. All we have to do is look at what is happening in Ukraine today, as well as what has happened to a number of other allies we have, through NATO, in eastern Europe.

We see the troll farms in St. Petersburg constantly attacking, on Facebook and on Twitter, the military individuals, the soldiers and troops, serving there. They also attack things like critical infrastructure in countries where Canadians are currently deployed, like Latvia. As we have witnessed in Ukraine and Estonia, they have not just gone after them through direct kinetic means to take out critical infrastructure, but they have also gone through cyberwarfare as well.

The Russians have done this very effectively in knocking down financial systems, knocking down transportation systems, and taking out power and water infrastructure in places like Estonia. As a prelude to the war in Ukraine, before they had actually started bombing these civilian targets in Ukraine, they were attacking them on cyber. It is part of hybrid warfare and it is the evolution of war.

There is a responsibility upon the Government of Canada to ensure that we are protecting not just our national infrastructure and the Government of Canada, that we are not just using CSE, or Communications Security Establishment, to protect national defence, but that we are also using a plethora of capabilities to ensure that our infrastructure here in Canada is protected.

That includes preventing our adversaries from going after our soft targets. That is what I think Bill C-26 is trying to accomplish, to ensure that telecommunications companies in Canada are stepping up to do their share to protect Canadians from cyber-attacks. We know that cyber-attackers have gone after things like our health care systems. They have gone after the medical records of Canadians. They have gone after the education records of students at schools and at universities. They go after retailers. They can go in through a retailer's back door, harvest all sorts of personal data, especially credit card information, and then use that for raising money, for transnational criminal gangs or for ransomware, as we have witnessed as well.

We must remember that we have a number of a maligned foreign actors at play here in Canada now and against our allies. It was just reported, again, that the People's Liberation Army was found guilty of hacking into U.S. critical infrastructure.

We know that the People's Liberation Army, under the control of the communist regime in Beijing, continues to attack cybersecurity assets around the world, including trying to break through the Canadian cybersecurity walls of our government and national defence on a daily basis.

As I mentioned, Russia has become very good at this. That does not mean that it is concentrating only on its near sphere of influence, NATO members in eastern Europe like Estonia, Latvia and Lithuania, but it is also targeting Ukraine. We know that it is targeting Moldova. We know that it has gone after countries like Romania, but it also does cyber-attacks here in Canada and in the United States.

Russia continues to be an adversary and we have to stand on guard to protect Canadians from those attacks.

● (1305)

We know that Iran, the regime in Tehran, is continuing to be a government that attacks its neighbours and attacks Israel and Canada through cyber-means. North Korea has developed an entire cybersecurity and cyberwarfare unit and continues not to just wreak havoc with the democratically elected, peaceful South Korea, but has also gone after Japan and the Philippines, and is going after U.S. infrastructure as well. Therefore, we have to take the necessary steps to make sure we can deal with transnational criminal organizations, with nefarious foreign states and with those who are trying to get rich through ransomware.

Here in Canada just a couple of years ago, we saw a situation in regard to the Royal Military College in Kingston, which the member for Kingston and the Islands is certainly aware of. The Department of National Defence stated that RMC had been a target. It originally called it a mass phishing campaign, but a month after the incident, it was established that the phishing campaign was actually a cyber-attack going after financial information and personal data of cadets. These had been compromised and published on the dark web, and were made available to a lot of people who participate on the dark web to profiteer from that information.

According to several observers who looked at the hack of RMC Kingston, it was attributed to a cybercriminal group called DoppelPaymer that did not seem to be connected to a nation-state actor. There are criminal organizations out there that are going about their criminal activities in such a way as to extract dollars from governments, retailers and private citizens, as well as from other corporations, to line their pockets and continue doing other nefarious things that sometimes go beyond the cyberworld.

I have said in the past, when we have talked about other legislation here dealing with cybersecurity, that we not only need the ability to defend, but also that the government has the responsibility, especially under national defence, to attack using cybersecurity. We cannot just be here deflecting the arrows; sometimes we have to be able to shoot down the archer. The way we do that is by having a very robust cybersecurity system. We need the best capabilities and the best personnel who are able not only to sit here and defend, that is to put up shields and fight off the attacks, but also are able to go out there and take out the adversaries, to knock out their systems, so that we are safer here at home.

With regard to some of the criticisms that have come out, I know that letters have come in from the Canadian Civil Liberties Association, and the Business Council of Canada wrote a very detailed brief, as did the Citizen Lab in looking at the bill. When we read through the documentation, we see that one of the concerns that has been raised, especially by the Business Council of Canada, is that there seems to be an imbalance. We are telling members of corporate Canada to go out there and make sure they have the proper cybersecurity systems in place, but at the same time we realize that it is not just up to them to do the defending. What we see is that the corporations are saying that either they have to do it or we are going to fine them up to $15 million or five years of jail time, and that the individuals who work for them could also be held criminally responsible for not doing enough.

Sometimes resources are not available. Sometimes there are new companies that may not have the ability to put in place the proper security systems. I look at a lot of the Internet service providers that we have, for example. They are covered under the Telecommunications Act, yet, as new start-ups, they may not have the personnel or the equipment to properly defend their networks. Would we go ahead and fine these companies up to $15 million? Then what would we do in regard to jail time and fines for those criminal organizations that are profiteering through cyber-attacks? Where is the balance in this? That is one of the concerns we have and one of the things we have to look at through our study at the industry committee when it brings this forward.

● (1310)

A huge concern has been raised, especially by the Canadian Civil Liberties Association, on how this would be implemented and how it may affect the privacy rights of Canadians at the individual level. Corporations have broader responsibilities and do not necessarily fall under the charter, but their clients who they are going to protect and the information they are going to be required to share with the Government of Canada could very well be violations of their clients' privacy rights.

When we look at section 7 of the Charter of Rights, we have to balance the right to life, liberty and security of a person with section 8 of the charter which says that we have freedom from search and seizure. When we drill down on section 8 and go to some of the legal analysis of our charter, as all the rights and freedoms are laid out, it tells us that the underlying values of freedom from search and seizure when it comes to individual privacy is the value of dignity, integrity and autonomy. Again, I think we are all concerned that when we look at Bill C-26 at committee, we ensure the bill balances those rights of the individual to be both secure and safe from cyber attacks, but do it without compromising privacy rights and charter rights as described in freedom from search and seizure. The way we do that is through warrants.

We know that through National Defence, the Communications Security Establishment, or CSE, which has a long-standing history of defending the Canadian Armed Forces, has to comply with the charter. It has to comply with all Canadian legislation and it cannot do indirectly what it is prohibited doing directly. Therefore, CSE cannot go to the National Security Agency, or NSA, of the United States, say that it is concerned that a Canadian maybe talking to a terrorist organization offshore and ask the agency to spy on that individual because CSE is prohibited from spying on the person and listening in through the Communications Security Establishment. CSE cannot go to the NSA and ask it to violate Canadian law on its behalf to find out what is happening in the same way CSIS cannot go to the FBI or the CIA and ask it to spy on Canadians. It cannot do indirectly what it is prohibited from doing directly under Canadian law. The way to get around that is to apply for warrants.

Judicial appointments are made to have supernumerary justices over these organizations to ensure that charter rights are protected, even when conversations take place inadvertently. In the past, CSE has listened in on people who may have been in Afghanistan funding the Taliban or al Qaeda. They may have family in Canada and were talking back and forth about something that had nothing to do with operations on al Qaeda or the Taliban. However, because it involved a Canadian citizen, it had to go through the proper processes to ensure that his or her charter rights were protected by getting a warrant to listen to those conversations. Whether they were listening electronically or through wire taps, it is all mandated to watch that we do not trip over the rights of Canadians under legislation.

Bill C-26 would not address this like we have under the National Defence Act, under the Criminal Code and under the whole gamut of cybersecurity that has been in place up to date. The privacy rights are paramount.

To come back to Bill C-26, the Supreme Court of Canada said in 1984, as well as in 1988, that privacy was paramount and was "at the heart of liberty in a modern state". Again, did the Liberal government ensure the bill was tested first to ensure those privacy rights were protected? This is what we will have to find out when we get Bill C-26 in front of committee.

● (1315)

We can look at information that has come from places like the Business Council of Canada. One of the concerns it raises goes back to this whole issue of huge fines on Canadian corporations, as well as the employees of those corporations, if they are found to have been not responsible enough to put in place proper security protocols to protect their clients from cyber attacks. Because it goes against individual employee as well, we will create another brain drain from Canada.

We are unfairly targeting Canadian employees who are going to be working for these cybersecurity firms, working in the telecommunications sector and in our financial institutions. If they are found to have erred, which a lot of times it is by error or by a lack of resources, then they are held criminally responsible and they are fined. The question becomes why they would want to work in Canada when they are afforded better protections in places like the United States, the European Union, the United Kingdom or Australia, which was held up by the Business Council of Canada as the gold standard we should be striving to achieve, and what it has done through their own cybersecurity protocols.

We want to ensure that we protect critical infrastructure, but we do not want to chase away very good Canadian employees and force them, with their skills, to go offshore where they have better protection and probably better pay. We want to ensure we keep the best of the best here. We want to ensure we do not go through a brain drain, as we have witnessed before when the Liberals have targeted professionals in Canada, such as lawyers, accountants, doctors or anyone who set up a private corporation. Now I fear the Liberals are going after individuals again who we need in Canada to protect us here at home, that they are creating a toxic work environment and those individuals will want to leave.

The Citizen Lab wrote a report entitled "Cybersecurity Will Not Thrive in Darkness". It brought forward a ton of recommendations on how bad this bill was. It suggested that there needed to be 30 changes made to the act itself.

We realize that the government has not done its homework on this. We need to ensure we get experts in front of us who are going to look at everything, such as there is responsibility upon government to help corporate Canada ensure we have the proper security mechanisms in place to prevent cyber attacks. We have to ensure that those corporations are not being coerced into sharing private information with the Government of Canada that could be a violation of private rights, which may be a violation of the Personal Information Protection and Electronic Documents Act, PIPEDA. We want to ensure that privacy rights will be cohesive, but, at the same time, collectively, we need to balance all federal legislation that is in contravention of each other.

We need to bring in the legal experts. The Canadian Civil Liberties Association needs to be before committee. The Citizen Lab, which is very concerned about individual privacy rights, has to be front and centre in the discussion. We need to ensure the Business Council of Canada, the Canadian Chamber of Commerce and others are brought forward, along with the department officials who were responsible for drafting this bill at the direction of the Liberal government.

I will reiterate that I will be voting in favour of the bill to ensure it goes to committee and the committee can do its homework. I would hope that the government will allow the committee to do a thorough investigation, as well as a constructive report with recommendations on how to change and amend the legislation.

Finally, I would remind everyone that the Supreme Court of Canada said, "privacy is at the heart of liberty in a modern society", and we have to take that to heart to ensure we protect Canadians from cyber attacks, as well as to ensure they have their privacy, dignity, integrity and autonomy respected.

● (1320)

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, when look at Bill C-26, I want to assure the member that the government has made very clear the importance of privacy rights. In fact, it was a Liberal administration that brought in the Charter of Rights, understanding and appreciating just how important privacy rights were. The legislation, which the Conservative Party is voting in favour of, and I grateful for that, is there to protect the integrity of the system. As we move more and more into that digital world, cyber-threats are very real and can have a profoundly negative impact. That is why we have to bring forward the legislation.

Given the potential threats to things such as the delivery of health care services to interactions on the net by Canadians, would the member not agree that it is important that legislation of this nature continue not only to deal with the threats but to build confidence in the system with Canadians?

Mr. James Bezan: Madam Speaker, I have a lot of trouble putting any confidence in the Liberal government. It took seven years for it to ban Huawei. It is a government that sat on its hands and did nothing about cybersecurity for the past several years. I know this is a government I cannot trust. When I look at Bill C-11, the Liberals are now trying to censor Canadians online. They are trying to control what people see online, which violates charter rights, especially when it comes down to freedom of expression, freedom of association and the ability to actually have discourse online about our political situation in Canada and around the world. When the Liberals try to put veils over certain parts of our information system, I have to be very concerned.

I look at Bill C-21 and how the Liberals have gone after responsible firearms owners like hunters, sport shooters and farmers. To me, that builds no trust in the government to get the job done.

● (1325)

[*Translation*]

Mr. Yves Perron (Berthier—Maskinongé, BQ): Madam Speaker, I thank my colleague for his speech. It was eminently sensible, and he made some good points. I am glad the Conservatives are going to vote in favour of the bill so that it can go to committee, and I hope we will all approach that work in good faith, as we should.

Over the past few weeks, I have had the opportunity to serve as a substitute at the Standing Committee on Public Safety and National Security. I had a chance to question a witness, and one of the things we talked about was quantum computing, a new and rapidly evolving technology that Canada is absolutely not ready for. My sense is that it will take a massive investment up front to prepare the country for future cyber-attacks by systems that could crack passwords at lightning speed.

Does my colleague see this as a priority issue? Does he think that the committee should discuss making a massive investment in R and D and creating a technical team to get ready for these new technologies?

[*English*]

Mr. James Bezan: Madam Speaker, we all have to be concerned about the rapid deployment of new technologies and how they can be used nefariously to attack Canadians. This comes back to Bill C-26 as well. Again, the government would be putting all the onus on corporate Canada to protect us, but at the same time, I wonder who will do the R&D, who will step up to ensure our technology and our ability to defend ourselves is deployed across the spectrum, whether it is government agencies, government departments, our provincial and territorial partners or corporate Canada. How are we going to ensure the safety of Canadians when it comes down to their personal information and ID, especially if we are seeing new malware out there that will harvest and hack passwords in a matter of seconds?

We have to be investing in R&D. The government has a responsibility and role to get it done, but we do not see that in Bill C-26.

Ms. Lori Idlout (Nunavut, NDP): *Uqaqtittiji*, I agree that there needs to be better privacy protections to ensure our rights are not violated. I wonder if the member could share with us whether he agrees there needs to be greater parliamentary oversight built into the bill.

Mr. James Bezan: Madam Speaker, I agree. Right now, this will be studied only at the industry committee, but it involves a huge component of national security and national defence. I hope that as legislation comes forward, we will see other studies come into play that look at the impacts of it as it applies not just to industry but to our national security. One would hope that the public safety committee would also undertake a study. There might be a requirement to split this bill, and perhaps OGGO, the government operations committee, needs to look at this as well.

There are multiple departments within the Government of Canada, like Shared Services Canada, but how do we make sure that they are fully up to scale with all of the technologies that are currently available and that they are developing the new technologies needed to defend Canadians here at home? We know that the Government of Canada already collects a pile of personal information from Canadians and that they have been targeted by nefarious foreign actors, transnational criminal organizations and cybercriminals right here in Canada.

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Madam Speaker, this is a very interesting debate and something we should be discussing thoroughly here in the House.

As my colleague has spent a lot of years as a defence critic and in the defence milieu, he is knowledgeable, so I want to ask him a bit about the People's Liberation Army's units 61486 and 61398. We know from public reports that these units have thousands and thousands of people working for them. The entire Canadian Armed Forces is somewhere around 60,000 to 70,000 people, so we would be outnumbered by their cyber-divisions alone.

Given the fact that AI is now in the public domain, does the bill go far enough in addressing the legitimate concerns that foreign actors create in everyday life here in Canada? What could be improved upon in the legislation?

Mr. James Bezan: Madam Speaker, my colleague is dead right that the People's Liberation Army in Beijing has established a number of different cybersecurity units and that their whole goal is to cyber-attack. Canada is not an ally of China, so we have been attacked by the regime in Beijing. It will continue to attack us here and attack NORAD, as we just witnessed with the high-altitude balloons going around doing surveillance on military installations across North America.

We have to be ready, and the cybersecurity command we have here in Canada has been slow to get off the ground under the leadership of the Liberals. We need more resources. We need to use our reserves to find the right type of personnel out there, who are currently working in the private sector. Maybe we can also put them to work part time to defend Canada's interests so that both the corporate world and our national defence will be under better control and better command, with ultimately better protection for all Canadians.

● (1330)

[*Translation*]

Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ): Madam Speaker, I had some interesting discussions with many people last week in the wake of the TikTok ban. Obviously, one of the reasons that the platform was banned was because the Chinese state could take advantage of the personal information that goes along with using that platform. Someone was telling me that Facebook and Instagram are already doing it, yet no one seems to be concerned.

Of course, the concern with TikTok is that it is the Chinese state that could use the information. However, Facebook's business model is to take our information and give it to private companies that then use it to sell products. I have a bit problem with that.

I think we have all had the experience of talking openly about a product with someone and seeing an ad for that product two minutes later on our phone. Obviously, there are all kinds of ways to avoid that, but I think a lot of people have no idea how to go about it. We could create legislation to try to tighten up the use of these platforms.

Does my colleague agree?

[*English*]

Mr. James Bezan: Madam Speaker, my colleague from the Bloc was spot on when he started talking about Canadians being very trusting. All consumers are very trusting when using social media like Facebook, TikTok and Instagram. When I was at the ethics committee, we looked at Clearview AI, which scraped images off of Facebook and Instagram to build up its databases to profile criminals. On top of that, we found out that it was racialized.

As Canadians and as consumers, we have to be very diligent with where we are sharing our information. I agree that we have to ask questions around social media platforms like Facebook, not just TikTok.

Mr. Ted Falk (Provencher, CPC): Madam Speaker, it is my pleasure to rise in the House today to share my thoughts and those of my constituents on Bill C-26. I am very pleased to have this opportunity.

Bill C-26 is a risky and tricky piece of legislation. On the one hand, we have serious and growing issues of cybersecurity, and on the other hand, we have the importance of personal privacy. We also have questions related to government accountability and oversight. I am sorry to say that the government has not done a stellar job on either one of those fronts to date. I am hopeful that members of this House can work together collaboratively to craft a piece of legislation around what has been proposed in Bill C-26 that balances both of those vital yet often competing priorities.

I grew up in the 1960s under the spectre of the Cold War. When I was a kid, the threat of foreign attack came from the air above us, from nuclear missiles from Russia or China. While our adversaries remain the same and current events have sadly brought the spectre of nuclear disaster to the forefront again, the method of attack to which we are most susceptible today is far more sophisticated and far more insidious.

Rather than bombs from the air above us, the weapons of our enemies are in the air all around us: Men and women are sitting at computers in dark rooms, in government agencies or at the local library sending out digital viruses. These cancers attack the Internet, telecommunication waves and the platforms we have become reliant on to what I would consider to be an unhealthy degree.

That is where I will pause for a moment, because I think the best thing we can do, the first step to securing our national security and the well-being of Canadians, is what nobody wants to do, which is to take a little step backwards to take a look at this. We need to divest ourselves of our all-consuming reliance on digital platforms, devices and infrastructure, and ensure that our most vital infrastructure always has a physical fail-safe to fall back on.

Let me give an example. Let us talk about digital currency for a second. Digital currency exists. Most Canadians have a credit card, a debit card and online banking. I do and I use them; it is convenient. However, that is not to say for a minute that I think progress demands that we do away with hard currency. It is exactly the opposite. Canadians have become more reliant on digital currency, forms of digital ID, smart phones, smart cars, smart homes, smart cities, smart bombs, smart banking and smart hospitals, and the really smart thing to do is ensure that we always maintain physical infrastructure and ensure we are in control and not crippled by the worst that could happen.

Nothing is impenetrable. No matter how good or amazing the technology that we create is, no device, no platform and no code has been created that cannot be hacked. Anything people make, people can break, and if they cannot, they will develop a machine that can break it.

I was reminded of a story last week of a military computer virus called Stuxnet. Stuxnet single-handedly destroyed one-fifth of Iran's nuclear centrifuges. Actually, that is not totally correct. The worm that Stuxnet was caused these sophisticated machines to self-destruct. It got into their systems, learned how they operated and then caused the powerful turbines to spin in reverse, shredding the machines. We have artificial intelligence so advanced that it can make decisions, and the people who created the technology do not even know how the decisions came about. It cannot even tell them. It is a little scary.

Digitized records are important. We have all come to rely on them, but I believe keeping a hard copy is also important. Ensuring that we maintain a hard physical currency is very important too, as is recognizing the value of currency produced by the Royal Canadian Mint. We need to ensure that our power grid still has a physical switch and that our hospitals and banking systems cannot be crippled by a bright kid with a laptop or a foreign actor with a more malicious intent.

The government has been very slow to address cyber-threats. Under its watch, the CRA was hacked. It said 5,000 accounts were affected, yet that number turned out to be 50,000. It did not address the issue. There were lots of excuses from the minister, but what really happened? One year later it happened again, and another 10,000 Canadians had their personal data accessed by hackers. Last year, the National Research Council was hacked.

● (1335)

I am sure that after this past week, the government is tired of talking about foreign interference in our elections, so I will not belabour that point, except to say that we did have foreign interference in our elections. The Prime Minister knew about it and he did nothing. Worse than that, he still refuses to tell Canadians the truth about what he knew and when he knew it. Like everything else, he refuses to take responsibility. I wonder sometimes just how much longer those on the government benches will allow him to do so. I would bet that right now the Reform Act is looking pretty attractive to them.

Last year, Rogers' network went down suddenly. Canadians could not access their banking. Businesses could not function. Emergency services were affected. Rogers and the government said it was a glitch, a hack. We will probably never know for sure, but the effect was the same: chaos. That is what our enemies want, and we do have enemies, both foreign and domestic, people who want to see anarchy and to cause chaos, fear and division. It sounds eerily familiar.

What legislative response have we seen from the government to date? I am seriously asking, because when I think back over the past seven years that the Liberals have been in power, I am not aware of any substantive action, either proactive or reactive, that they have taken to address our cybersecurity and the glaring vulnerabilities that exist with respect to it. To that end, I am glad that we are now finally having this important discussion. We need to beef up our security systems, beef up our cybersecurity system and keep Canadians safe.

As the government always says, Canadians have a right to be safe and to feel safe. The obvious irony is that it only says it when it is clear that Canadians are neither safe nor feeling safe. Canadians should be able to feel safe, should be safe and should have confidence in the cybersecurity system they rely on.

My time is almost gone, and that is a shame because there are so many things we need to talk about with respect to this bill, although I am confident that my colleagues will be able to further articulate some of the concerns. However, I do want to say one word about privacy.

Many Canadians are concerned about the ever-increasing size, scope and reach of government in this country. The Prime Minister has increased the size of government by some 30%, and this bill gives such sweeping powers to the government that it has prompted numerous civil liberties groups, including the Canadian Civil Liberties Association, the International Civil Liberties Monitoring Group and the Privacy and Access Council of Canada, in addition to several other groups and academics, to express their very serious concerns about this legislation. They call it "deeply problematic" because it "risks undermining [the] privacy rights [of Canadians], and the principles of accountable governance and judicial due process". That is a lot to unpack in just one sentence.

Had this legislation come forward three years ago, I would have probably said that it was a no-brainer and that we should get it done as national security trumps personal privacy. However, after the violations of civil liberties, even basic liberties, that we have witnessed over the past three years from the government, I would not be so eager to say that we should just get it done. There is also the government overreach, the control and the abject absence of even a semblance of accountability.

As vital as our national security is, the government, the ministers and the Prime Minister simply cannot be trusted with more power, and that is what this bill does. It gives the government of the day more power through the Governor in Council and through its agencies to establish regulations and to further limit and restrict the freedoms and privacy of individual Canadians.

It is my hope that as members in this House, we can strike the right balance after hearing from all sides and craft a piece of legislation that accomplishes everything we want and need in it. However, as it stands, Bill C-26 gives way too much power to a government that has proven time and time again that it is unable and unworthy to wield it.

● (1340)

Mr. Mark Gerretsen (Parliamentary Secretary to the Leader of the Government in the House of Commons (Senate), Lib.): Madam Speaker, I am glad the member brought up the issue of foreign interference and the rhetoric the Conservatives have been spreading the last little while. I want to read a quote from Fred DeLorey, who was the Conservative Party's 2021 campaign manager. He said, "I can confirm, without a shadow of a doubt, that the outcome of the election, which resulted in the Liberals forming government, was not influenced by any external meddling."

Can the member comment on that quote, given the context and the comments he made during his speech?

Mr. Ted Falk: Madam Speaker, this is an important question. Some time ago, I did a term on the National Security and Intelligence Committee of Parliamentarians, and what I learned there was that we have phenomenal security agencies in this country. One of those is the CSE, the Communications Security Establishment, which monitors cybersecurity. It does phenomenal work.

I was coming back from a meeting one day, driving down the highway. It happened to be a Friday, and I noticed vehicles pulling campers and boats, with roof racks and bicycles attached to their bumpers. I thought, is it not wonderful that we live in a country where we have absolutely no idea about the existential cyberthreats that are out there? Why is that? It is because our security agencies are doing a phenomenal job at keeping us safe and providing this kind of environment.

The obligation of the government, when it gets advice from our security agencies, is to act on it.

● (1345)

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Madam Speaker, unfortunately, we have seen that, when it comes to everything that affects all citizens, the government is ignoring security issues and the threats that foreign interference can pose. We are seeing partisanship everywhere. We are talking here about cybersecurity. We want our electoral system to be airtight. We also do not want democracy to be affected.

Is this the right time for this bill? Is it designed well enough that we can do the same as our Five Eyes colleagues who took the bull by the horns far in advance?

[*English*]

Mr. Ted Falk: Madam Speaker, this is a very relevant question. Is it the right time for a bill like this? I would like to give a very brief answer: Yes, it is absolutely the right time for this. Is it the right bill yet? No, it is a good starting point. That is how we can look at this bill. I am happy to vote in favour of this bill, to get it to committee. I am hopeful, from the comments I have heard from members of the Bloc and the NDP, that they are eager to give this bill a robust study and make the necessary amendments that will address the cybersecurity requirements in our country to keep critical infrastructure and our citizens safe, but also to respect the privacy of Canadians. Those are equally important elements. I am looking forward to the study on this bill.

Ms. Lori Idlout (Nunavut, NDP): *Uqaqtittiji*, I would like to thank the member for his very informative intervention, where he very clearly stated his concerns with the broad powers the government seems to want to grant itself.

Can the member talk about what concerns regular Canadians might have, regular Canadians who have not done anything wrong, and how they may be impacted by the extreme ministerial powers that might emerge from this bill if it is not changed?

Mr. Ted Falk: Madam Speaker, I am just going to read an excerpt from the bill, because it really encapsulates the answer to the member's question. It states the bill would authorize the Governor in Council, which is cabinet, "to designate any service or system as a vital service or vital system". It would also authorize the Governor in Council "to establish classes of operators in respect of a vital service or vital system". It also "provides for the exchange of information between relevant parties".

We cannot currently do that. Our security and law enforcement agencies cannot transfer information without a judicial warrant. Why would we allow the government and cabinet to do that?

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Madam Speaker, it is an honour, as it always is, to rise in the House of Commons of the Canadian people and speak to Bill C-26, an act respecting cybersecurity, which seeks to amend the Telecommunications Act and make subsequent amendments to others acts.

I want to say from the outset that cybersecurity is a critically important issue. For those of us who have been watching the news, we have even seen bookstores like Indigo impacted by ransomware, and we know that no Canadian, business or government agency is immune to cybersecurity threats. As Conservatives, we obviously support taking robust action on cybersecurity and we look forward to the bill going to committee, where we can hear from stakeholders who have expressed uncertainty about what the impact of the bill is going to be. Certainly, I hope we can work across lines to make a better piece of legislation and address the very real challenges we are facing in this cybersecurity age, in this cyber age that we are facing.

I am going to go into a bit of background on the bill, because my constituents might not have heard of this legislation. For their benefit, I am going to give a bit of summary of what I understand the changes to be.

The threat of malware in our telecommunications sector and critical infrastructure does pose a serious threat to Canada. It is important that we respond to these threats proactively, in light of the inevitable future attacks that will happen in our cyberspace. As I said, Conservatives will support legislation to defend our telecommunications sector and our other critical infrastructure from threats, the likes of which, as I stated earlier, have been levied against Canadian individuals, corporations and government agencies repeatedly.

In order to evaluate this legislation, I would like to take some time to consider how the proposed bill might impact our economy, our national security and our commitment to protecting the civil rights of Canadians. Although legislation relating to cybersecurity threats is now long overdue, we should remain vigilant to protect the rights of Canadians and our domestic corporate actors, who could be seriously impacted by the unintended consequences of this legislation. Notably, I am somewhat concerned by the sweeping discretionary powers that are granted to the minister and the Governor in Council in this legislation. I would also like to talk about some of the objectives of the bill and then describe how this current proposed legislation could fail in achieving its intended purpose.

The bill is presented in two parts. The first would amend the Telecommunications Act to promote the security of the Canadian telecommunications sector, and the second part of the act would enact the critical cyber systems protection act. The amendments to the Telecommunications Act are intended to protect against ongoing threats of malware, which poses a threat to the Canadian telecommunications system, and the critical cyber systems protection act aims to strengthen the cybersecurity systems that are so vital to our national security and public safety, and it would allow the government to respond to these cyber-threats.

The aim of this legislation would implicate operators in a broad variety of fields, including the finance, telecommunications, energy and transportation sectors, just to name a few, all critical parts of our infrastructure. With these aims in mind, it is important to consider how expansive the government powers being talked about here are, new powers to the government, how these new powers will affect all these sectors that affect our day-to-day lives, and whether these new measures are proportionate and necessary to be implemented.

To begin, the powers afforded to the minister present economic and financial risk for critical systems operators and telecommunication system providers. The first consideration is the minister's ability to direct telecommunication service providers to comply with an order to prohibit a provider from using or providing certain products or services to a specific individual or entity. Those are pretty broad powers. The bill would implicate the operations of private telecommunications organizations, and therefore the legislation requires safeguards to protect the economic viability of these companies. The bill would also allow the minister to compel telecommunications companies to obey government directives or face the consequences of significant monetary penalties.

In giving the minister such expansive powers, the government may have failed to consider the potential economic impact of these unchecked provisions on service provisions. Telecommunications revenues contribute over $50 billion to Canada's GDP, yet the government has not provided clear and adequate safeguards in this legislation to limit the extent to which or the frequency with which it might use these service provisions and how they might be restricted under the instance of even a minor cyber-threat.

● (1350)

Large, medium and small regional market players would be impacted by this legislation if appropriate safeguards are not adopted in the amendment stage. Large telecommunications service providers make up about 90% of the market share, and any directive to suspend a service by these large market players could impact a significant amount of the Canadian population. Although we hope that such orders will seldom be issued, the vagueness of the language in the bill does not guarantee this.

Meanwhile, we see small and medium-sized players who disproportionately service under-serviced areas in Canada; I am thinking of rural and remote communities. These small and medium-sized players often have trouble dealing with the regulatory complexity and the financial investments needed to meet regulatory thresholds, and we could see these small and medium-sized players just fold up or get bought out at a fraction of what their value would have been. We would really see this as a consequence for rural and remote communities, which are struggling, even today, to get access to basic services like high-speed Internet.

For these reasons, the overbroad provisions in the bill do not lend themselves to a standard of proportionality.

A stakeholder group, Citizen Lab, released a research report on Bill C-26 from the Munk School, authored by Dr. Christopher Parsons. The report outlines, in its recommendations, that the legislation should be amended to allow telecommunications service providers to obtain forbearance and/or compensation for orders that would have "a deleterious effect on a telecommunications provider's economic viability".

The Business Council of Canada is likewise concerned about the CCSPA requiring that all critical systems operators undertake the same precautionary actions to protect themselves from cyber-threats. The Business Council of Canada notes that the legislation would require a singular standard of all service providers "irrespective of their cyber security maturity". We know that there are highly funded firms with a lot of resources that have highly superior cybersecurity systems, and then we have our more infant, junior tech companies that are trying to grow so that they can attract capital. These regulatory requirements of holding them to the same standard could have a negative effect on growing the tech ecosystem here in Canada.

Moreover, the Business Council of Canada notes that the legal threshold for issuing the directives is too low. The low threshold to issue these orders to an operator would allow the possibility of lost revenue for operators because of an absence of due diligence on the part of the government, a government that has had its own cybersecurity problems. I have serious reservations that a government that is unable to run its own IT systems will have a better capability of telling private companies how to run their IT systems.

The council further notes that the monetary penalties are unduly high and are not proportionate, given the benefits of compliance in the event of a perceived or actual cyber-threat. These companies in Canada want to live by the rules. They want to work with the Canadian government. Their reputations are at stake, yet the government is treating them like they are bad actors by putting these fines in place, when maybe we should be looking at working and engaging more with our telecom sector to have a more friendly relationship on this issue.

Another group, Norton Rose Fulbright, noted that there is still considerable uncertainty as to how detailed the cybersecurity plans must be and how it would alter industries' existing policies and agreements. Clearly, there is a lot of uncertainty about this, but it is too important to let it go aside, so I am looking forward to this coming to committee, where we can have some of these stakeholder witnesses come and talk about things so that we can clear up the uncertainty and we can have targeted cybersecurity measures that actually result in benefits to Canadians.

Other technical experts, academics and civil liberties groups have serious concerns about the size, scope and lack of oversight around the powers that the government would gain under this bill. Civil liberties groups are particularly concerned about the government's ability to direct telecommunications providers to do anything needed by secret order. While the legislation lists what might be included by the minister or Governor in Council, the ambiguity of the wording leaves open the possibility of compelling a telecommunications company to do more than is officially stated. This is particularly noteworthy because of the significant monetary penalties that can be levied against these companies, to the tune of up to $10 million a day.

Liberals, in many cases, have perhaps neglected to consider the privacy of Canadians through this legislation.

● (1355)

Bill C-26 would allow the government to bar any person or company from receiving specific services, which raises concerns about the discretion the government has in making these decisions. Again, it is very unclear. This is too important. We should bring the bill to committee and vote on it, but there are lot of things we need to get right in the legislation. We look forward to looking at that.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Mr. Speaker, my colleague had a very insightful speech and talked a bit about how there are some concerns related to the oversight that would be associated with the wide and sweeping powers the government may be granting itself in the bill. I am wondering if he could expand a bit more on why it is important that, through the processes of debate in this place and through committee work, we ensure that we have the appropriate balances in place to ensure we get that oversight side of things right.

Mr. Dane Lloyd: Mr. Speaker, Parliament exists to defend the rights and liberties of the Canadian people. Oftentimes, I find this legislation is highly technical. The technical legislation is often where we see the biggest changes that would impact people's lives. When the government proposes to give sweeping powers to the minister to have control over sectors that impact every facet of Canadian lives, we need to do our due diligence as parliamentarians. We need to bring forward the stakeholders, the witnesses and the civil liberties advocates to ensure that the rights and liberties of Canadians are protected.

STATEMENTS BY MEMBERS

● (1400)

[*English*]

ZAHID MALIK

Mr. Shafqat Ali (Brampton Centre, Lib.): Mr. Speaker, I rise today to honour the late Zahid Malik, a beloved Pakistani Canadian community leader, who passed away on February 16 at the age of 52 fighting cancer. Zahid Malik was a successful small business owner who operated Active Marketplace, a flea market in Ajax, Ontario.

Zahid Malik was a generous and kind-hearted man who never backed down from a challenge, especially if it meant giving back and improving community. On weekends, he would provide free meals at his flea market and, most recently, he raised $40,000 to support the victims of last fall's massive floods in Pakistan. His passing is a huge loss for his family, friends, the community and all those who experienced his kindness first-hand.

Our thoughts and prayers go out to him and his loved ones. He will truly be missed.

* * *

MOOSE JAW WALK FOR WARMTH

Mr. Fraser Tolmie (Moose Jaw—Lake Centre—Lanigan, CPC): Mr. Speaker, in small towns in Saskatchewan, people are always eager to support a good cause. They look after their neighbours. It is what makes representing a riding like Moose Jaw—Lake Centre—Lanigan such a pleasure.

One of those causes is Moose Jaw's first-ever Walk for Warmth, which is happening later this week. Over 180 people have already signed up for this tremendous fundraiser. These funds will be going toward the city's first women's emergency shelter and will also help to continue the operation of a warming shelter.

Winter in Saskatchewan can be harsh and cruel, with temperatures dropping to below -40°C at times. I am proud of all those people who are stepping up to help Moose Jaw's most vulnerable. I thank everyone involved for their hard work and their support for this great cause. I wish them all the best for a successful walk.

* * *

GULF WAR ANNIVERSARY

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Mr. Speaker, 32 years ago this week was the end of the first Gulf War, in which over 4,000 Canadian Armed Forces members served. It was also the first conflict in which Canadian women played an active combat role.

I joined with the Persian Gulf Veterans of Canada to lay a wreath on the National War Memorial last week to recognize their service. The war began in 1990 when Iraq invaded neighbouring Kuwait. I was a university student at the time, and it was the first time that we saw war in real time on our TV screens. Regardless of how Canadians felt about the war at the time, once we sent our military personnel there, we all supported the women and men who left their families for the unknown, not knowing when or if they would ever return.

For these veterans and their families, their willingness to serve and their bravery will not be forgotten. I ask all members to join me in thanking these brave veterans.

* * *

[*Translation*]

GENDER-BASED VIOLENCE

Ms. Andréanne Larouche (Shefford, BQ): Mr. Speaker, *Backlash: Misogyny in the Digital Age* is a shocking but necessary documentary. A more virulent strain of misogyny than ever before has been flooding our screens for far too long.

Harassment, defamation, lynching, sextortion, the dissemination of intimate photographs, and rape and death threats all go mostly unpunished. The most pernicious effect is that more and more women are practising self-censorship, remaining silent and giving up their right to speak on digital platforms.

Cyberviolence is a democratic issue. We need to take action. We need to get to the heart of this problem that still affects, in particular, far too many women and girls. Over 30,000 people signed a petition calling on the federal government to legislate to counter cyberviolence.

I want to thank and recognize the co-directors of this documentary, Léa Clermont-Dion and Guylaine Maroist, for waging this necessary battle.

As International Women's Day approaches, we need to stand in solidarity with victims and address the issue of cyberviolence, which disproportionately affects women and marginalized groups in our society.

* * *

● (1405)

BERT BLEVIS

Hon. Marc Garneau (Notre-Dame-de-Grâce—Westmount, Lib.): Mr. Speaker, with the launch of the Alouette I satellite in 1962, the men and women at Communications Research Centre Canada in Ottawa made Canada a leader in the field of space research and communications.

[*English*]

Dr. Bert Blevis was among them. He was also a key figure in the Hermes program, which connected Canada's northern communities and paved the way for satellite-to-home service, earning Canada an Emmy in 1987, which he accepted alongside the then communications minister Flora MacDonald.

[*Translation*]

He also signed the historic COSPAS-SARSAT memorandum of understanding on the use of satellites for locating planes, boats and persons in distress.

[*English*]

He was also a member of the Canadarm review board and served on the transition team to establish the Canadian Space Agency.

Dr. Blevis passed away on January 31. We thank him and his colleagues for being the shoulders on which Canada became, and still stands as, a space leader.

* * *

NATURAL RESOURCES

Mr. Rob Morrison (Kootenay—Columbia, CPC): Mr. Speaker, critical minerals present a generational opportunity for Canada in many areas, with exploration, extraction, processing and downstream product manufacturing among them. The future is not void of extraction of critical minerals. In fact, without critical minerals there are no batteries, no electric cars, no wind turbines and no solar panels. Wind turbines need platinum and rare earth magnets. Electric vehicles require batteries made from lithium, cobalt and nickel. All critical minerals are identified by the government in its critical minerals strategy.

What is absent from the list is metallurgical coal, a required ingredient to produce steel needed to build electric cars, solar panels and wind turbines. The hard-working mining families of the Elk Valley in Kootenay—Columbia have been providing this critical mineral to the world since the late 1800s. Currently, metallurgical coal sustains 30,000 jobs and provides $1.5 billion in revenue annually to the three levels of government. We are counting on the NDP-Liberal government to acknowledge all of the minerals required to build a sustainable future, including metallurgical coal.

* * *

COMMUNITY VOLUNTEER AND SPORT MENTOR

Mr. Ryan Turnbull (Whitby, Lib.): Mr. Speaker, today I want to acknowledge an extraordinary woman named Shauna Bookal, whose impact on the sport community in Durham Region has been immense.

Shauna is an outstanding field hockey player and actively supports many sports initiatives throughout the community. She has been a prominent mentor in sports and has been recognized within the Black community for her dedication in developing future leaders. Shauna is a rising star and has received recognition for her years of volunteer service.

In 2019, she was inducted into the Toronto Sport Hall of Honour; in 2020, she received the Sovereign's Medal for Volunteers from the Governor General of Canada; in 2021, she received the Ontario Volunteer Service Award; and in 2022, she was recognized as one of Canada's Top 100 Black women to watch.

Members will please join me in acknowledging Shauna Bookal for her countless contributions to our community and for mentoring young people to realize their full potential, both as athletes and community leaders. I thank Shauna for all she does.

UKRAINE

Mr. Arif Virani (Parkdale—High Park, Lib.): Mr. Speaker, on February 24, 2022, to the shock of the entire democratic world, Russian armed forces started an illegal bombing campaign of the Ukrainian capital of Kyiv in an attempt to overrun the entire country. An invasion that Vladimir Putin thought would be over in a matter of days has now endured for over one year. That is a testament to the people of Ukraine, the courage of their armed forces, the leadership of President Zelenskyy and the response of western allies, like Canada, that have stepped up with humanitarian aid, economic assistance, refuge and, most importantly, weapons to shore up Ukraine in this fight against naked Russian imperialism.

This war can only end with one outcome: a safe and secure Ukraine, which includes all of its territory, meaning Crimea and the Donbass. The resolve of the Ukrainian people in reaching this goal remains firm, and equally, Canada's resolve in supporting Ukraine in its time of need remains unwavering.

Slava Ukraini.

* * *

● (1410)

MEDICAL ASSISTANCE IN DYING

Hon. Ed Fast (Abbotsford, CPC): Mr. Speaker, life is precious and is a beautiful gift. With that in mind, I stand here in support of Canada's most vulnerable. Eight years ago, we warned the Liberal government that its assisted death legislation would create a slippery slope that would put at risk the lives of many vulnerable Canadians. We were right.

The Prime Minister has engineered an unprecedented expansion of Canada's assisted suicide regime by including mentally ill persons and signalling he wants to include children as well. There is absolutely no consensus among Canadians that we should do this. My bill, the mental health protection act, would repeal the government's decision to extend assisted death to mentally ill persons.

Instead of inexorably moving toward a culture of death, let us celebrate and nurture a culture of life. Let us provide these vulnerable Canadians with the social and mental health supports they need to enjoy meaningful and joy-filled lives.

* * *

[*Translation*]

FASHION DETOX CHALLENGE

Mrs. Élisabeth Brière (Sherbrooke, Lib.): Mr. Speaker, this month people are going to take up the fashion detox challenge, which consists in abstaining from buying new clothes for one month.

The fashion industry is one of the most polluting industries in the world. That is why we need to change our consumer habits and turn more toward thrift shops and buying local. Buying local stimulates the economy and supports entrepreneurs in Sherbrooke while thrift shops give new life to our clothing and other items.

Last week, I went to Comptoir familial, a second-hand clothing store in Sherbrooke. Guylaine Ruest and her amazing team of volunteers offer second-hand clothing and items at a low price at two locations. I invite everyone in Sherbrooke to check out the second-hand clothing store and maybe even find a treasure.

Our government is supporting our merchants and organizations and helping them deal with foreign corporations including by funding the buy local initiative. Let us continue to encourage organizations and businesses here at home.

* * *

[*English*]

THE ECONOMY

Mr. Dan Albas (Central Okanagan—Similkameen—Nicola, CPC): Mr. Speaker, the Liberal government says it wants to triple the carbon tax up to $170 a tonne. Thanks to British Columbia's recently tabled budget, we know how much economic harm tripling the carbon tax may cause.

On April 1, the carbon tax goes up to $65 a tonne and may cost British Columbians an extra $600 million a year. It is estimated that with the Liberal plan to triple the cost, the cost may be as high as a staggering $5 billion in British Columbia by 2030. Even the province has said in its own budget that "rural communities may have higher indirect carbon tax burdens (e.g. through higher shipping costs resulting in a higher price for goods) and colder regions of the province may have higher carbon tax costs for home heating."

However, we should hold British Columbia's beer, because the Prime Minister is not done yet. On April 1, this government is also hiking the excise tax on beer, wine and spirits by another 6.3%.

This is all made-in-Canada inflation from a Liberal government that is out of touch and does not care. After eight years of the Liberal government, many Canadians can no longer afford to pay their bills. They need leadership that helps keep life affordable, and under the Conservative leader, they will get it.

* * *

FREEDOMS IN CANADA

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Mr. Speaker, Canadian artists are succeeding on digital platforms with the support of fellow Canadians and from viewers around the world without Bill C-11.

The Liberals' plan is to regulate user content-generating websites, like YouTube, where hundreds of thousands of hours of video content are uploaded every minute. Canadian artists, legal experts and digital content producers are speaking out against Bill C-11, yet the Liberals are not listening. What we see and search online now is different from what we would have after the bill and after the Liberal gatekeepers put regulations in place that would change online algorithms.

Bill C-11 represents yet another example of the Liberals' waste of time and public resources in the name of demanding more control and power over Canadians. In a free and democratic country like Canada, the government should not tell us what we can and cannot see on the Internet. We need to kill Bill C-11.

* * *

● (1415)

ZAHID MALIK

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Mr. Speaker, I rise today to recognize an important stakeholder in my community who lost the battle against cancer.

Zahid Malik was a young, dynamic and humble community worker who really represented the best qualities of our community and the people who strive to strengthen it every day. He leaves behind a legacy as an accomplished small business person, a dedicated philanthropist, a husband and a loving father of three. He was selfless and always ready to lend a helping hand to others without seeking anything in return.

For public servants, our constituents and stakeholders represent the core of our work and the motivation by which we carry out the work in this chamber. Zahid Malik was exactly that: an irreplaceable part of our community who made us all better as public servants and as people. He will be greatly missed by everybody who knew him. May he rest in peace.

* * *

ACCESS TO ADDICTIONS TREATMENT

Ms. Lisa Marie Barron (Nanaimo—Ladysmith, NDP): Mr. Speaker, I rise today to speak about an urgent matter related to the toxic substance crisis.

As we all know, this crisis has been devastating for communities, resulting in countless lives lost and families torn apart. More needs to be done to address this crisis, yet some in this House would rather use misinformation and score political points than care about the best interests of those struggling.

We know that solutions based on the advice of medical health experts save lives; these include safer supply and on-demand treatment for those who are struggling with addiction. Recovery without supports can become a revolving door, and relapses to street drugs are particularly dangerous.

Harm reduction has an important role to play in recovery. We need more examples of the collaborative work that is happening through events like the community dinner and dialogue that took place in my riding of Nanaimo—Ladysmith just a few days ago. At this event, frontline workers, substance users and members of the community all came together to find a path forward.

The Liberal government must prioritize the health and safety of people. I urge all members of this House to work together and support these initiatives to save lives.

[*Translation*]

DENIS RINGUETTE AND JACQUES PELLERIN

Mr. Yves Perron (Berthier—Maskinongé, BQ): Mr. Speaker, today I salute the courage, determination and dedication of two volunteer firefighters from Berthier—Maskinongé.

I want to pay tribute to Denis Ringuette, who is celebrating 50 years of service as a volunteer firefighter in Louiseville, as well as Jacques Pellerin of Yamachiche, who has completed 52 years of loyal service.

They have stepped up for over 50 years, always willing to risk their lives to save others and always ready to suddenly leave a family dinner or a child's party to run towards danger and protect their community. Conviction and a sense of duty spur them on.

Their dedication has kept their fellow citizens safe and protected all these years. Their outstanding discipline and sense of duty has no doubt brought their community peace of mind.

It is with great respect that I congratulate them for their diligence and perseverance.

I want to thank these gentlemen.

* * *

[*English*]

BEIJING

Hon. Michael Chong (Wellington—Halton Hills, CPC): Mr. Speaker, for years, CSIS has assessed that Beijing's foreign interference "can pose serious threats" to the security of Canada. CSIS tracked this interference and brought it to the attention of the Prime Minister, as have others, like Global Affairs Canada's G7 rapid response mechanism.

CSIS advised the Prime Minister that "Canada can make use of a policy that is grounded in transparency and sunlight in order to highlight the point that [foreign interference] should be exposed to the public" and that "Canada can counter [foreign interference] activities by building resilience.... To build resilience, Canadians, communities and all levels of government need to be aware of [foreign interference] threat activities."

The Prime Minister has ignored this advice. He needs to heed the advice of experts, treat Beijing's foreign interference as the serious threat it is and tell us and Canadians exactly what is going on.

* * *

PETER HERRNDORF

Ms. Julie Dzerowicz (Davenport, Lib.): Mr. Speaker, I rise to pay tribute to Peter Herrndorf, a giant in the Canadian arts and culture community and a beloved leader, who died on February 18. Peter spent a lifetime devoted to nurturing our artists, storytellers, journalists and administrators to tell the stories of Canada.

Among many accomplishments, Peter was instrumental in creating The Journal at the CBC and The Agenda at TVO. During his 19-year tenure as president and CEO of the National Arts Centre, he brought together artists and performers from across the country to make it the creative force it is today. He also developed the National Arts Centre's Indigenous Theatre, the first national indigenous theatre department in the world. His most recent role was as chair of Luminato.

Our deepest sympathies go to his wife, Eva Czigler; his children, Katherine and Matthew; and his entire family.

Peter was a passionate defender of public broadcasting and Canadian arts and culture. He will be deeply missed, but his contributions have left a lasting legacy and inspired a new generation of Canadian artists and talent.

ORAL QUESTIONS

● (1420)

[*Translation*]

DEMOCRATIC INSTITUTIONS

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, for the past 10 years, the authoritarian government in Beijing has been trying to give the Prime Minister a helping hand politically, starting with a $200,000 donation to the Pierre Elliott Trudeau Foundation.

Our intelligence services have since informed the Prime Minister that the Chinese government has interfered in two elections to help the Liberal Party, yet the PM has done absolutely nothing.

Will he finally allow a public independent investigation so Canadians can get the truth?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, it will come as no surprise to you that I disagree with the opposition leader's false claims that the government did nothing. As soon as we came to power, we took action against foreign interference in our elections. Ours is the only government ever to have done so.

When my friend, the opposition leader, was the minister responsible for democratic institutions, he did nothing when intelligence agencies raised the issue over 10 years ago.

[*English*]

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, we did not have to, because the Communist dictatorship in Beijing was not helping the Conservative Party to get elected.

Contrary to that, for 10 years the Communist dictatorship in Beijing has been helping the Prime Minister. It gave $200,000 in donations to the Trudeau Foundation and interfered in two successive elections to help the Liberals win. Moreover, the Prime Minister knew about it. After numerous briefings to that effect, he has done absolutely nothing to stop it because he benefits from it.

Will the Prime Minister finally allow a public and truly independent investigation of it?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, we take the issue of foreign interference in Canada's electoral system, any foreign interference, very seriously.

That is why when we formed government, we took a number of unprecedented steps that did not exist when my friend was a minister in the previous government. We created the National Security and Intelligence Committee of Parliamentarians precisely so that parliamentarians from all political parties could have access to classified information and published reports for Canadians. We set up an independent panel of senior public servants to follow exactly the issue of foreign interference in the elections, and we will continue to do more.

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, all they have done is had the former CEO of the China-financed Trudeau Foundation write a report about it in which he unsurprisingly says, "Do not worry; be happy."

We know why the Liberals want to cover this up: They benefited from Beijing's interference in two successive elections. The question is, why is the NDP not actually doing its job? New Democrats have been working against transparency by preventing top Liberal campaign operatives and PMO officials from testifying in committee.

Why will the NDP not stop its cover-up coalition and allow top-level officials to testify and answer questions?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, the Leader of the Opposition wants top-level officials to testify publicly before parliamentary committees.

The good news is that is exactly what they did last week, including the heads of our intelligence agencies, the deputy minister of foreign affairs, and the national security and intelligence advisor to the Prime Minister. I know my friend would be very excited to know that I am going to procedure and House affairs committee myself on Thursday, and I would be happy to answer any questions.

From the beginning we have said that we take this issue very seriously. We have put in place unprecedented steps to deal with foreign interference, and we will continue to do more.

● (1425)

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, we learned that the Prime Minister now has a big announcement to make at 5:00 p.m. today. This, after 10 years of having known that Beijing was interfering to support him with donations to the Trudeau Foundation and help in numerous federal election campaigns. Now he is announcing something.

We know that he is probably going to try to sweep this under the rug by naming a Liberal establishment insider to have a secretive process that would never bring about the truth. What we do not know for sure is whether the NDP is once again going to be a co-conspirator in making that happen.

Will we have a final and clear public investigation so that Canadians know the truth?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, the Leader of the Opposition was the minister responsible for democratic reform in the previous Conservative government.

In 2013, CSIS identified foreign interference as a challenge in the electoral context. Mr. Harper's former national security advisor raised this publicly in 2010, 13 years ago. When my hon. friend was the minister responsible for this very file, he did absolutely nothing to deal with the question of foreign interference.

I know he is frustrated that we have done so much. The good news is that we will continue to do more because we take this issue very seriously.

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, that member could have walked across the floor and let me know that the Trudeau foundation had received $200,000 from Beijing, let me know that the dictatorship in Beijing was planning to interfere in successive elections to help Liberals get elected. If they had been transparent about that back then, we would not be having this conversation now. Instead, we have had 10 years of cover-ups from the Prime Minister, who has benefited from the interference, known about it, been briefed on it and done nothing except to try to sweep it under the rug.

Will the NDP stop covering up for the Liberals and get top PMO and Liberal party officials to answer questions before our committee?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, just because the Leader of the Opposition keeps insisting on a falsehood does not make it real. He knows very well that our government took unprecedented steps to deal with this issue, because we take it seriously: a panel of senior public servants, chaired by the Clerk of the Privy Council; setting up in law the National Security and Intelligence Committee of Parliamentarians, including representatives from all political parties.

We have taken this issue seriously. We have made senior officials available at parliamentary committees. We will continue to do everything we can to strengthen Canadian democratic institutions.

[*Translation*]

Mr. Alain Therrien (La Prairie, BQ): Mr. Speaker, the revelations about Chinese interference reported in The Globe and Mail are cause for concern.

Whether the outcome of the last election would have been the same is not the issue. Any time the integrity of the democratic process is threatened, it is the responsibility of all of us in the House to defend that process. Public trust in our democratic system is at stake here. This goes far beyond partisan politics.

Will the Prime Minister create an independent commission of public inquiry on foreign interference in our elections?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, I agree with my hon. colleague that this should be a non-partisan issue, because we all have an interest in protecting and strengthening our democratic institutions.

Our government has introduced a series of robust measures that were assessed by independent experts following the last two federal elections. The good news is that we are always looking for additional measures that we can bring in with the support, I hope, of all parliamentarians in order to strengthen our democratic system.

Mr. Alain Therrien (La Prairie, BQ): Mr. Speaker, let us talk about the experts. Jean-Pierre Kingsley, the former chief electoral officer, Gerald Butts, a former advisor to the Prime Minister, and even Morris Rosenberg, all agree that there needs to be a public inquiry on the integrity of our elections.

We can look all we want, but it seems that no one is opposed to shedding light on any threat to the functioning of our democratic system. There must be no doubts about the legitimacy of the presence of a member in the House. That is something we definitely do not want.

When will the government establish a public and independent inquiry on foreign interference in elections?

● (1430)

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, I believe that our government has been very transparent about our efforts to counter foreign interference in our elections and our democratic system.

We look forward to working with all parliamentarians in the House of Commons and the Senate. That is exactly why we created, for example, a parliamentary committee to study these and other issues and to report to Canadians. We created intelligence review agencies to effectively ensure that our democratic institutions are protected, and we continue to look for other solutions at the same time.

[*English*]

Mr. Peter Julian (New Westminster—Burnaby, NDP): Mr. Speaker, Canadians are very troubled about the allegations of foreign interference in our elections, but the Prime Minister does not seem concerned at all.

The former head of CSIS, the former head of Elections Canada and even Morris Rosenberg, who wrote the 2021 federal election report, are all encouraging the Prime Minister to go forward with a national public inquiry on foreign interference. PROC of the House of Commons has even adopted an NDP motion that the House may vote on soon, calling for a public inquiry as well.

Therefore, why is the Prime Minister so opposed? Why is he refusing to get answers for Canadians?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, our government is taking the issue of foreign interference in Canada's democratic institutions very seriously. As my colleague heard, our government has taken unprecedented steps since we formed the government in 2015 to put in place a series of measures precisely to provide greater transparency and understanding to Canadians on a threat that has existed for well more than 13 years, which has been publicly discussed for over a decade.

The good news is that our government takes it seriously. The good news is that the 2019 and 2021 elections were decided freely and fairly by Canadians.

[*Translation*]

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Mr. Speaker, in a democratic society, few things are as crucial as the integrity of the electoral process and confidence in institutions.

There are serious allegations of interference, and it is this Prime Minister's responsibility to launch a public inquiry to get to the bottom of it. People deserve transparency. The former head of the Canadian Security Intelligence Service, or CSIS, along with a former chief electoral officer, former senior public servant Morris Rosenberg, and an NDP-led House of Commons committee are calling for a public inquiry.

Why is the Prime Minister saying no?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, I agree with my hon. colleague. It is important that Canadians have confidence in our democratic institutions.

We have taken the issue of foreign interference seriously since the moment we formed government. We have implemented a series of measures, including legislative measures, to ensure that our democratic institutions are protected from unacceptable interference.

As my hon. colleague well knows, we share his concern. The good news is that we will continue to do what is necessary.

[*English*]

Ms. Melissa Lantsman (Thornhill, CPC): Mr. Speaker, we found out that CSIS uncovered a plan to influence the Prime Minister with a $200,000 donation to the Trudeau Foundation from agents of the communist regime in Beijing. The response was to blame CSIS. That is another page out of the playbook of divide, distract, deflect and deny, while the confidence in our democracy hits an all-time low.

The Prime Minister needs to end the cover-up and come clean with Canadians about what he knew and when he knew about it. The Prime Minister refuses. What is he hiding?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, as my hon. colleague, the Minister of Intergovernmental Affairs, has said, we take the threat of foreign interference very seriously, which is why we have taken concrete action, like putting in place threat reduction measures for CSIS and cracking down on foreign funding which could interfere with our domestic elections.

With corresponding transparency through the creation of bodies like the National Security and Intelligence Committee of Parliamentarians to ensure that we are up front with Canadians, all members should be united in protecting our elections. They are sacrosanct. Canadians, and Canadians alone, determine them.

Ms. Melissa Lantsman (Thornhill, CPC): Mr. Speaker, the allegations of foreign interference are serious and they deserve a serious response from a serious Prime Minister. They need to be investigated and they need to be investigated by a credible, non-partisan and independent body. They need to be investigated by Parliament, not by Liberal insiders.

With the help of the NDP, the Prime Minister is refusing to send his chief of staff to committee. Again, what is he hiding?

● (1435)

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, it was this government under the leadership of the Prime Minister that created the National Security and Intelligence Committee of Parliamentarians to encourage and foster collaboration across partisan lines, because this is an issue that transcends that dynamic. We will continue to shine a light on the threats that are posed by foreign interference so we can protect our democratic institutions, especially elections, because Canadians, and Canadians alone, must be reassured that they determine their elections and no one else.

Hon. Michael Chong (Wellington—Halton Hills, CPC): Mr. Speaker, for years, CSIS has tracked Beijing's foreign interference and has said, "foreign interference is a serious threat to the security of Canada." For years, CSIS has advised the Prime Minister that "Canada can make use of a policy that is grounded in transparency and sunlight in order to highlight the point that foreign interference should be exposed to the public."

Will the Prime Minister heed this advice, be transparent and let PMO officials testify before a parliamentary committee?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, I appreciate my colleague's question and I also embrace his concerns around transparency. This is a government that has raised the bar of transparency through the creation of NSICOP and through the creation of the National Security and Intelligence Review Agency, which both have robust access to classified information so we can be up front with Canadians in the ways in which we are protecting all of our institutions, especially elections.

As my colleague, the Minister of Intergovernmental Affairs, said, we have good news. Two independent panels have concluded that both of the elections in 2019 and 2021 were free and fair. We will continue this work together.

Hon. Michael Chong (Wellington—Halton Hills, CPC): Mr. Speaker, they concluded overall that they were free and fair.

Last election, the G7 rapid response mechanism in Global Affairs Canada tracked Chinese Communist Party interference targeting candidates like Kenny Chiu. Despite Global Affairs tracking interference in real time during the election, nothing was done. Kenny Chiu was not informed. Clearly, the critical election incident protocol did not work.

Since the PMO had a hand in setting up this protocol, will the PMO let its officials testify in front of a committee in order to tell us why the protocol was set up the way it was?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, as my colleague knows, this government set up the SITE panel and the critical instant reporting protocol to ensure that independent, non-partisan, professional public servants would make decisions about which allegations of foreign interference would be disclosed. This is a process that has served our democracy well.

Now we will take the recommendations from Morris Rosenberg and work closely with the public service to implement them so we can build on the strong track record of this government, which remains vigilant and clear-eyed about fighting against the threats of foreign interference.

[*Translation*]

Mr. Luc Berthold (Mégantic—L'Érable, CPC): Mr. Speaker, the Liberal Prime Minister initially denied allegations of foreign interference in our elections by the communist regime in Beijing. He thought he could sweep the whole thing under the rug and people would move on, but that did not happen. Suddenly, all kinds of things were revealed in the papers, on Global News, in the Globe and Mail, and the revelations keep coming. Every day, we find out more about how the communist regime in Beijing interfered in our elections. While the PM looked the other way, the Trudeau Foundation returned $200,000 to a Chinese businessman.

Why is the Prime Minister refusing to launch a public inquiry into Beijing's interference in our elections?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, as my colleague clearly stated, our government took this matter seriously the moment we took office. My colleague across the way claims people looked the other way, but he knows that is not the case. As my colleague pointed out, there were threats over 10 years ago, and if his government had taken them seriously, it might have implemented robust measures like the ones we implemented specifically to counter this kind of unacceptable interference. We will keep doing what needs to be done to strengthen our institutions.

Mr. Luc Berthold (Mégantic—L'Érable, CPC): Mr. Speaker, if he wants to talk about the past, then let us talk about 2013. In front of a group of women gathered for a Liberal Party fundraiser, a person in the audience asked the Prime Minister what country he admired, other than Canada. He answered, and I quote: "There's a level of admiration I actually have for China. Their basic dictatorship is actually allowing them to turn their economy around on a dime."

We will not take any lessons from the Liberal Party's past. The regime in Beijing employed a sophisticated strategy to disrupt the 2021 federal election through its diplomats and their proxies. That is what we learned from The Globe and Mail.

Why is he refusing to allow Katie Telford to testify before the committee?

● (1440)

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, my colleague mentioned 2013. I thought he was going to say that that was when CSIS identified the potential threat of Chinese interference in our election. Who was the minister responsible for the integrity of democratic institutions in 2013? It was the current Leader of the Opposition. He did nothing in 2013 or in 2014. He did not do anything in 2015 either.

Mr. René Villemure (Trois-Rivières, BQ): Mr. Speaker, there are two possibilities: Either Chinese authorities are interfering in our electoral system and we have to do everything in our power to stop them, or there is no interference and a commission of inquiry will help restore public trust in our electoral system. In any case, the best thing to do, or rather, the only thing we can do to ensure that the public continues to trust their institutions, is to launch an inquiry.

Under these circumstances, when will the government call an independent commission of public inquiry?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, as I said a few moments ago, since we formed government, we have acknowledged the threats of foreign interference in our democratic system, in our democratic institutions. That is why we amended the Canada Elections Act to prevent foreign contributions to our election campaigns. That is why we passed legislation, a bill, to create a committee in charge of overseeing the national security agencies, with representatives from all parties, including the Bloc Québécois, and we referred this important matter to those members.

Mr. René Villemure (Trois-Rivières, BQ): Mr. Speaker, let us be serious. The Prime Minister must realize that he is sending the wrong message by refusing to create a commission of inquiry. What does he have to hide? What is he trying to protect? Who is involved and how?

Those kinds of questions are not the right message to send. The message should be that we will never let anyone interfere in our electoral system, and we will do everything in our power to prevent any foreign interference. To do that, we need an independent commission of public inquiry.

Will they set up an independent commission of public inquiry?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, I agree with my hon. colleague that we must work together to do whatever it takes to safeguard elections in Canada and our democratic institutions.

I have good news for him: That is exactly what our government has been doing since we came to power. We are always looking for advice on how to strengthen the robust measures that are already in place.

We will continue to do whatever it takes because we agree with my colleague that this interference is completely unacceptable.

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Mr. Speaker, the Standing Committee on Procedure and House Affairs passed a motion calling for the creation of an independent commission of public inquiry on foreign interference in our elections.

The committee agreed with the Bloc Québécois proposal that the commission chair be appointed with the consent of all parties represented in the House. Why is that important? Because it must transcend partisan politics. What matters most is the absolute infallibility of the electoral system.

Will the government comply with the committee's request and create a commission of inquiry into foreign interference in elections?

Hon. Dominic LeBlanc (Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Mr. Speaker, I agree with my hon. colleague that we must work together, as parliamentarians, precisely to counter foreign interference in our democratic institutions.

My colleague knows this very well because she sits on the parliamentary committee. I look forward to seeing her when I attend on Thursday.

We have been transparent with parliamentarians, but we have also introduced important measures to counter foreign interference. These measures are working very well.

● (1445)

[*English*]

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Mr. Speaker, the Globe and Mail reported, based upon a review of CSIS documents, that Beijing launched "an orchestrated machine" to help the Liberals in the 2021 election. In the face of these alarming revelations, Canadians deserve answers from the Prime Minister. What they do not deserve is a Prime Minister who obstructs, deflects and hides.

If the Prime Minister has nothing to hide, will he let his chief of staff testify before a committee, or is he going to double down on his cover-up?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, as my colleague has heard now on a number of occasions, we take these matters very, very seriously. We approach them very soberly, and that is why this government has put in place the authorities required for CSIS to both address and mitigate potential foreign interference.

That is why we have also created the requisite transparency for Canadians, including through the creation of NSICOP, NSIRA, and the independent panels, which have both examined the circumstances and the allegations around the 2019 and 2021 elections. Yes, both those elections were free and fair, but we will continue to do this work together.

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Mr. Speaker, Conservatives have tried to bring the Prime Minister's chief of staff to testify at committee three times. The Liberals, with the support of the NDP, blocked that effort three times, despite scandalous reports that senior PMO officials had been briefed by CSIS about Beijing's interference and did nothing about it.

Is the Prime Minister shielding his chief of staff because he knows his PMO turned a blind eye to Beijing's interference?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, my colleague and the member of the parliamentary committee had the benefit of hearing extensive evidence from our government's most senior public servants implicated in the area of national security and intelligence, including the Prime Minister's national security advisor.

It is important for my colleague to remember that this is not a partisan issue. That is why we will continue to be upfront in that committee. That is why we will continue to leverage the other agencies and bodies, which are there to raise the bar of transparency and sunlight in the way we fight against foreign interference, so we can protect our democratic institutions.

Mr. Kyle Seeback (Dufferin—Caledon, CPC): Mr. Speaker, what are they trying to hide? That is the question.

It is pretty clear that this Beijing communist influence operation has been going on in Canada for a long period of time. We know that senior members of the PMO were briefed. All we are asking is that they come to testify, but they hide. They obfuscate. They will not deliver these people.

Why? That is the question that Canadians should be asking themselves. What are they hiding? Why will they not bring her to testify?

Hon. Marco Mendicino (Minister of Public Safety, Lib.): Mr. Speaker, every reasonable member in this chamber can look at the laws we put into place, including the bodies and agencies, to readily see that they contribute to being transparent and upfront with Canadians. Those are important institutions that are there so we can explain to Canadians how we are tackling this issue together.

The parliamentary committee has heard from witnesses. We are continuing to look for ways we can be transparent with Canadians so we can undertake the work of fighting together against foreign interference to protect our democratic institutions.

* * *

CLIMATE CHANGE

Ms. Laurel Collins (Victoria, NDP): Mr. Speaker, Canada's spy agency has warned us that the climate crisis will threaten national security, critical infrastructure and our food systems, but in the face of this clear and very real threat, we have the Conservatives, who deny that we need to act, and the Liberals, who keep delaying while handing out billions to big polluters. Oil and gas CEOs are laughing as they rake in record profits and scale down their climate commitments.

The climate crisis threatens everything we hold dear. When will this government force big polluters to clean up their act and stop making Canadians pay the price?

Hon. Steven Guilbeault (Minister of Environment and Climate Change, Lib.): Mr. Speaker, my colleague's question points exactly to the reason why, in the last year alone, we have presented the first-ever emissions reduction plan for Canada, which shows a path of how Canada will meet its 2030 targets. For the first time in history, we have put forward a national adaptation strategy. Both have been applauded by industry, non-governmental organizations and experts alike, and it is why we are investing $120 billion to fight climate change and support Canadians.

● (1450)

GROCERY INDUSTRY

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Mr. Speaker, Canadians are really worried about keeping up with the high cost of their groceries, and the prices just keep going up.

While people are stretching their budgets to handle growing costs, rich corporations and grocery chains are making massive profits. Last week, the European Central Bank expressed concerns that CEOs are using the cost of living crisis and inflation to hike their prices, and the Bank of Canada is admitting to having the same fears.

Will the Liberals finally admit that rich CEOs and corporate greed are helping drive up food prices, and will they make them pay what they owe?

Hon. Randy Boissonnault (Minister of Tourism and Associate Minister of Finance, Lib.): Mr. Speaker, I thank the hon. member for his question.

We have been very clear on this. We have spoken with the CEOs of grocery companies in this country. We have referred the matter to the Competition Bureau. My colleague, the Minister of Innovation, Science and Industry, has been very clear on this matter.

When it comes to asking large corporations to do their fair share, we have the Canada dividend recovery, which makes sure that the banks and the insurance companies in this country pay their fair share. Profits in excess of $1 billion will be subject to additional tax.

We are making sure that Canadians can meet the affordability challenge they are facing. That is our job. We are on it.

* * *

GENDER-BASED VIOLENCE

Hon. Judy A. Sgro (Humber River—Black Creek, Lib.): Mr. Speaker, during the pandemic, gender-based violence increased at an alarming rate. We simultaneously saw that crisis lines were used more than ever across Canada, and this demand, unfortunately, continues today.

Could the Minister for Women and Gender Equality and Youth share what our government is doing to respond to this heartbreaking increase and provide support to those experiencing gender-based violence?

Hon. Marci Ien (Minister for Women and Gender Equality and Youth, Lib.): Mr. Speaker, I thank the hon. member for shining a light on this very important issue.

Crisis hotlines are a lifeline for women fleeing domestic violence because they provide a connection to safe resources. Our announcement last week of $8 million to support crisis hotlines across Ontario is our ninth agreement with our provincial and territorial counterparts. The bottom line is, if someone is experiencing gender-based violence, when they call or text, someone will be there 24 hours a day, seven days a week, 365 days a year.

HOUSING

Mr. Jasraj Singh Hallan (Calgary Forest Lawn, CPC): Mr. Speaker, after eight years of this Liberal Prime Minister's failures, home is where the broken heart is.

Housing has become more unaffordable, unattainable and more broken than ever before. The Governor of the Bank of Canada admitted that it was the Liberals' overspending that caused eight consecutive bank interest rate hikes in one year, and now homes are more unaffordable than ever before. After eight years of the Liberals' failures, mortgage costs do not even cover interest payments.

Will the Prime Minister take some responsibility for breaking housing and stop gatekeeping so we can fix everything he broke?

Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.): Mr. Speaker, I will inform the hon. member that he just has to look very close around himself to see that the biggest gatekeepers are all in his caucus.

They vote against every housing measure to remove barriers against more housing supply. They vote against supports for first-time homebuyers to not only build more affordable housing, but also to help them access more homes. They voted against the rapid housing initiative. They voted against the co-op program. They voted against the national housing co-investment fund. I am running out of time, but they need to get their act together.

Mr. Jasraj Singh Hallan (Calgary Forest Lawn, CPC): Mr. Speaker, we will always vote against failed Liberal policies that double home costs across this country. After eight years of the Liberals' failed policies, rents, mortgages and home prices have doubled, and home ownership is nothing but a dream for newcomers.

Not everyone has a trust fund, such as the Prime Minister does, or can absorb all the tax hikes the Liberals keep causing for newcomers and Canadians alike. Will the Liberals finally take some responsibility, admit that they have caused this housing crisis and get out of the way so we can show them how to fix it?

Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.): Mr. Speaker, Canadians can see through the gimmicks and the hot air. This is the fact: When we brought real measures to help Canadian renters with the cost of rent, the Conservatives not only voted against it, they also played procedural games in the House to delay the passage of those much-needed rental supports.

In addition to that, we have passed legislation to increase the housing supply to help Canadians who are purchasing their first home, and we have put in place measures to make sure that we remove barriers to building more housing supply. For all of these measures, the Conservatives voted against them.

Ms. Michelle Ferreri (Peterborough—Kawartha, CPC): Mr. Speaker, nine out of 10 young Canadians have completely given up the hope of ever owning a home. Why is that? It is because, under this Prime Minister, housing and rental prices have doubled. The average monthly mortgage payment for a Canadian family is $3,000. This is outrageous. Canadian families are suffering. Food is up 12%. The time for change is long overdue.

Will the Prime Minister show some leadership, step down and take accountability or get out of the way so we can fix what he has broken?

● (1455)

Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.): Mr. Speaker, their party's record on housing is very clear. Not only while in government, but also while in opposition, the Conservatives have not taken the time to reflect on the importance of federal leadership and investment in housing. Their caucus has been very clear that it believes the federal government should do less on housing. We on this side of the House believe we should do more, and we are doing more.

[*Translation*]

Mr. Richard Martel (Chicoutimi—Le Fjord, CPC): Mr. Speaker, here is how Canada has changed since 2015. After eight years under this Prime Minister, average mortgage payments have more than doubled. After eight years under this Prime Minister, the cost of groceries has gone up by 11.6%.

In a G7 country, it is now extremely difficult for people to feed and house themselves. The Prime Minister says none of this is his fault. Will he at least admit that he has done Canadians wrong and accept responsibility for what he broke?

Hon. Randy Boissonnault (Minister of Tourism and Associate Minister of Finance, Lib.): Mr. Speaker, what are we hearing from the members opposite? Hopelessness. Useless words and facts that will not help Canadians. What we are not hearing from the members opposite is a plan. They have no plan for housing, no plan to fight climate change, no plan for the economy and no plan to make life more affordable.

Their team has no plan. Fortunately, we are over here on this side.

* * *

IMMIGRATION, REFUGEES AND CITIZENSHIP

Mr. Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ): Mr. Speaker, the Prime Minister made a rather unexpected comment as the House was rising for a two-week recess. He said that we all want Roxham Road to close. That was news to us. For years we have been asking the government to close Roxham Road, explaining that Quebec has exceeded its capacity, that it is not safe and that it is creating an illegal human smuggling industry. Now he tells us that he wants to close Roxham Road.

That raises a question: Why did the government recently renew the lease on the adjacent land for ten years if it truly wants to close Roxham Road immediately?

Hon. Sean Fraser (Minister of Immigration, Refugees and Citizenship, Lib.): Mr. Speaker, as the member well knows, closing Roxham Road is not a simple matter. It is essential that we work with the communities, with the province and with our partners in the United States. I will continue to work with our partners in the United States and in Canada to ensure that Canada meets its obligations to refugee claimants.

Mr. Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ): Mr. Speaker, the Prime Minister also said that simplistic solutions will not be how it is done. We agree on that. Speaking of simplistic solutions, there are just 17 days left before the Conservative leader's ultimatum expires, but we will come back to that.

We have a simple solution, not a simplistic one. It involves suspending the safe third country agreement. That way, there will no longer be any advantage to crossing at Roxham Road to file a claim for refugee protection that could be filed at any regular border crossing. That is the humane thing to do.

When will the federal government suspend the safe third country agreement? It could do so as early as today. When will it do so?

Hon. Sean Fraser (Minister of Immigration, Refugees and Citizenship, Lib.): Mr. Speaker, suspending the agreement with the United States will just move the problem elsewhere. It is not a real solution. It is essential that we work with communities across the country. It is essential that we continue our work with the United States and the provinces.

I have a meeting with my counterpart from Quebec. I will continue to work with her and with the other provinces and communities to come up with a sustainable solution.

* * *

[*English*]

CANADIAN HERITAGE

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Mr. Speaker, these Liberals are so determined to have control over the lives of Canadians that they want to control what Canadians are able to see on the Internet.

The online censorship bill is a back door for the Liberals to silence their critics. Social media executives have said that the measures in this bill are the same used by North Korea, Cuba and the communist regime in Beijing.

When will the Liberals scrap this attack on free speech?

Hon. Pablo Rodriguez (Minister of Canadian Heritage, Lib.): Mr. Speaker, I do not think my colleague understands what he is talking about.

If he is talking about Bill C-11, it is simply asking streamers to support Canadian culture. If he is talking about C-18, it is simply asking the web giants to support independent journalism.

One thing remains: the Conservatives keep filibustering things that are absolutely essential for Canadians. If they do not want to help, they should stay out of the way and let us do the job.

● (1500)

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Mr. Speaker, while Conservatives are standing up for Canadian creators and helping them to be successful, the Liberals are looking to do everything they can, and I am sure if we let them, they would freeze the bank accounts of Canadians they disagree with. The Liberals could not even pick Canadian content out of a lineup if we circled it for them.

After eight years of the Prime Minister, it is time for a government that protects Canadian free speech and that protects Canadian creators' rights. Will the Liberals scrap their online censorship bill?

Hon. Pablo Rodriguez (Minister of Canadian Heritage, Lib.): Mr. Speaker, Conservatives think that culture is what one finds in a yogourt bowl.

They never raise it. They do not care about it. They stand up for the web giants and that is it—

Some hon. members: Oh, oh!

The Deputy Speaker: Order, order.

[*Translation*]

The hon. minister, from the top.

[*English*]

Hon. Pablo Rodriguez: Mr. Speaker, we are here, supporting our culture, our artists, our creators, our music industry, our books, our television, our movies.

What are Conservatives supporting? They are supporting web giants and tech giants. That is it. They are standing up for them, not for Canadians.

On this side, we are standing up for Canadians.

[*Translation*]

Mr. Gérard Deltell (Louis-Saint-Laurent, CPC): Mr. Speaker, we, the Conservatives, stand up for Quebec and the provinces.

Last April, the Government of Quebec sent a letter to the Minister of Canadian Heritage. What did the Minister of Canadian Heritage do with that letter? He went into his office, looked around to ensure no one was there, lifted his pile of files and put the letter at the bottom. He did nothing for one year. With the collusion of the Bloc Québécois, there has been radio silence.

The Minister of Canadian Heritage is a seasoned parliamentarian. He knows that the best way to tackle a file is to bring people before a parliamentary committee.

Will the Minister of Canadian Heritage persuade his Bloc friends to say yes to Quebec's demand?

Hon. Pablo Rodriguez (Minister of Canadian Heritage, Lib.): Mr. Speaker, the government has said yes to various demands made by Quebec. We are working with Quebec. What Quebec wants is to see Bill C-11 passed for the music, film and television industries.

The Conservatives, who have filibustered the bill the entire time, have suddenly woken up to say that culture is important. Since when has culture been important to the Conservatives? They could not care less. Our government will be there for our artists despite the Conservatives.

* * *

OFFICIAL LANGUAGES

Mr. John Aldag (Cloverdale—Langley City, Lib.): Mr. Speaker, in British Columbia and across the country, more and more young people are interested in learning French. Last week, to launch Francophonie Month, I visited an immersion class with the Minister of Official Languages.

Can the minister tell the House how she is supporting French-language instruction in our province?

Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.): Mr. Speaker, I want to thank my friend and colleague from Cloverdale—Langley City for his important question. I also wish him a happy Francophonie Month.

I was very pleased to be in the Vancouver area last week where we announced an investment of nearly $13.5 million, in partnership with the Government of British Columbia, to support a series of projects to recruit, train and retain more francophone teachers.

The federal government will always be there to support our francophone communities across the country.

* * *

[*English*]

HEALTH

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, the Prime Minister said this week that he was surprised that his own health department granted a permit to a company to get into the cocaine business. I do not know why he would be surprised. His own addictions minister put out an ordinance on January 30 allowing for cocaine, crack, heroin and other deadly drugs to be possessed and used in British Columbia. This is the obvious consequence of his decision.

Why does he not reverse his decision and ban cocaine and other deadly drugs?

Hon. Carolyn Bennett (Minister of Mental Health and Addictions and Associate Minister of Health, Lib.): Mr. Speaker, there are very strict rules in place for obtaining and maintaining a controlled substance licence in Canada. These licences by Health Canada for controlled substances are for scientific and medical purposes only. Companies cannot sell products to the general public.

Health Canada has contacted the companies holding a licence to reiterate the very narrow parameters of their licence and asked them to retract any misleading statements. If the strict requirements are not being followed, Health Canada will not hesitate in revoking the licences.

● (1505)

Hon. Pierre Poilievre (Leader of the Opposition, CPC): Mr. Speaker, the misleading statements are coming from the government, which actually decriminalized cocaine, crack, heroin and other deadly drugs. We can forgive the company for believing that when it got a permit to get into the cocaine business that is exactly what it meant. In fact, the company got the permit for cocaine in two months, so it is faster to get a cocaine permit than a passport in Canada under the Prime Minister.

Why do we not bring back some common sense and ban cocaine and other dangerous drugs to protect our people?

Hon. Carolyn Bennett (Minister of Mental Health and Addictions and Associate Minister of Health, Lib.): Mr. Speaker, the member knows full well that Health Canada acted swiftly and has issued regulatory letters to Adastra Labs and Sunshine Earth Labs regarding the misinformation they published. Health Canada spoke to both companies and requested immediate action to retract and clarify their statements. Both Adastra Labs and Sunshine Earth Labs issued a retraction and updated their press release. Health Canada issued a bulletin to all licensed dealers across the country clarifying their responsibilities and authorities under their licences.

* * *

COMMITTEES OF THE HOUSE

Mr. John Nater (Perth—Wellington, CPC): Mr. Speaker, my question is for the Chair of the Standing Committee on Procedure and House Affairs. The committee has charged the chair to table before the House a report calling on the government to launch an inquiry into foreign interference in Canadian elections, while also maintaining the committee's agenda and scheduled meetings into these serious allegations.

Will the chair of the procedure and House affairs committee do the right thing, rise in the House today after question period and table the committee's report?

Hon. Mark Holland (Leader of the Government in the House of Commons, Lib.): Mr. Speaker, as is the case with all committees, that committee report will be given the opportunity to be—

An hon. member: If the chair's not here, can the vice chair answer?

The Deputy Speaker: Order, please. Can a member answer their own question? Let me talk to the people at the table for just one moment and I will come back.

After consulting with the table, a member cannot answer their own question, so the first person to stand up gets the opportunity to answer that question.

The hon. government House leader.

Hon. Mark Holland: Mr. Speaker, I appreciate the opportunity to stand, and I appreciate the enthusiasm for hearing me speak. However, as is always the case, when committees bring forward reports, in due course they will appear before the House and there will be an opportunity for the chamber to deliberate on those reports.

TELECOMMUNICATIONS

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): Mr. Speaker, last week, the York Region Liberal caucus announced a $19-million investment in YorkNet through the universal broadband fund. This funding will improve broadband capacity for over 3,800 underserved households in York Region, closing 99% of the underserved gap.

Could the Minister of Rural Economic Development please update the House on the work our government is doing to make sure all Canadians have access to reliable high-speed Internet?

Hon. Gudie Hutchings (Minister of Rural Economic Development, Lib.): Mr. Speaker, I thank my colleague from Newmarket—Aurora for his dedication to rural Ontarians.

It is great news for the people of the York Region, for small business, big business, not-for-profits and, frankly, good news for everyone. We know that having access to reliable high-speed Internet is the economic equalizer to open up countless opportunities. Since 2015, we have on the table over $7 billion for connectivity. We have connected over a quarter of a million households, but we are not stopping. By 2026, 98% of Canadians will be connected and by 2030, 100% of Canadians will have access to Internet.

* * *

● (1510)

FISHERIES AND OCEANS

Ms. Lisa Marie Barron (Nanaimo—Ladysmith, NDP): Mr. Speaker, open-net fish farms pollute our waters and harm wild Pacific salmon. The health of wild salmon is critical. First nation chiefs across British Columbia have been calling on the Prime Minister to get these harmful fish farms out of our waters, but he is refusing to meet them. He is in luck as B.C. first nations are currently in Ottawa advocating to protect wild Pacific salmon.

Will the Prime Minister meet with these first nations and commit to get these fish farms out of the water, with a plan for all those impacted?

Hon. Joyce Murray (Minister of Fisheries, Oceans and the Canadian Coast Guard, Lib.): Mr. Speaker, I am happy to say that I met with the delegation this morning and we have plans to continue working together so that we can include all of the first nations affected by open-net pen aquaculture as we transition away over the coming years.

[*Translation*]

OFFICIAL LANGUAGES

Mr. Alain Rayes (Richmond—Arthabaska, Ind.): Mr. Speaker, we have reached the final analysis of Bill C-13 on modernizing both official languages.

Tomorrow, in committee, members will address the amendments on the issue of language clauses to ensure that francophone minority communities will indeed receive the money invested by the federal government when an agreement is reached between the provinces and the federal government or between the territories and the federal government. Such clauses would ensure equity for all francophones in the country. Every francophone advocacy group agrees on that.

I would like the minister to clearly indicate whether she agrees with these language clauses, please.

Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.): Mr. Speaker, I want to thank my colleague for his important question.

As he aptly noted, Bill C-13 is currently before the Standing Committee on Official Languages for a clause-by-clause review. Official language minority communities have been waiting for this bill for a long time. Like them, I look forward to having this bill adopted.

I hope that the committee will complete its work shortly since stakeholders from one end of the country to the other want this bill passed as soon as possible.

GOVERNMENT ORDERS

[*English*]

BUSINESS OF SUPPLY

OPPOSITION MOTION—PUBLIC HEALTH CARE FUNDING AND DELIVERY

The House resumed from February 16 consideration of the motion.

The Deputy Speaker: It being 3:13 p.m., pursuant to order made on Thursday, June 23, 2022, the House will now proceed to the taking of the deferred recorded division on the motion relating to the business of supply.

Call in the members.

And the bells having rung:

The Deputy Speaker: The question is on the motion. May I dispense?

Some hon. members: No.

[*Chair read text of motion to House*]

● (1525)

(The House divided on the motion, which was negatived on the following division:)

(Division No. 262)

YEAS

Members

Angus	Ashton
Bachrach	Barron
Blaikie	Blaney
Boulerice	Cannings
Collins (Victoria)	Davies
Desjarlais	Garrison
Green	Hughes
Idlout	Johns
Julian	Kwan
MacGregor	Mathyssen
May (Saanich—Gulf Islands)	McPherson
Morrice	Singh
Vuong	Zarrillo– — 26

NAYS

Members

Aboultaif	Aitchison
Albas	Aldag
Alghabra	Ali
Allison	Anand
Anandasangaree	Arnold
Arseneault	Arya
Atwin	Bains
Baker	Baldinelli
Barlow	Barrett
Barsalou-Duval	Battiste
Beaulieu	Beech
Bendayan	Bennett
Bergeron	Berthold
Bérubé	Bezan
Bibeau	Bittle
Blair	Blanchet
Blanchette-Joncas	Block
Blois	Boissonnault
Bradford	Bragdon
Brassard	Brière
Brunelle-Duceppe	Calkins
Caputo	Carrie
Casey	Chabot
Chagger	Chahal
Chambers	Champagne
Champoux	Chatel
Chen	Chiang
Chong	Collins (Hamilton East—Stoney Creek)
Cooper	Cormier
Coteau	Dabrusin
Dalton	Damoff
Dancho	Davidson
DeBellefeuille	Deltell
Desbiens	Desilets
Dhaliwal	Dhillon
Diab	Doherty
Dong	Dowdall
Dreeshen	Drouin
Dubourg	Duclos
Duguid	Duncan (Stormont—Dundas—South Glengarry)
Dzerowicz	Ehsassi
El-Khoury	Ellis
Epp	Erskine-Smith
Falk (Battlefords—Lloydminster)	Falk (Provencher)
Fast	Fergus
Ferreri	Fillmore
Findlay	Fisher
Fonseca	Fortier
Fortin	Fragiskatos
Fraser	Freeland
Fry	Gaheer

Gallant
Garon
Généreux
Gerretsen
Gladu
Goodridge
Gourde
Guilbeault
Hallan
Hardie
Hoback
Housefather
Hutchings
Ien
Jeneroux
Jowhari
Kelloway
Khalid
Kitchen
Koutrakis
Kramp-Neuman
Kusie
Lake
Lambropoulos
Lamoureux
Lapointe
Lattanzio
LeBlanc
Lehoux
Lewis (Essex)
Liepert
Lloyd
Long
Louis (Kitchener—Conestoga)
MacDonald (Malpeque)
Maguire
Martel
May (Cambridge)
McCauley (Edmonton West)
McGuinty
McKinnon (Coquitlam—Port Coquitlam)
McLeod
Mendès
Miao
Miller
Morantz
Morrissey
Murray
Naqvi
Ng
Normandin
Oliphant
O'Toole
Paul-Hus
Perkins
Petitpas Taylor
Poilievre
Qualtrough
Redekopp
Rempel Garner
Roberts
Rodriguez
Romanado
Ruff
Sajjan
Samson
Savard-Tremblay
Scheer
Schmale
Serré
Shanahan
Shields
Sidhu (Brampton East)
Garneau
Gaudreau
Genuis
Gill
Godin
Gould
Gray
Hajdu
Hanley
Hepfner
Holland
Hussen
Iacono
Jaczek
Joly
Kayabaga
Kelly
Khera
Kmiec
Kram
Kurek
Kusmierczyk
Lalonde
Lametti
Lantsman
Larouche
Lauzon
Lebouthillier
Lemire
Lewis (Haldimand—Norfolk)
Lightbound
Lobb
Longfield
MacAulay (Cardigan)
MacKinnon (Gatineau)
Maloney
Martinez Ferrada
Mazier
McDonald (Avalon)
McKay
McLean
Melillo
Mendicino
Michaud
Moore
Morrison
Motz
Muys
Nater
Noormohamed
O'Connell
O'Regan
Patzer
Pauzé
Perron
Plamondon
Powlowski
Rayes
Reid
Richards
Robillard
Rogers
Rood
Sahota
Saks
Sarai
Scarpaleggia
Schiefke
Seeback
Sgro
Sheehan
Shipley
Sidhu (Brampton South)
Simard
Small
Soroka
Steinley
Stewart
Strahl
Tassi
Thériault
Thomas
Tochor
Trudeau
Turnbull
Valdez
van Koeverden
Vandal
Vecchio
Vien
Vignola
Virani
Wagantall
Waugh
Weiler
Williams
Yip
Zimmer
Sinclair-Desgagné
Sorbara
Sousa
Ste-Marie
St-Onge
Stubbs
Taylor Roy
Therrien
Thompson
Tolmie
Trudel
Uppal
Van Bynen
Van Popta
Vandenbeld
Vidal
Viersen
Villemure
Vis
Warkentin
Webber
Wilkinson
Williamson
Zahid
Zuberi– — 298

PAIRED

Members

Badawey
Lawrence– — 2

The Deputy Speaker: I declare the motion defeated.

I wish to inform the House that because of the deferred recorded division, Government Orders will be extended by 13 minutes.

* * *

POINTS OF ORDER

ORAL QUESTIONS

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Mr. Speaker, I am rising on a point of order arising out of question period. A question was asked of a committee chair, and I am looking for clarification. I have had some personal experience with this in the chamber.

I would refer you to the 42nd Parliament. As a matter of fact, it happened to be the day the Prime Minister first decided to do Prime Minister's questions, where he answers every question. At that time, I was the second vice-chair of the access to information, privacy and ethics committee, and the chair and the vice-chair were both away on parliamentary business. A question was asked of the committee chair for that committee, and as the second vice-chair at that time, I stood to answer the question.

As it happens, the Prime Minister did not answer all of the questions that day, but more importantly, I think it served the House well to have someone who was an authorized spokesperson for the committee answer the question. There is often debate in this place about the appropriate role of parliamentary secretaries on committees and the right posture of the government toward committees, and I do not think it makes a lot of sense to have government members answer questions about committee business.

I wonder if the Chair might reflect on this point and come back with some guidance. I think the House would be well served if the Chair first looked to see if an authorized spokesperson for the committee is standing before proceeding to the government bench. I would welcome the Chair's reflection on that point at some appropriate time, whether that is right away or further down the line.

● (1530)

The Deputy Speaker: I will refer to it at a later point, but I will go to the hon. member for Perth—Wellington on the same point of order.

Mr. John Nater (Perth—Wellington, CPC): Mr. Speaker, I would refer you to *Beauchesne's*, sixth edition, which is one of this House's great authorities. It makes note of the importance of seeking information from the committee, in which case the chair or the vice-chair is certainly the appropriate person.

I would seek the guidance of the Chair, however, for situations in which the chair of the committee may be available online but nonetheless failed to indicate to the Chair that they were present online to answer the question. Therefore, I would seek the Chair's guidance. I would add that as vice-chair of the Standing Committee on Procedure and House Affairs, I am certainly ready, able and willing to table the committee's report at the soonest and nearest convenience of this House.

The Deputy Speaker: It is not often we get to bring out *House of Commons Procedure and Practice*, but I thought we would do that.

On the same page that was quoted, in the section "Questions Concerning Matters Before Committees", footnote 92 cites pages 10,207 and 10,208:

> On occasion, questions directed to committee Chairs have been answered by Ministers and points of order have been raised. For example, during Question Period, opposition Members twice addressed questions to the Chair of a standing committee and the Government House Leader responded.... In the 2008 example, the Liberal House Leader rose the following day on a point of order and asked the Speaker if someone other than the Chair of a committee could respond to a question concerning the agenda of a committee. The Speaker advised that his role is to "take a look at those who are standing to answer and choose who is going to answer".

I can say that during today's session, no hands went up on Zoom and no other vice-chair stood up. The person who asked the question could not answer the question. Therefore, the government House leader was the one who got to answer that question, because he did stand to answer it.

However, we will look at it further. I do not want to be revising this book, so it is probably going to stand, but we will have a further look at it as well. I appreciate the interest.

The hon. parliamentary secretary to the government House leader.

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Mr. Speaker, just to add a bit to it, the concern I would have is that the types of questions that could be posed to chairs, from what I understand, are somewhat limited, dealing strictly with the timing of things on a committee's agenda. For anything beyond that, as I understand, it should be the option of the government to determine who answers the question.

The Deputy Speaker: It is getting too deeply in the weeds, but yes, the questions have to be based on the agenda of the committee at hand. I appreciate that intervention as well.

ROUTINE PROCEEDINGS

[*Translation*]

HEALTH

Hon. Jean-Yves Duclos (Minister of Health, Lib.): Mr. Speaker, I am pleased to table, in both official languages, the report on COVID-19 rapid test procurement and distribution.

* * *

[*English*]

COMMITTEES OF THE HOUSE

HEALTH

Mr. Sean Casey (Charlottetown, Lib.): Mr. Speaker, I have the honour to present, in both official languages, the 10th report of the Standing Committee on Health, entitled "Addressing Canada's Health Workforce Crisis".

[*Translation*]

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this report.

* * *

● (1535)

[*English*]

COURT CHALLENGES PROGRAM ACT

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.) moved for leave to introduce Bill C-316, An Act to amend the Department of Canadian Heritage Act (Court Challenges Program).

He said: Mr. Speaker, I am happy to introduce my private member's bill, which would enshrine the court challenges program into federal law. The court challenges program supports Canadians seeking to bring cases of national significance that protect our constitutional rights. It plays a vital role in ensuring that the government acts within the bounds of the Constitution and the Official Languages Act.

Enshrining this program into legislation would provide greater certainty for the program and allow it to continue its important work well into the future. It would send a strong message about the importance of protecting the rights of Canadians, and it would demonstrate Parliament's shared commitment to ensuring that the rights and freedoms guaranteed by the charter and the Official Languages Act are respected and upheld.

(Motions deemed adopted, bill read the first time and printed)

PETITIONS

HEALTH

Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP): Mr. Speaker, I rise today to present a petition initiated by Ryan Hooey and the Canadian National Institute for the Blind on the importance of fully accessible insulin pumps for persons with diabetes.

Diabetes and sight loss are closely connected. Here in Canada, 25% of people with sight loss, one in four, have diabetic retinopathy. An estimated 750,000 Canadians live with this condition. Individuals living with sight loss and diabetes live independent lives but are unable to safely and independently use insulin pumps due to the lack of accessibility features.

That is why thousands of petitioners call upon the Government of Canada to ensure that Health Canada approval processes for new medical devices such as insulin pumps include an accessibility assessment, and to work with insulin pump manufacturers to address the safety concerns with the existing insulin pumps, expressed in the contraindications, and ensure that future contraindications are not considered for insulin pumps.

● (1540)

TAXATION

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Mr. Speaker, I am honoured today to stand in this place to present a petition signed by over 14,000 people from across the country.

Due to the fact that counselling therapy and psychotherapy have long been extremely beneficial tools for those seeking mental health supports, and that registered therapists and psychotherapists in Canada are required to charge GST and HST, while other service providers are exempt from charging this tax, the petitioners are calling on the government to remove that unfair GST/HST requirement for all counselling therapists and psychotherapists.

I have a private member's bill, Bill C-218, that would actually do just that.

The signatories of this petition are calling on the government to make these changes in a budgetary bill so that they will not be charged GST.

IRAN

Mr. Mark Gerretsen (Kingston and the Islands, Lib.): Madam Speaker, I rise today to present a petition on behalf of 5,381 signatories, who call to the attention of the government the atrocities that are happening in Iran.

Specifically, they are calling on the government to declare the entire Islamic Revolutionary Guard Corps a terrorist entity. They are asking for the government to designate authorities to investigate reported threats and stalking by the IRGC against Iranian Canadians and their third party agents. They are further asking the government to create legislation to revoke visas of Iranian officials and their families living in Canada who have embezzled billions of dollars into Canada through business fronts and properties.

They are asking for Canada's allies to end all negotiations with Iran and to provide continuous support to Iranians fighting for regime change by opening discussion between world leaders and the Iranian people to support the transition to a secular, democratic Iran.

THE ENVIRONMENT

Mr. Don Davies (Vancouver Kingsway, NDP): Madam Speaker, I rise to introduce a petition signed by many constituents in the Lower Mainland of British Columbia, who point out that Canada has signed the 2030 Nature Compact, which commits us to halt and reverse biodiversity loss by 2030.

They point out that the Fraser delta is recognized as a Ramsar wetland of international importance, a western hemisphere shorebird reserve network site and part of the southwest B.C. priority area. They point out that researchers have published peer-reviewed studies warning of extensive habitat loss and risk of ecological collapse on the Fraser River delta. Finally, they note that Environment and Climate Change Canada experts have warned of unmitigable and irreversible species-level risk to western sandpipers and shorebirds should the Roberts Bank terminal 2 project proceed as designed.

The petitioners are calling on the government to halt any further work on the proposed Roberts Bank terminal 2 project until a regional assessment of the cumulative impacts, environmentally, socially, culturally and economically, is complete to preserve this remarkable habitat.

* * *

QUESTIONS PASSED AS ORDERS FOR RETURNS

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, if the revised response to Question No. 1134, originally tabled on January 30, could be made an order for return, this return would be tabled immediately.

The Assistant Deputy Speaker (Mrs. Alexandra Mendès): Is that agreed?

Some hon. members: Agreed.

[*Text*]

Question No. 1134—**Mr. Blake Desjarlais**:

> With regard to government policies on funding directed towards First Nations, Inuit and Métis people, broken down by department since fiscal year 2015-16: (a) what policies, processes, and protocols exist to validate claims of Indigenous ancestry or Indigenous community; (b) what reviews or audits have been conducted to ensure that government funding has not been delivered to individuals, organizations, or companies that falsely claim an Indigenous identity; (c) is the government aware of any funding that has been allocated to individuals, organizations, or companies that falsely claimed an Indigenous identity; and (d) for each funding allocation in (c), how much funding has been recalled on the basis of false claims of Indigenous identity?

(Return tabled)

[*English*]

Mr. Kevin Lamoureux: Madam Speaker, I would ask that all questions be allowed to stand at this time.

The Assistant Deputy Speaker (Mrs. Alexandra Mendès): Is that agreed?

Some hon. members: Agreed.

GOVERNMENT ORDERS

[*English*]

TELECOMMUNICATIONS ACT

The House resumed consideration of the motion that Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, be read the second time and referred to a committee.

Mr. Kyle Seeback (Dufferin—Caledon, CPC): Madam Speaker, it took eight long years for the Liberal government to recognize that cybersecurity threats exist in this country and around the world. Congratulations to them for coming to the party a little late.

The Liberals have now presented a bill to try to address issues of cybersecurity in the country. As I said, it took them eight years to get there, but I have to say I am pleased that the Liberals have decided to finally do something. I look forward to this bill being passed so that it can be extensively studied at committee.

There are some things in this bill that are good. I know praising the Liberal government is strange territory for me, but I will say that the bill would give the government some tools to respond quickly to cyber-threats. There is currently no explicit legislative authority in the Telecommunications Act to ensure that telecom providers are suitably prepared for cyber-attacks. This is a good reason why this bill should probably move forward to committee to be studied.

The challenge I have, though, includes a whole number of things. My issue with the government is trust. While I do want this legislation to go to committee, I have extraordinary concerns about this bill. Many of these concerns have been raised by many groups across the country, and I do want to speak to some of those in the probably somewhat whimsical hope that the government will listen and take some of these amendments seriously.

There has been a very bad track record of the government responding to concerns from the opposition or from outside organizations with respect to legislation. There is a view that the Liberals are going to do what they want to do on pieces of legislation and that they really do not care what other people have to say. I am very concerned that the government is not going to listen to the very serious concerns that have been raised about this bill.

I have my own concerns when I look at how the government has behaved with respect to other pieces of legislation. We have to look at Bill C-11. There has been a multitude of organizations that have said the bill needs further amendment. Margaret Atwood has said that she has grave concerns about the legislation, that she supports the intent but has grave concerns about the implementation and how it is going to affect artists and content creators. We have had folks who compete in the YouTube sphere who have raised all kinds of concerns about Bill C-11, and the government's response has been that it does not care what they have to say, and that it is going forward with the legislation as it is.

The Senate has made a number of amendments to Bill C-11. I suspect the government's attitude is going to be the same, which is that it does not care what the amendments are and that it is going to proceed with the bill as it sees fit.

We also have only to look to Bill C-21 as well. We had the minister clearly not aware of what constituted a hunting rifle and a hunting gun. The Liberals introduced amendments at committee, and it took extraordinary push-back from Canadians from coast to coast to coast to get them to wake up and withdraw those amendments that they had put in at the last minute.

What it speaks to is that, despite having at its disposal the entire apparatus of the Canadian government, the Liberals are still unable to get legislation right. It takes an enormous amount of effort and hue and cry across the country saying that this has to stop and that this has to be changed. If there is not a massive uprising, the government tends not to listen to the legitimate concerns of other constituents or other groups when it introduces legislation.

With that context, it is why I have real concerns that the government is not going to listen to some of the serious concerns that have been raised with respect to Bill C-26. I am going to go through some of those.

The Canadian Civil Liberties Association has some very serious concerns. It has issued a joint letter that says that the bill is deeply problematic and needs fixing, because it risks undermining our privacy rights and the principles of accountable governance and judicial due process. This is a big bell that is going off, and I hope the government is listening. As I have said, I do not have a lot of faith, given other pieces of legislation where thoughtful amendments have been put forward and the government decided not to do anything with them.

● (1545)

I want to enumerate a few of the concerns from the Canadian Civil Liberties Association. On increased surveillance, it says that the bill would allow the federal government “to secretly order telecom providers” to “do anything or refrain from doing anything necessary...to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption”.

That is a pretty broad power. Where is the government putting the guardrails in that would limit the effects of this or protect the privacy rights of Canadians? That is something I think is incredibly concerning.

On the termination of essential services, Bill C-26 would allow the government to bar a person or a company from being able to receive specific services and bar any company from offering these services to others by secret government order.

Where are we going to have the checks and safety checks on this? Unfortunately, I am not in a position where I think I can trust the government to do the right thing on these things. We have seen it through vaccine mandates, in the legislation on Bill C-21 and in how the Liberals are trying to push through Bill C-11 without listening to reasoned amendments. If reasonable concerns are raised about Bill C-26, I just do not have faith the Liberals are going to take those concerns seriously and make the amendments that are necessary. I really hope they do.

On undermining privacy, the bill would provide for the collection of data from designated operators, which would potentially allow the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations. When someone takes the de-identified personal information of Canadians and does not say how they are going to deal with it or what protections they have in place to make sure it is not misused, what happens in the event that they take that information and somehow there is a government breach? Where does that information go? These are things I think we should be extraordinarily concerned about.

There was also an analysis provided with respect to this by Christopher Parsons, in a report subtitled "A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act". Parsons raises concerns about vague language. The report notes that key terms in the bill, such as "interference", "manipulation" and "disruption", which trigger the government's ability to make orders binding on telecom service providers, are unidentified.

Where are the guardrails in the legislation to prevent government overreach and therefore protect Canadians? This is something that I think all Canadians should be watching and be very concerned about. They should be letting their voices be heard by the government on this.

The report talks about how the minister of industry's scope of power to make orders is also undefined. We would be giving a whole host of undefined powers to the minister and the government that would allow them to have all kinds of sensitive information. These are things that may be necessary, but I do not know. They are highly concerning to me. They should be highly concerning to Canadians, and I hope the government will hear from real experts at committee.

Let us not have a two-day committee study where we think Bill C-26 is perfect as it is and bring it back to the House of Commons, bring in time allocation or closure and pass it through. We have seen that story before, and we do not want to see it with the piece of legislation before us. My really big hope is that the government is going to take the time to really consider the seriousness and breadth of Bill C-26 and make sure we have the ways to protect Canadians.

I just want to add that the Business Council of Canada has released its own letter to the Minister of Public Safety, expressing its incredibly deep concerns with respect to the bill: there is a lack of a risk-based approach, information sharing is one-way and the legal threshold for issuing directions is too low.

There are three reports, right there, that are outlining significant concerns with Bill C-26, and I, for one, just do not believe the government is going to listen or get it right. It does not have the track record of doing so, but I am hoping it will, because cybersecurity is incredibly serious as we move toward a digital economy in so many ways. I really hope the government is going to listen to these things, take them seriously, do the hard work at committee and bring forward whatever amendments need to be brought forward, or, if the amendments are brought forward by the opposition, listen to and implement those amendments.

● (1550)

Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP): Madam Speaker, the NDP sees the growing threat of cybersecurity, and we also see that Canada is far behind. However, we have concerns about transparency, and I know that the NDP member for Cowichan—Malahat—Langford has been instrumental in strengthening and making bills that the Liberals have brought to the floor more appropriate, so I have more than enough confidence that the NDP will ensure Canadians get the transparency and protection they believe in.

My question for the member is whether he could speak to the point that the government legislation before us would allow for a complete exemption from the Statutory Instruments Act. That would mean such orders could not be reviewed by Parliament through the scrutiny of the regulations committee. I wonder if I could get some comments on that.

Mr. Kyle Seeback: Madam Speaker, I would just add that to the list of things I am concerned about with this particular piece of legislation. I am glad and encouraged that the member has stated that New Democrats are going to try to strengthen this piece of legislation. I hope they do that. They talk about wanting transparency and I hope they are going to work really hard for transparency on this.

Conservatives would love to see transparency at a different committee, where we are trying to get someone to come and testify. Maybe the New Democrats can bring their love for transparency to that other committee and we can have PMO officials testify there.

● (1555)

Mr. Randy Hoback (Prince Albert, CPC): Madam Speaker, one of the things I have heard in talking to universities and different groups is that one of the faults of this piece of legislation is that they have to share this information with the government when they have been attacked, but it is a one-way street. When they see an attack happen, they share it with the government, but there is no information given to other businesses to help them protect against attacks similar to that in nature.

Could the member talk about why it is important and what it means to companies when they are attacked and how it can hurt not only their bottom line? Indigo, for instance, would be a good example of what happens when there is a cybersecurity attack.

Mr. Kyle Seeback: Madam Speaker, everyone here knows how serious cyber-attacks are. I often get a notification from Google that says it believes one of my passwords was exposed in a hack of some other organization and that I should take steps to make sure the password is not used in any other applications. We know that the threat of cyber-attacks exists and we know the damage caused.

What I go back to is that we know we need to do something, and I am glad that the government is doing it. It has taken it eight years, but it is finally here trying to deal with this issue. What it has to do is make sure that every voice on this is heard, whether it is industry saying it needs some information back, or whether it is others saying the threshold for some of these things is too low or asking what guardrails are put in place on some of the things.

The government has a lot of work to do and I hope it is willing to do it at committee.

Mr. Don Davies (Vancouver Kingsway, NDP): Madam Speaker, I think everybody in the House agrees that we need to up our game in this country to protect Canadians and our society from cyber-attacks.

My specific question has to do with certain specific vulnerable groups. I am thinking of young people, particularly teenagers between the ages, say, of 13 and 19. Even more particularly I am thinking of young girls and women who may be subject to all sorts of cyber-bullying and other offences, as well as seniors who can be victims of cyber-fraud.

I am wondering if my hon. colleague has any thoughts as to how Bill C-26 might impact those particularly vulnerable groups and what suggestions he may have legislatively to help protect them.

Mr. Kyle Seeback: Madam Speaker, that is a pretty tough question to answer in about two minutes.

As the father of a 16-year-old daughter, I am constantly worried about what is going on in the cybersphere for her, whether or not there is an instance of bullying going on. There have certainly been episodes of bullying in her real life. I know that at one point she was eating her lunch in the bathroom because she was being bullied by some folks. Online harassment and bullying are serious problems. I do not know enough about this particular piece of legislation to know if it would actually deal with that, but if not, I really hope that it would.

We have a lot of work do for seniors who are vulnerable to these things. This is something the government has to take on. Whether or not it is just waking up to it now as part of this bill, we need to educate seniors. I host events like this with seniors, where we let them know about the threats of cybersecurity and other things. The government needs to pick up the ball on that a little more as well.

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

This legislation consists of two separate parts. The first portion, among other things, would give the Governor in Council powers to order telecommunications providers to secure their systems against threats and to remove malicious actors from our telecommunications infrastructure. The second portion would create the critical cyber systems protection act, which would establish a cybersecurity compliance framework for federally regulated critical infrastructure operators. This would specifically regulate the sectors of finance, telecommunications, energy and transportation.

I believe that in principle, this legislation appears promising. I think we can all agree that we need a robust cybersecurity framework in Canada. However, it is worth noting that under the current government, we have done the least to bolster our resilience to cyber-attacks compared to all other Five Eyes partners. We lag behind our western allies in national security, and as such, Canada has failed to secure our critical infrastructure against complex and ever-evolving cyber-threats in the modern world. Therefore, before I get into the specific merits and deficiencies of this legislation, I want to speak about the emerging threats to our critical infrastructure and the pressing need to protect our national security.

Threats to our critical infrastructure are real and imminent. In fact, Caroline Xavier, chief of the Communications Security Establishment, or CSE, recently testified before the public safety and national security committee and stated, “cybercrime is the most prevalent and most pervasive threat to Canadians and Canadian businesses.” She also noted, “Critical infrastructure operators and large enterprises are some of the most lucrative targets.”

While there are several forms of cyber-attacks that our critical infrastructure operators are vulnerable to, the Canadian Centre for Cyber Security has noted in its most recent annual national cyber-threat assessment that ransomware is the most disruptive form of cybercrime facing Canadians and that critical infrastructure operators are more likely to pay ransoms to cybercriminals to avoid disruption. For example, in 2018, cybercriminals deployed a malicious software and successfully held the city hall of a municipal government in Ontario hostage, which resulted in that government paying $35,000 to the hackers to avoid disruption. However, this is not always an effective strategy. A survey of Canadian businesses found that only 42% of organizations that paid ransoms to cybercriminals had their data completely restored.

In 2021, the CSE stated that it was informed of 304 ransomware incidents against Canadian victims, with over half of them in critical infrastructure. However, it acknowledged that cyber-incidents are significantly under-reported, and the true number of victims is much higher.

The enormous economic toll that these cyber-breaches have on Canadian companies is worth noting. According to IBM, in 2022, the average cost of a data breach, which includes but is not limited to ransomware, to Canadian firms was $7 million. There is currently no framework to ensure that companies report when they are victims of these attacks. I will acknowledge that the legislation before us takes steps to address this pervasive issue that Canadians are facing; however, it is certainly an overdue effort.

We saw the damage a cyber-attack of this magnitude can cause in May 2021, when a U.S. energy company was subject to a ransomware attack carried out by a Russian-based criminal group that successfully extorted roughly $4.3 million in coin-based currency. As members may remember, this attack disrupted the largest fuel line in the U.S. for five days and led to President Biden calling a national state of emergency. In 2021, at the U.S. Senate committee on homeland security, the CEO of that company testified that he had no emergency preparedness plan in place that specifically mentioned "ransom or action to ransom". This incident underscores the fact that we as a country must enhance preparedness and improve the resiliency of our critical infrastructure in order to avoid similar incidents.

Therefore, I am pleased to see this proposed legislation come forward. However, it is worth noting that this is the first substantive legislative response to this issue during the government's tenure, despite a steady increase in cyber-threats over the years.

● (1600)

The entirety of our federally regulated critical infrastructure is connected to the Internet in some way, and it is extremely important to prevent malicious actors from setting up on our infrastructure and attacking it. Previously, there has been no mechanism for the government to formally remove a company from our telecommunications networks.

The clearest example of the need for this mechanism would be the controversy surrounding Huawei, a company that was part of the design of our 5G networks despite glaring national security concerns related to its activities and relationship to the Communist Party in Beijing. It is a significant move that this company will be kicked off our servers, but it is a delayed one. We know that under China's national intelligence law, the CCP has the authority to instruct any company to hand over information to support, assist and co-operate with state intelligence work. Accordingly, we ought to be cautious and avoid contracting with companies that could potentially compromise the security of our critical infrastructure.

It is certainly positive that Canada will be able to kick malicious actors such as Huawei off our networks. However, many have noted that we lessened our credibility among the Five Eyes nations due to our delayed response to this issue. Indeed, the United States lobbied Canada for years to exclude Huawei from our 5G mobile networks and warned that it would reconsider intelligence sharing with any countries that use Huawei equipment.

In some respects, this legislation is a positive step toward establishing a baseline standard of care for organizations whose functions are integral to our critical infrastructure. As I have previously mentioned, incidents of cyber-attacks often go unreported or underreported. This legislation's mandatory reporting mechanism, which specifies that a designated operator must immediately report an incident to the CSE and the appropriate regulator, is a welcome step toward addressing this issue. However, the act does not prescribe any timeline or give any other information as to how "immediately" should be interpreted by an operator.

As I have just laid out, there are aspects of this legislation that my Conservative colleagues and I fully support. However, I have concerns with several elements of the bill.

First and foremost, there is a complete lack of oversight over the sweeping new powers afforded to the cabinet ministers, regulators and government agencies mentioned in this legislation. Alongside a lack of oversight, there is little information on the breadth of what the government might order a telecommunications operator to do.

It is evident that this bill draws on much of Australia's legislative model, which was first introduced in 2018 and eventually amended. However, we did not follow suit in terms of the oversight measures Australia included in its critical infrastructure protection act. Notably, Australia introduced political accountability mechanisms alongside its legislation, including a requirement for regular reporting, an independent review and the production of a written report. The Conservatives would like to see annual reporting from the minister on what actions have been taken and a public disclosure of the orders that the government is making under these newly afforded powers.

In terms of concerns from the public, we have heard from a number of organizations that are concerned that elements of this legislation undermine the privacy rights of Canadians. In September of last year, several privacy rights organizations signed an open letter to the Minister of Public Safety, which laid out their concerns with Bill C-26. For example, they were concerned about the sweeping new powers this legislation would give to the government over access to the personal data of Canadians and the data of companies. They noted that Bill C-26 "may enable the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations."

I think we can all agree that while enacting measures to improve the resilience of our critical infrastructure is of the utmost importance, civil liberties and privacy must be fully respected when drafting those measures. On the other hand, we have heard from stakeholders who are concerned about the regulatory burden this legislation may have on businesses, especially small and medium enterprises.

Many stakeholders have noted that the high costs and business impacts of a cyber-incident already incentivize companies to ensure rigorous cybersecurity protocols. Recent statistics released by Statistics Canada found that in 2021, Canadian businesses spent over $10 billion on cybersecurity, a 41% increase compared to 2019. Many stakeholders have noted that the proposed penalties related to this act, which reach up to $15 million and five years of jail time, are touted as being intended to promote compliance rather than to punish. However, I think we can all agree that a $15-million fine would indeed be unduly punitive on a small business that may be subject to this act. Therefore, we must ensure that fines and compliance costs are distributed evenly so as not to stifle competition and endanger the viability of small and medium enterprises in our critical infrastructure sectors.

Finally, we face a problem related to definitions and the scope of this bill. Various terms are not defined, including what constitutes a cyber-incident, and it is not immediately clear how the government will determine who is subject to this legislation. I look forward to receiving an explanation from the government to demystify some of the vague language found within it.

● (1605)

To conclude, a threat to our critical infrastructure is a threat to our national security. I think all parties agree that the government must take strong and immediate action against cyber-attacks. We support this bill in principle, but we believe that it needs to be amended significantly to ensure greater transparency and accountability from the government and future governments. I look forward to studying and amending this bill at the public safety committee with my colleagues across all parties.

Mr. Don Davies (Vancouver Kingsway, NDP): Madam Speaker, like my colleague, I think we are broadly supportive of the aims and principles of this bill but have some significant concerns about many of the details. This includes that the bill would open the door to new surveillance obligations; would allow the termination of essential services, perhaps without due process; may undermine privacy; lacks guardrails to constrain abuse; and has some relatively disturbing secrecy provisions that would obviate the minister from having to be accountable to Parliament by publishing the measures he takes.

Among the many concerns expressed about the bill, which ones does the member find the most troubling that he would like addressed at the committee stage?

● (1610)

Mr. Doug Shipley: Madam Speaker, all of those are legitimate concerns that we will be addressing at the public safety committee if and when this bill gets there. I do not know if I can rank them today, because I think they are all significant. Everybody has different issues that come to mind based on what is most important to them. Obviously, privacy is one of the most important things to people.

What I mentioned in my speech was the ability for companies to still manage themselves once these fines have been imposed. We do not want to put out of business the small and medium-sized companies that have already had cyber-attacks, and then give a fine on top of that.

There are many things we need to address in committee. I am looking forward to studying the bill with my colleagues from all sides when it gets there.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Madam Speaker, there has been a lot of talk about TikTok and the fact that it could be used as a tool for interference. In fact, I closed my account at that time and, like everyone else, removed the app from my device.

What does my colleague think about apps like WeChat, which are known to be spying platforms? What does he think about the fact that a G7 parliament, like Canada's, has been using Zoom for years, a Chinese app that once interrupted a live meeting of Chinese dissidents? It is disturbing, to say the least.

[*English*]

Mr. Doug Shipley: Madam Speaker, to be quite candid, I have two teenage boys who are always kidding that I am a bit of a dinosaur when it comes to different social media platforms. I have never had TikTok. I do not know much about it, but I understand there have been a lot of issues with it. I think with all of our social media platforms, we need to stop, review them and look at who is taking information from them, because a lot of information can be gleaned from them.

We jumped into this new media method many years ago without knowing the direction and road it was going to take. Now that we are well down it, I think it is time we looked at all these different platforms and realized what information is being taken from them.

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): Madam Speaker, it is with great pleasure that I rise to discuss Bill C-26, an act respecting cybersecurity. I will be addressing elements of the legislation that deal with securing Canada's telecommunications system.

As Canadians rely more and more on digital communication, it is critical that our telecommunications system is secure. Let me assure the House that the Government of Canada takes the security of that system seriously. That is why we conducted a review of 5G technology and the associated security and economic considerations. It is clear that 5G technology holds lots of promise for Canadians: advanced telemedicine, connected and autonomous vehicles, smart cities, clean energy, precision agriculture, smart mining, and lots more.

However, our security review also made it clear that 5G technology will introduce new security concerns that malicious actors could exploit. Hostile actors have long sought and will continue to seek to exploit vulnerabilities in our telecommunications system. The Canadian Security Intelligence Service recognized this in its most recent public annual report. The report said, “Canada remains a target for malicious cyber-enabled espionage, sabotage, foreign influence, and terrorism related activities, which pose significant threats to Canada’s national security, its interests and its economic stability.”

The report said that cyber-actors conduct malicious activities to advance their political, economic, military, security and ideological interests. These actors seek to compromise government and private sector computer systems by manipulating their users or exploiting security vulnerabilities. The CSIS report also highlighted the increasing cyber-threat that ransomware poses.

The Communications Security Establishment has similarly raised concerns about threats like ransomware in recent public threat assessments. We have seen how such attacks by criminal actors threaten to publish victims' data or block access to it unless a ransom is paid. It is not just cybercriminals doing this. CSIS has warned that state actors are increasingly using these tactics, often through proxies, to advance their objectives and evade attribution.

To be sure, Canadians, industry and government have worked hard to this point to defend our telecom system, but we must always be alert and always be guarding against the next attacks. This has become more important as people are now often working remotely from home office environments, and the challenges are accentuated by the 5G technology. In 5G systems, sensitive functions will become increasingly decentralized to be able to be faster where speed is needed. We all recognize cell towers in our communities and along our highways, and 5G networks will add a multitude of smaller access points in order to increase speeds. The devices the 5G network will connect to will also grow exponentially. Given the greater interconnectedness and interdependence of 5G networks, a breach in this environment could have a more significant impact on the safety of Canadians than with the older technology. Bad actors could have more of an impact on our critical infrastructure than before.

The security review we conducted found that, for Canada to reap the benefits of 5G, the government needs to be properly equipped to promote the security of the telecommunications system. We need to be able to adapt to the changing technology and the threat environment.

Now, for these reasons, we are proposing amendments to the Telecommunications Act. The amendments would ensure that the security of our telecommunications system remains an overriding objective. This bill would add to the list of objectives set out in section 7 of the Telecommunications Act. It would add the words “to promote the security of the Canadian telecommunications system.” It is important to have these words specified in law. It would mean that the government would be able to exercise its power under the legislation for the purposes of securing Canada's telecommunications system.

● (1615)

The amendments also include authorities to prohibit Canadian telecommunication service providers from providing and using products and services from high-risk suppliers in 5G and 4G networks if deemed necessary after consultation with the telecommunications providers and other stakeholders. They would also give the government the authority to require telecommunications service providers to take any other actions to promote the security of the telecom networks, upon which all critical infrastructures depend.

We have listened to our security experts, Canadians and our allies, and we are following the right path. We will ensure that our networks and our economy are kept secure. A safe and secure cyberspace is important for Canadian competitiveness, economic stability and long-term prosperity.

It is clear that the telecommunications infrastructure has become increasingly essential, and it must be secure and resilient. Telecommunications present an economic opportunity, one that grows our economy and creates jobs.

The amendments to the Telecommunications Act accompany the proposed critical cyber systems protection act. This bill will improve designated organizations' ability to prepare, prevent, respond to and recover from all types of cyber incidents, including ransomware. It will designate telecommunications as a vital service.

Together, this legislative package will strengthen our ability to defend telecommunications and other critical sectors, such as finance, energy and transportation, that Canadians rely on every single day.

The legislation before us today fits with the Government of Canada's telecommunications reliability agenda. Under this agenda, we intend to promote robust networks and systems, strengthen accountability and coordinated planning and preparedness.

Canadians depend on telecommunications services in all aspects of their lives, and the security and reliability of the network has never been more crucial. They are fundamental to the safety, prosperity and well-being of Canadians.

We will work tirelessly to keep Canadians safe and able to communicate securely. This legislation is an important tool to enable us to do that.

● (1620)

[*Translation*]

Ms. Andréanne Larouche (Shefford, BQ): Madam Speaker, I thank my colleague for his speech. In January, I requested a meeting with the Université de Sherbrooke, which has a research chair in cybercrime. I learned a lot about how behind the times Canada is.

This bill is good, but it comes at a time when we are at greater risk than ever before. The federal government does not seem to be taking cybercrime seriously, yet many European countries have other models and have made headway against cybercrime. How can we address the fact that we need to catch up?

We have to act faster to protect ourselves from cyber-attacks. There is also the whole issue of Hydro-Québec and the fact that those are interprovincial lines. How are the authorities going to be able to manage all that given the agreements and the importance of respecting Quebec's and the provinces' jurisdiction over certain types of critical infrastructure?

It is high time this critical infrastructure was included in a bill to protect it. I would like to hear my colleague's thoughts on that.

[*English*]

Mr. Tony Van Bynen: Madam Speaker, I share the member's sense of urgency in making sure that we advance opportunities to make the networks safer. The technology has developed very quickly in recent years, so it is important that we stay ahead of that technology.

On the relationship between the provinces and the federal government, I think it is important that we develop reliable agreements where appropriate, but telecommunications is the responsibility of the federal government, and we are not going to shirk from our responsibilities in making sure that the network is safe for our citizens.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Madam Speaker, I too reiterate the thoughts of my Bloc colleague that we are quite behind in this with respect to what other countries are doing.

However, my concern has to do with the broad scope of powers being granted to the minister in this bill. It was specifically written so that some of these orders were not published in the Gazette, so I would really love to hear from the hon. member why the bill was crafted specifically to keep that public piece of information out.

Mr. Tony Van Bynen: Madam Speaker, we all realize how important security is. In some cases, it may be necessary to act without making the information available so that the perpetrators of fraud against the cyber-network understand what is being accomplished. There are situations where information needs to be maintained securely. A responsible government will do so on the basis of being accountable and transparent to the extent that is appropriate, and I believe the government will do that.

Mr. Alex Ruff (Bruce—Grey—Owen Sound, CPC): Madam Speaker, I will build on that last question a bit because I think the member took it out context, though I may be wrong.

The question is around specific cyber-incidents or transgressions that need to be dealt with by the appropriate authorities. The issue is the legislation itself and how the power would be used by our security establishments. One of the criticisms that needs to be fleshed out at committee is how this bill and the legislation get reported back here to the House of Commons and to Canadians.

Would the member agree that it would be an important addition or amendment to the legislation to include the requirement for an annual report back to Parliament on how this legislation is progressing and what key changes our national security organizations have made so that Canadians can understand how their lives are being impacted in the cyber-realm?

Mr. Tony Van Bynen: Madam Speaker, I believe that transparency, to the extent that is possible without jeopardizing security, is important. Committees will contribute a significant amount of improvements, and the government will listen to reasonable solutions, amendments and additions to protect the safety of Canadians. That is a value that we all share.

Mr. Mike Morrice (Kitchener Centre, GP): Madam Speaker, I want to continue the line of questioning of other members on balancing the need to address cybersecurity and privacy at the same time.

One group that has shared some concerns is the Citizen Lab. It has put together a report called “Cybersecurity Will Not Thrive in Darkness” and has offered 30 recommendations for the governing party to consider at committee.

I wonder if the member has seen this report and if there are any recommendations in the report that he sees worthy of going ahead with. He may not see them all as worthy of going ahead with, but are there some recommendations that he thinks we should pursue?

● (1625)

Mr. Tony Van Bynen: Madam Speaker, no, I have not seen those recommendations, but it would be appropriate for those recommendations to be presented to the committee for consideration.

Mr. Marty Morantz (Charleswood—St. James—Assiniboia—Headingley, CPC): Madam Speaker, six years ago Statistics Canada found that more than one-fifth of all Canadian businesses were impacted by cybersecurity incidents, a sobering statistic in its own right. That was six years ago.

What we need to understand is that cyber-technology moves at a mile a minute. What is groundbreaking one year can become ordinary or obsolete even just a year later. I do not doubt that cyber-defence systems in Canada, both by the government and by private businesses, have become much more sophisticated throughout the last several years, but the technology used for cyber-attacks, whether by foreign or by domestic actors, has developed even more quickly.

We are seeing this play out in real time. Just a month ago, Indigo fell victim to a ransomware attack. Online purchases became impossible. In-store purchases could still happen, but only if one was carrying cash. Most alarming of all, information about the chain's employees was accessed. The situation continues to drag on, Canada's largest bookstore chain held for ransom. The emergency that Indigo finds itself in is terrible, but back in January the Russia-tied group that carried out this attack, LockBit, did something far more cruel when it hacked the SickKids Hospital in Toronto.

Those are just two examples of how cyberwarfare transpires in Canada, amongst thousands of other examples every single year. Today, particularly at a time when we know foreign powers are actively seeking to undermine Canada, its institutions and its critical infrastructure, it is time for the government to step in and put forward a cybersecurity strategy. It almost goes without saying that in this digital age, online systems run just about everything that keeps this nation up and running, including hospitals, banking and the energy that heats our homes.

What the government has failed to realize until now is that as these systems become more digitized, so too do they become more vulnerable. This was on full display when SickKids was hacked. Lab results, imaging results and the hospital's phone lines were wiped out for days before order was finally restored. Just in 2020, CRA was hacked, compromising the accounts of 13,000 Canadians. Bold action is what is needed to fight against attacks of that scale, and it is Parliament's job to provide that action.

When I look at a bill like Bill C-26, I start by thinking about what it would let the government do and whether that would be an improvement on our existing cybersecurity regime. In that regard, there is actually a lot to like here. Now more than ever, cyber-attacks can take place in little more than the blink of an eye. An attacker could dig its claws into a company's online system, inflict all the damage it wants, take all the information it wants, and it might be hours later than the affected company realizes what it is being done to it.

Having a rapid response to those incidents is absolutely critical. It is clear to me that the type of broad, sweeping powers contained in this bill would allow the government to provide that rapid response. It would also bring some much-needed cohesion to the link between the state and telecom providers. Right now, telecoms can decide to work with the government and prepare for a cyber-attack, but this is entirely voluntary. They can share information with the government, but only if they really feel like it.

As far as having a unified cybersecurity strategy goes, ours is laughable. It is about time that we act accordingly and fall in line with our Five Eyes allies. This bill covers such an important policy area, yet in so many ways it just does not get it right. It is another page in that long Liberal book entitled, “Having the right intention and making the wrong move”. I should not have to say this in a room full of parliamentarians, but here we are: the written text of a law actually matters.

A law needs to be clear. It needs direction. It needs guardrails. That is why it is so strange to come across a bill that lets a minister go up to a telecom provider and make them “do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system.” All the power goes to the minister with nothing in the way of guardrails constraining their power.

When I read this part of the bill, I was reminded of one of my favourite Abraham Lincoln quotes. Abraham Lincoln said, “Nearly all men can stand adversity, but if you want to test a man’s character, give him power.” That is what this section does, it provides immense power to the Minister of Industry, which is not abridged or protected in any way.

There is nothing wrong with a law that gives the government new powers, but in this case, with the cyber-threats that we are currently facing, that type of law is exactly what we need to get right now.

● (1630)

The problem here is that we are debating a bill today where those new powers are not specified and are not restricted whatsoever. Alongside the Canadian Civil Liberties Association, I am seriously concerned about the way that Bill C-26 would infringe on the privacy rights of Canadians.

This bill would allow the government to collect data from telecoms. With guardrails in place, this would actually make a lot of sense. The government might want to see the weak spots in a company's cybersecurity system, for example. With the government being able to get these companies to do anything, we do not have a clue what it will demand to collect.

As it stands now, there is no way of stopping them from collecting personal data and juggling it between various departments. Foreign affairs, defence, CSIS, anyone could take a look if the state decides that it is relevant.

At the minister's discretion, the data could even go to foreign governments. Again, this all comes back to the problem of unchecked power. With zero restraints in place, we can only assume the worst. Like so many bills under the Liberal government, what we are seeing here is a government-knows-best approach.

I am really not sure how it can defend this level of information sharing. “Well, yes, we could share one's personal information, but we definitely will not do that.”

It wants Canadians to give it the benefit of the doubt. The government is well past the point of being given the benefit of the doubt.

The Canadian Civil Liberties Association says that the bill is "deeply problematic and needs fixing", because "it risks undermining our privacy rights, and the principles of accountable governance and judicial due process".

A number of organizations and individuals have raised red flags. The Business Council of Canada wrote to the Minister of Public Safety, expressing the business community's concerns about Bill C-26, including the potential of brain drain, as the result of personal liability and unduly high monetary and criminal penalties.

The council also expressed concerns that information sharing is one-way. Operators are required to provide information to government but receive nothing back from government.

The bill misses the opportunity to implement an information-sharing regime that could benefit all operators subject to the law.

Aaron Shull, managing director of the Centre for International Governance Innovation said that Ottawa should deploy a wide range of strategies, including tax breaks to individual small businesses, to take cybersecurity more seriously.

The Munk School issued a report on Bill C-26 where they itemized a series of deficiencies including that "the breadth of what the government might order a telecommunications provider to do is not sufficiently bounded."

There are massive, glaring issues in Bill C-26.

What is so unfortunate about this is that I think that enhancing Canada's cybersecurity is something that all parties can get behind. I am willing to see this bill move forward but it is going to need some major amendments in committee, amendments that protect civil liberties and constrain abuse.

There needs to be a threshold test, providing that an order being given by the government is proportionate, reasonable and, above all else, necessary. The minister should have to table reports, annually perhaps. How many orders did they issue in a given year? What kinds of orders, broadly speaking?

If the government mishandles someone's personal information, which it likely will, this bill needs to make it clear that those people will be compensated.

We find ourselves debating another highly important, poorly crafted bill, courtesy of the Liberal government.

I want to see this bill go to committee so that experts, especially those with a focus on civil liberties, can help make this bill work.

To be clear, if the issues in this bill concerning privacy and impacts to businesses are not addressed, the Conservative Party is ready to pull its support immediately and put up a very strong defence to stop this bill from going beyond committee.

After all, if the Liberals cannot manage Canada's cybersecurity, they can just get out of the way and let Conservatives handle it.

● (1635)

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, I understand that the Conservative Party is going to actually be voting in favour of the legislation. I am glad to hear that because we recognize that it does not matter which political party one is of, the issue of cybersecurity is something that we all need to take seriously.

Listening to the debate today, Conservatives come up and say, yes, they support the bill and it is a bill that they want to see go to committee.

Given the member's comments, does the Conservative Party actually have any amendments that it is prepared to share, through the House of Commons, with Canadians? What tangible amendments would they like to see made to the legislation that he could share with us prior to it going to committee?

Mr. Marty Morantz: Madam Speaker, I want to thank my colleague from Winnipeg North. It is always nice to get a question from a fellow Winnipegger. I love the Prairie pragmatism of his question on what amendments might we put forward.

The purpose of my speech and the speeches we have heard from our side of the House today is to point out the flaws in the bill. We will support the bill to get to committee stage and it is at committee stage where we can have a fulsome discussion with the experts about these flaws and come up with serious, practical amendments that make this bill even stronger. I think my colleague from Winnipeg North would agree it is in everybody's interest to make this bill as strong as possible.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Madam Speaker, I thank my colleague for his riveting speech.

I would like to ask him what he thinks about the government's strategy on Huawei and 5G. It seems to me that there were a lot of about-faces, that it took a long time and that there was a lot of dilly-dallying.

I would like to hear my colleague's thoughts on that.

[*English*]

Mr. Marty Morantz: Madam Speaker, I do not have a lot of comfort that the government will get it right given how many years it dragged its feet on Huawei. I think we have every reason to be concerned that this bill might come out of committee without the necessary amendments.

One of the things I am particularly concerned about is the sentence I referred to from the bill that a minister can do or refrain from doing anything necessary to secure the Canadian telecommunication system. That statement needs to be measured against section 7 and 8 of the charter, which is the right to life, liberty and security of person and to be secure against unreasonable search and seizure.

We need to make sure that this bill can stand the scrutiny of the courts in case any business or individual affected by it decides to bring a charter challenge. I think there are serious concerns around the idea of giving a minister unfettered power, as one of my political heroes, Abraham Lincoln said, who I mentioned earlier in my speech.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Madam Speaker, just before the hon. member's speech, we heard from a Liberal member. One of the things the member spoke about in his speech was specifically that the government knows best and to just trust the government on this and we will be fine. That came out of one of the answers to a question I asked.

Can he expand on that in terms of the concern we have with the answers we are hearing today, and in terms of the transparency and accountability required in this bill?

Mr. Marty Morantz: Madam Speaker, there is every reason to think that the government will mess this up. For example, this morning, there was a story about the CBC taking the personal, private information of its employees and posting it online against their will and without their consent.

My colleagues across the way might say the CBC is an independent body, but the reality is the CBC is mandated as a Crown corporation under federal legislation and has to report to the Minister of Canadian Heritage on an annual basis. The government has some culpability in this. If we see the CBC messing this up, how can we trust the government to get it right?

Mr. Dan Albas (Central Okanagan—Similkameen—Nicola, CPC): Madam Speaker, it is a pleasure to rise on behalf of the good people of Central Okanagan—Similkameen—Nicola.

I welcome this debate because essentially what the government has put forward in the bill is two words: "Trust us". We should trust the government and give it all these powers for the Telecommunications Act, expanding it drastically. We should trust the government when it comes to designating cybersecurity systems as being of such importance that a whole host of new rules should be put upon them. That is what the government is asking us to do.

This is the same government that took years to answer the question of whether we will allow Huawei in our 5G infrastructure. It is a question that has infuriated our allies because they expect Canada to be a trustworthy party in the Five Eyes' intelligence and sharing. It has also infuriated the companies themselves, as many had hoped to utilize the technology. Now, I was against the use of Huawei, but these enterprises are in a competitive venture and will take any particular opportunity to compete and try to lower their prices. However, this government wasted years for that infrastructure to be procured. I believe this also infuriated many Canadians who wanted a simple yes or no on Huawei.

I think the government went through three public safety ministers who said that an answer was coming. Finally, it said no, answering Conservative calls for "no way to Huawei". However, now it has put forward a bill that would essentially give the power to the government. For example, the government would be able to bring forward an order that could not be reviewed by Parliament. In fact, the Statutory Instruments Act is being exempted from both the telecommunications component in Bill C-26 and the new cybersecurity part, the critical cyber systems protection act.

I am the co-chair of the Standing Joint Committee for the Scrutiny of Regulations, which is a committee tasked by the House and the other place to ensure that when the government creates an order or regulation, it does not exceed the authority granted to it by Parliament. We are able to make sure that when a department or ministry is charged with a delegated authority that it does so justly, and in light of the legislation, that it does not, ultra vires, exceed it.

However, in the legislation before us, the government is effectively saying that it gets to place secret orders that cannot be reviewed by Parliament. Now, members may say that they can go to a justice to be able to have a case heard in court. Again, who can be designated under this proposed bill is an open question. Someone could go in front of a justice, but guess what, Madam Speaker? The government reserves the right to actually make its accusations in a closed-door fashion where a person or company does not have to be there to defend themselves against the evidence that is brought to the court. There, a person or company may be subject to an order that is so secret that it cannot even be said within a closed hearing with an independent judge.

Now, some may say, "Well, so what? It is for national security." However, we actually do not know. There are so many different organizations that can make powers here. Everyone from the responsible minister to the appropriate regulator, the minister of foreign affairs, the minister of national defence, the chief of the defence staff, the chief or an employee of the Communications Security Establishment, the director or an employee of the Canadian Security Intelligence Service or any other person or entity that is prescribed in the regulations can exert power.

"Trust us", says the government. The government wants us to give it this power, and it will choose who can use it on whom; Parliament will never know anything about it. Even if a person or company protests, they will not be able to hear the evidence in court as to why they must comply.

● (1640)

Granted, I believe that, within Canada's interests, we should have the ability to work with providers around concerns, but I have great reservations on this. This bill says, "Trust us." The government says this repeatedly. When we ask questions about foreign interference or share concerns about Huawei, the answer is, "Trust us." This is not a respectful way to do it.

Let me tell everyone about a respectful way to do these things. Having brought forward a bill, it would perhaps be respectful to bring it to the committee stage first. There is a process where a committee can have hearings on potential legislation before it comes to this place for second reading. This offers the committee the flexibility to begin hearings and mould whether those powers are going to be broadly met in this House. In a minority setting, that would have been ideal.

However, that is the past; the government has brought forward this bill and we are at second reading. What would have been even better is to look at the example of Australia, which decided to hold a number of different inquiries over a period of years. I know the government is very sore around the subject of inquiries these days, but these commissions were set up and asked what information government should have, as well as how and with what kinds of regulations data should be regulated by government. Essentially, it took the approach that someone's personal data is their own, and they should be able to direct it.

Over a series of commissions, some with 800-page reports, they decided on a process for making changes. They would focus on privacy, deciding what the government could keep and could not keep, and they went through that legislative process. Then they said they were going to regulate industry by industry. We should notice that the proposed critical cyber systems protection act casts such a wide net that it could be anything from pipelines to sewage water treatment plants or air transit systems.

● (1645)

We do not know because the government just says to trust it. However, I know, and I am sure others know as well from experience, that every industry uses different technology. Therefore, a one-size-fits-all, big, bossy government, as the member for Carleton would probably call it, does not have the touchpoints or the understanding. All we know is that these orders can be placed on any industry at any time and that those orders will never be looked at by Parliament. To me, the government is asking for too much.

Again going to the Australian model, Australia said it was going to start with data privacy rights in telecommunications, energy systems and banking. It picked the industry that it was going to focus on and made sure it got it right before putting forward the new rules that allowed for a steady process. Instead of a holus-bolus process where everything gets thrown into Bill C-26 with the government telling Canadians, members of Parliament and members of the other place to just trust it, we could have had smart legislation that would be reviewed at committee. Hearings could be held, and we could find out what is reasonable for each industry and what is not. From a privacy standpoint, we could also ask what the government means when it designates someone under this act. Does it mean a person or a company? What are their rights and responsibilities? Unfortunately, this is all on the government side; it decides, saying, "Trust us."

My colleagues and I will be seeing this bill go to committee. However, I have to protest in this place that this is not the way to make our systems better and provide more trust in our institutions. "Trust us" is not an argument, and the government should know better by now.

● (1650)

Mr. Mark Gerretsen (Parliamentary Secretary to the Leader of the Government in the House of Commons (Senate), Lib.): Madam Speaker, I listened with great interest to the member. I heard him speak at length about why the bill is so horrible. He then concluded his speech by saying that he would vote in favour of sending it to committee. If it is so horrible, why would he bother to vote in favour of it? Why not just vote against it?

Mr. Dan Albas: Madam Speaker, Conservatives have been calling for the government to deal with the very real threat of foreign interference for years. This is not only a threat on the government side but also something that takes on other forms, such as cyber-espionage.

Not everything in this bill is terrible, but it could have been structured better. As the previous member from Winnipeg said, Conservatives on the committee will work to make the legislation better and ask qualifying questions. Moreover, we will pull support if the current government continues to stonewall and ask us to trust it without offering better arguments or better amendments.

[*Translation*]

Mr. Martin Champoux (Drummond, BQ): Madam Speaker, I commend my Conservative colleague for his speech.

We have heard concerns about the fact that legislating in this manner and governing essential cybersecurity infrastructure could have an impact on the freedom of expression of Quebeckers and Canadians.

I would like to ask my colleague whether he believes it is possible to implement such legislation so that we can regulate and govern essential cybersecurity infrastructure as needed while protecting freedom of expression. I would like to hear his thoughts on that.

[*English*]

Mr. Dan Albas: Madam Speaker, I do not have a precise answer to the member's question, but I do know that this is not it. The government has basically thrown everything to a one-sided argument. Industry has raised concerns with the government that there is no two-way communication. Industry can report to government, but there is no way to have any kind of forward guidance from the government in this legislation. Those one-way streets lead nowhere.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Madam Speaker, I appreciate the speech my colleague made. I think the track record here is one of the biggest points I took from his speech. Specifically, he referenced how the government delayed enforcing its decision on Huawei for years. This is not a new concern after eight years of the Liberals delaying and refusing to act or provide leadership while many of our global counterparts have done so.

Specifically, he emphasized the example of Huawei very well. Could he expand a little on how damaging the delay was to Canada's international reputation on cybersecurity?

Mr. Dan Albas: Madam Speaker, governments are made of people, and people make mistakes. After talking to many of our allies and seeing what our other Five Eyes partners in the United States, Great Britain, New Zealand and Australia have done, the government probably heard the feedback that it was a black eye that it took so long for Huawei to be banned from Canada's 5G infrastructure. This is now perhaps an overreaction to try to make up for that.

Let me say this. In this place, in this country, we want laws that are just, fair, and most of all, practicable. Unfortunately, this is a one-size-fits-all, big, bossy government that asks us to trust it because it knows the shots and will take them as it sees them. It has not done well in the past, and I believe that this overshoot is to respond to that lack of credibility with respect to Huawei. However, two wrongs do not make a right.

[*Translation*]

The Assistant Deputy Speaker (Mrs. Alexandra Mendès): Order.

It is my duty pursuant to Standing Order 38 to inform the House that the questions to be raised tonight at the time of adjournment are as follows: the hon. member for Victoria, Taxation; the hon. member for Stormont—Dundas—South Glengarry, Immigration, Refugees and Citizenship; the hon. member for Lanark—Frontenac—Kingston, Cannabis.

● (1655)

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Madam Speaker, today I will be talking about the bill we have been discussing for the past few hours, Bill C-26, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts.

From the outset, I would like to mention that in 2019, when I arrived in the House of Commons, the topic on everyone's lips was the data breach at Desjardins. To put things into context, at the time I was a member of the Standing Committee on Access to Information, Privacy and Ethics. I was determined to find out how we might protect privacy and decorrelate the social insurance number that we were using far too readily as a means of identification. My colleagues see where I am going with this.

It took a scandal for the government to do something about this. Now I am no longer a member of the Standing Committee on Access to Information, Privacy and Ethics, I am vice-chair of the Standing Committee on Procedure and House Affairs. Again, it took a scandal being uncovered by the media for the government to truly listen to us.

This is a case of being lax when it comes to the security of the electoral process and national security. I am addressing all those who are listening to us; I hear their concerns. For the past six months, the Standing Committee on Procedure and House Affairs has been looking into Chinese interference in our electoral process. It is likely that there will be an announcement in the near future that will once again demonstrate that we really need to sound the alarm to get things moving. Of course, the Bloc Québécois will always be vigilant. The Bloc Québécois will be there every time it is important to get to the bottom of various allegations or scandals. We will force the government to take action for our constituents, because they deserve it.

In light of all that, it goes without saying that Bill C-26 is a step in the right direction. The bill introduced by the Minister of Public Safety aims to strengthen the security of Canada's telecommunications system. That said, I want to be honest. I have serious concerns. Over the past few years, my confidence in the government on security issues has been eroded. The government must not stick its head in the sand. Quebeckers need assurances. They need to be assured that this paternalistic and so-called well-intentioned government is doing its job, particularly in its areas of jurisdiction. That is all we ask and all we expect.

We know that China, Iran and Russia can be considered hostile powers that do not wish us well. When someone does not wish us well, we have to protect ourselves. The government absolutely has to come up with systems to guard against what we have seen since the latest scandals. We demand an explanation, and answers are to be expected, yet the government says everything will be fine and we should move on to other things. Unfortunately, our constituents feel betrayed and lack confidence in this government because it is not taking things seriously, as all the numbers indicate.

Regarding what is going on with Beijing specifically, I wonder if there is something we do not know. Why are we taking action so late in the game? Why are we always reacting? I am fed up with all this dissatisfaction. Every time I go back to my riding, my constituents want to talk to me about this, and I get why they are feeling discouraged.

● (1700)

As members know, I will be going to the United Kingdom. We are going to be taking a look at the procedures in different Commonwealth countries so we can implement other countries' best practices with respect to national defence and protection against interference in our elections.

I know that when having discussions with my colleagues, I am going to have to tell them that the process is ongoing even though the British and the Australians understand the situation and have taken action. The Americans, too, understand and are taking action. I am wondering if our closest allies, our Five Eyes partners, still have confidence in us.

For quite some time, the Bloc Québécois maintained that the government needed to tighten control over broadcasting. That is unequivocal. It was part of the discussion on the Huawei and 5G infrastructure file. We continued to call out the government for its indecision, which went on too long. This proves once again that we were right. However, international pressure from our closest allies was needed to make the government take action.

Everything is always so urgent. Urgency seems to be an imperative that really drives this government. We would like to see the government change its ways and become more proactive rather than reactive. With Bill C-26, I think we finally have a starting point. Obviously, there is a lot of work to be done to go further in terms of accountability, in terms of the legitimacy of disclosure on all sides, so we can prevent situations like the one we are in.

I agree that it is a noble goal. Of course I agree with everything about the security of our critical systems. Do we have everything we need right now to deal with both internal and external threats? The answer is no. That is what we have been told and what we continue hearing, at both the Standing Committee on Procedure and House Affairs and the Standing Committee on Access to Information, Privacy and Ethics. We must act. This bill must be quickly sent to committee to be fine-tuned and given some teeth. It is urgent.

I am making a wish and sending it out to the members of the government. I am asking them to always keep in mind our collective security. I trust that they will. We have faith, but we need to be proactive, smart. We also need to talk to our constituents, to speak to people's intelligence. They have suggestions. The G20 countries have good practices that we need to adopt as quickly as possible. We need to set aside partisanship in the interest of our democracy. We need to ensure that the legislation resulting from Bill C-26 really makes people feel safe and lets them know that there is a public, non-partisan institution there to watch out for threats.

The bill names six public organizations that will be given the power to order investigations to make sure things are being done right. I am talking about the Superintendent of Financial Institutions, the Minister of Industry, the Bank of Canada, the Canadian Nuclear Safety Commission, the Canadian Energy Regulator and the Minister of Transport. These are critical sectors of our society and our economy. We must not take threats lightly. Is this enough? We will need experts to tell us whether this is truly legitimate, both for whistle-blowers and for the dissemination of information, because people need to know.

Since I only have about 30 seconds left, I would like to say to those who were just here that the government took action with regard to TikTok because, once again, there was an urgent need to do so. I hope that any future interventions will be undertaken proactively.

● (1705)

[*English*]

Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.): Madam Speaker, I appreciate the comments the member has made. However, when we go to these conferences, one thing that is important to recognize is that even with the legislation, compared to other countries, this is an ongoing issue and cybersecurity is dealt with in a wide variety of ways. What we are talking about today is a very important tool. We have been talking about it and have the legislation before us. We now have an opportunity. In listening to members on all sides of the House, we see that there is a will to support the legislation going to committee. My concern is that if we do not allow that opportunity, there is a finite amount of time. We would like to see the legislation go to committee so that opposition members could propose ideas, suggestions and possible amendments.

Could the member provide her thoughts in regard to the importance of trying to get the legislation to the next stage, given that everyone seems to be supporting the legislation?

[*Translation*]

Ms. Marie-Hélène Gaudreau: Madam Speaker, that is a very interesting question. Here is what I would say in response. If my colleague and I were to switch places, I would say that one of the truly urgent and useful things we could do would be to fine-tune and improve the bill to show that the government really cares about cybersecurity and wants to make sure it protects Canadians from all cyber-attacks and any potential interference while strengthening transparency.

If I were in government, which will never happen, I would make sure I handed over everything if someone asked me for information. I would not hide anything to avoid a potential scandal a year from now. I would take it that far with this bill. That would be the first step in a constructive process.

[*English*]

Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP): Madam Speaker, there were definitely some words in the member's speech that I have to agree with as a member of the NDP, which are really around the Liberals' not taking due care in preparing these pieces of legislation that are coming to the House of Commons. They are not taking due care. They are bringing in these bills that need so much work, and it just appears that perhaps they are not committed to doing their best here. I wonder if they are not qualified, if they are outsourcing to people who are not qualified or what is going on here. I would like to hear if the member really thinks that this is salvageable in committee.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Madam Speaker, in my opinion, a government that knows where it is headed and has the competence to get there does not stumble around and try to clear its conscience or improve its own image. On the contrary, a leader who is in a really good position does not wait for the opposition's proposals to figure out what to do. My colleague asked a good question. I will let people come to their own conclusions in that regard.

[*English*]

Mr. Alex Ruff (Bruce—Grey—Owen Sound, CPC): Madam Speaker, I will ask a question I asked earlier of another member. In this member's opinion, what does she view as the greatest threat to Canada's cybersecurity? Is it state actors? Is it cybercrime and cyber-technology? Specifically, what does the member think is the greatest threat that we face as a nation around cybersecurity?

[*Translation*]

Ms. Marie-Hélène Gaudreau: Madam Speaker, that is exactly one of the questions we need to ask the experts. We must listen to them and accept their recommendations. We must take action based on the analyses of scientists, particularly those who may have had to reconsider some mechanisms.

Obviously, it is important to be ready to act. The answer might be very different depending on the situation. We are hearing a lot about foreign interference in elections these days. We would like this bill to help put an end to that.

● (1710)

[*English*]

Mr. Alex Ruff (Bruce—Grey—Owen Sound, CPC): Madam Speaker, I will take maybe a different tack today to contribute to this debate on cybersecurity. I am going to tell a story about Tom and how he has been impacted by technological changes over the last couple of decades. Before I tell Tom's story, I have to share Emily's story with technology and why this legislation and changes to cybersecurity in Canada are so important and so needed.

Before I get into that, I think it is important to first lay out in simple terms what this bill is about from my current understanding. There are really two parts to the bill.

The first part is about amending the Telecommunications Act to address and fix the security needed for our Canadian telecommunications system. The bill would do this by addressing it through two means. First, it would "direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system." As well, it would establish some monetary penalties tied to those changes.

The second part of the bill is all tied to the critical cyber systems protection act. It would provide the framework for the protection of our critical cyber systems, which are vital to national security and public safety. It would do that through five different aspects. First, it would authorize the government to designate those services that are vital to Canadians, those critical sorts of services, what they are and what systems are tied to them. Second, it would authorize the government to establish who is responsible for maintaining those systems. Third, it has how these cybersecurity incidents would be reported and how Canadians and institutions comply with those changes. Fourth, it lays out how information would be shared and, arguably, needs to be protected. Finally, it gives the "so what" of the enforcement and the consequences for non-compliance with the legislation.

In reality, this bill is quite lengthy and very technical, so I am going to focus most of my speech around two important aspects of the bill. The first aspect is the threats to cybersecurity. The second is information sharing and the need to protect Canadians' privacy rights while highlighting the important need for transparency. How would the government ensure the accountability of any institution affected by this bill, particularly the government itself, with the additional powers this legislation would grant it?

Let us get back to Emily. She is a senior citizen and a retired teacher. She uses a mix of online banking and billing, although she still prefers to handle the majority of her financial transactions right at the bank. She has a fledging social media presence mainly to stay in contact with her grandchildren and friends. She even has a TikTok account at her grandchildren's urging. We will see if she is going to change her mind and delete that sooner than later.

Being online and connected is essential to all Canadians now, more than ever, as a lot of Canadians rely on the Internet for their daily lives. It is about more than just conducting business and paying bills. As I have mentioned, we have seen an increased dependency on the Internet, especially for government services. In the last few years, under the Liberal government, it continues to shift more and more government services online, while unfortunately decreasing service delivery for those without access to the Internet at the same time. I will not go into detail on all the shortfalls I see with the current approach, considering that a large portion of rural Canada still do not have access to high-speed or dependable Internet.

What threats does Emily face? She complains about getting emails and phone calls from people alleging to be affiliated with her bank or service providers. She wonders about the advertising that shows up on her social media feeds that align with something she only mentioned in an email to a friend. How is all of this happening?

To quote the director of CSIS from December 4, 2018, over four years ago, during a speech that he gave to Bay Street, which I have extracted from Stephanie Carvin's *Stand on Guard*, Mr. Vigneault stated that the greatest threat to our prosperity and national interest is "foreign influence and espionage." While terrorism remains the number one threat to public safety, "other national security threats—such as foreign interference, cyber threats, and espionage—pose greater strategic challenges".

In her book, Professor Carvin clearly lays out the risks associated with cyber-attacks, whether malware, ransomware, a targeting of critical infrastructure, denials of services or others. She talks about cyberterrorism, cyber-espionage and cybercrime, so how do we deal with this?

● (1715)

We deal with this not only through this legislation, but also, mainly for some of the challenges we have, as my colleague from Selkirk—Interlake—Eastman talked about in much greater detail earlier today in his speech, our Canadian Armed Forces, the Communications Security Establishment and even our federal police services, which have ways to deal with this. My colleague hinted that sometimes the best defence is a good offence.

Offensive cyber-operations are really not the bailiwick of this legislation, although I would offer that there is some overlap, as we look at a lot of these threats Canadians and Canadian institutions are facing are financed through cyber-attacks and more here at home. We need to tackle this and get the balance right.

The bottom line is Emily and Canadians like her being affected by all of these cyber risks. Professor Carvin pointed out that at least 10 million Canadians had their data compromised in 2017 alone. Unfortunately, this number is likely under-reported, and neither the government nor the private sector fully understand the scale of the problem. To sum up, the threats are huge.

Bill C-26 must balance privacy rights while ensuring national security. Increased use of encrypted apps, data being stored in the cloud on servers outside of Canada, IP protection and more factor into the challenges of getting this legislation right. In order to deal with these threats, the legislation would need to enable our security establishments with robust, flexible powers. However, these robust powers must come with clear guidance on how far and when to inform the public. This is essential in rebuilding our trust in our democratic institutions.

The Business Council of Canada has already publicly expressed concerns over the current draft of this legislation. It rightly identified that large companies, and also small- and medium-sized enterprises, are concerned that the sheer amount of red tape tied to this bill is extremely high.

We need to get the balance right. It is vital, and it is going to require significant expert testimony at committee. Although I would argue the legislation is desperately needed, and I would argue even late in coming, it needs to be done right and cannot be rushed through debate or review at the committee stage.

I have some final comments. This legislation is needed to protect Canadians. However, this legislation needs to be reviewed regularly and needs to include safeguards. I know if he gets the chance, the member for Winnipeg North might ask about what amendment we are recommending. There is no annual reporting mechanism in this bill, so the government should have to table an annual report to Parliament outlining the progress on this legislation, and include an updated cyber threat assessment to Canadians and what it has been hearing back from the companies impacted by this legislation.

Sean McFate, in this book *The New Rules of War: Victory in the Age of Durable Disorder*, wrote, " Secrets and democracy are not compatible.... Democracy thrives in the light of information and transparency."

Finally, I will conclude with Tom's story and how he has been impacted by technology. The bottom line is that he has not been. He does not have a cell phone. He does not use the Internet. He only pays in cash and does not have a credit card. The only way he is currently being impacted is when he shows up to try to get some federal services from the government. He cannot do it because he does not have any of that, and he cannot get anybody to show up in an office to work.

Ms. Jennifer O'Connell (Parliamentary Secretary to the Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.): Madam Speaker, I listened intently to the member opposite's speech. He spoke about transparency. He talked about advertising and constituents who wondered how certain ads were targeted to them. He spoke about annual reporting.

In that vein, I am curious if the member opposite would like to report to the House anything that the Conservative Party has done to condemn their leader for the misogynistic, anti-women hate hashtags that were used to target individuals who promote hate towards women and violence. That is a form of domestic terrorism CSIS has highlighted as well.

Would the member opposite like to talk about clarifying in the House how Conservatives are going to address the cyber-attacks against women in this country?

● (1720)

Mr. Alex Ruff: Madam Speaker, I suggest that the member ask the member for Carleton, the Leader of the Opposition, to answer that question because I cannot speak for him other than to state that he has put out a very clear, definitive statement condemning the hashtags that were put on some videos, which he knew nothing about. I will leave my comments at that.

The last time I checked, we are debating Bill C-26, legislation that is needed to protect Canadians. It needs to be improved and debated to get it right so we can deal with threats of political interference from foreign states, such as the Communist Chinese government. That is of utmost importance to Canadians.

[*Translation*]

Mr. Maxime Blanchette-Joncas (Rimouski-Neigette—Témiscouata—Les Basques, BQ): Madam Speaker, I listened carefully to my colleague's speech.

The Bloc Québécois has often supported the need for the government to tighten cybersecurity controls. I am curious about the Conservative Party and I have a question for my colleague. There has been a lot of doubt and uncertainty concerning cyber-attacks and companies like Huawei. We know and people know that a former candidate for the Conservative leadership worked with Huawei.

I would like my colleague to explain to me what credibility the Conservative Party has today, as we talk about cybersecurity and Chinese interference, because one of its own members, who was a leadership candidate, worked with a company like Huawei. The giants in this world, the Five Eyes in particular, have stopped doing business with this company. Today, we are once again asking how that party can lecture everyone else about cybersecurity.

[*English*]

Mr. Alex Ruff: Madam Speaker, I think the public record of the House and this party in the chamber has been clear-cut on the issue of Huawei. We have called for it to be disavowed, taken off devices and not be allowed to be a provider here. That was passed a year and a half ago.

Whether someone had private employment prior to them declaring or running in a leadership race is a great question for the individual. Because somebody's past history involved them working for different institutions and companies, yes, we can judge those individuals, but let us talk about the public record here. I would argue that there has been no party in the history of Canada that has stood up more for the defence and sovereignty of this nation than the Conservative Party of Canada.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Madam Speaker, a common theme I have heard, highlighted well from members from the Conservative side, is how past records are one of the best indicators for future success or failure. Certainly, when it comes to the issues surrounding Huawei and cybersecurity, we see Canada, especially its reputation on the world stage, being greatly diminished by the actions and, in many cases, inactions of the Liberal government and the Prime Minister over the course of five years.

Could he expand on how those past actions have diminished Canada's reputation among allies and partners?

Mr. Alex Ruff: Madam Speaker, I referenced a couple important books and a couple references by some of our esteemed national security experts across this country. If people read through that and read some books that are out there, they would see this is a threat that has been building for the better part of a decade or more.

The government has known about this since the day it formed government, yet we have seen no action. As mentioned by the CSIS director from 2018, here we are almost five years later, and we are just now seeing this important legislation being delivered.

● (1725)

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Madam Speaker, it is an honour to rise again in the House to speak to Bill C-26, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts. My Conservative colleagues and I, as has been indicated, support this legislation being sent to committee for further study, as it needs a lot of further work and amendments.

For those watching this debate, who have not had time to review the legislation, the bill has two main parts, as has been explained throughout the day. The first part would amend the Telecommunications Act to add the promotion of the security of the Canadian telecommunications system as an objective of the Canadian telecommunications policy and to authorize the Governor in Council and the Minister of Industry to direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system.

The second part of the bill would enact the critical cyber systems protection act, which is a new act, that attempts to provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety and that are designed to operate as part of a work, undertaking or business that is within the legislative authority of Parliament. Services and systems that would initially be designed and designated as vital are telecommunications systems, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems, banking systems, and clearing and settlement systems. Any additions to this list of vital systems can be made and added to by the Governor in Council.

The critical cyber systems protection act would have several components to it. It would authorize the Governor in Council to designate any service or system as a vital service or vital system; it would authorize the Governor in Council to establish classes of operators in respect of a vital service or vital system; it would require designated operators to, among other things, establish and implement cybersecurity programs, mitigate supply-chain and third-party risks, report cybersecurity incidents and comply with cybersecurity directions; it would provide for the exchange of information between relevant parties; and would authorize the enforcement of the obligations under the act and impose consequences for non-compliance. Those would be significant consequences, I might add.

On its face, it seems that the Liberals have finally awoken after eight years of doing absolutely nothing on this file, yet somehow they hastily scrambled to cobble together a proposition for sweeping changes to a regulatory framework, which this legislation would enact.

The Civil Liberties Association said, “The problems with the Bill lie in the fact that the new and discretionary powers introduced by C-26 are largely unconstrained by safeguards to ensure those powers are used, when necessary, in ways that are proportionate, with due consideration for privacy and other rights. The lack of provisions around accountability and transparency make it all more troubling still.” We understand that a modernization in this field may be required to do so without the caveats of being necessary, proportionate and reasonable to take it one step too far for Canadians to accept.

For support of this argument, the Liberals only need to look at the research report from Citizen Lab, written by Christopher Parsons. The report is called "Cybersecurity Will Not Thrive in Darkness, A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act". That report provides 30 recommendations that clearly lay out common sense changes and how this legislation could be improved to include transparency or at least apply limitations on the government's authoritarian use of power. For the benefit of the careless drafters and my Liberal colleagues across the way who would happily vote on any flawed legislation their leader tells them to without bothering with independent thought or even reading its criticisms, I will take some time and share the flaws.

Citizen Lab also seems to address what appears to be a recurring theme with the government: a lack of transparency and limitations on the government's authoritarian use of power. It too addresses that, "The minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything...that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption."

● (1730)

That, too, seems a little broad. Amendments need to be applied that include a limitation on the minister's powers, ensuring that actions are necessary, proportionate and reasonable. This government has proven that it cannot be trusted with powers without strict limitations. It is simply unable to self-regulate.

The Canadian Civil Liberties Association and Christopher Parsons agree again on the lack of privacy and broad provisions around information sharing.

The CCLA writes:

> Also concerning are the very broad provisions around expanding information sharing with a long list of potential recipients including Ministers of Foreign Affairs and National Defence, the Canadian Security Intelligence Service (CSIS), and also, once an agreement is signed, with provincial governments, foreign governments, or international state organisations, again, at the Minister's discretion. The Communications Security Establishment (CSE), Canada's signals intelligence agency is also a key recipient of information.

The Citizen Lab review echoes how the government ought to have included provisions that respect information privacy. To any Canadian listening, this does not sound like too much to ask. Specifically, the Citizen Lab report recommends that "information obtained from telecommunications providers should only be used for cybersecurity and information assurance activities".

It also recommends that "government should explain how it will use information and reveal the domestic agencies to which information is disclosed". The report says "information obtained for telecommunications providers should only be used for cybersecurity information assurance activities". It should only be used for "data retention periods", and that it "should be attached to telecommunications provider's data". Citizen Lab states that "data retention periods should be attached to foreign disclosures of information". It also indicates that "telecommunications providers should be informed which foreign parties receive their information", and "legislation should delimit the conditions wherein a private organization's information can be disclosed".

Why does the government need to be told that its legislation has these fundamental flaws by outside organizations? Many are asking: Do these Liberals have no shame when it comes to the privacy of Canadians?

The CCLA further points out that, although there is an appeal process through judicial review, when the subject of an order finds it to be unreasonable or ungrounded, it suggests that, under Bill C-26, the government overlooks the basic, fair process that even a national security threat would receive. The Citizen Lab, on the other hand, discusses that the government fails to compensate for government intrusion into small business. Mr. Parsons proposes that the legislation should be amended such that telecommunications providers can seek moderation of "certain orders where implementing them would have a material impact on the provider's economic viability".

In conclusion, while it is notable that the Liberal government has finally awakened to this topic, the legislation has again missed some pretty traditional marks of Liberal legislation. It leaves citizens at risk of major government overreach. It takes the privacy and information of Canadians for granted. It relies on a system of review that falls short of due process, and it leaves businesses susceptible to bearing the costs of an overbearing government. Lastly, this is typical lazy Liberal legislation.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Mr. Speaker, let us look at the bungling that has gone on in recent years. Ottawa arrested Meng Wanzhou, not for a common law crime, but for failing to comply with an American embargo. It kowtowed to the Americans on an embargo that Canada does not even share.

There is also Ottawa's refusal to follow the leadership and initiative of the U.S., which acted very quickly with regard to Huawei. Does that not demonstrate a glaring lack of vision?

● (1735)

[*English*]

Mr. Glen Motz: Mr. Speaker, I think many Canadians are wondering why the government took so long to act on Huawei. Our Five Eyes allies have certainly put pressure on Canada and acted previously to ensure that their 5G systems were not compromised, which had been found to be the case with the Huawei technology. That is why, in my statement, I made some comments that this government is finally waking up, after all this time, to deal with some of these issues we are facing as a country.

Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP): Mr. Speaker, I will say it again: It does not feel like the Liberals are taking due care in presenting legislation. In listening to the debate today, I am really concerned, not only as a Canadian but also as a parliamentarian, that there is not enough knowledge in the House to be even having this discussion. I would like to know from the member whether there have been adequate technical briefings from the Liberal government in regard to this legislation, because it seems like this is a lot more serious than what this debate is holding to today.

Mr. Glen Motz: Mr. Speaker, we all know that cybersecurity issues are a fast-moving target and how they change almost monthly. One thing that I can be confident in is our national security agencies that deal with some of these issues on cybersecurity. They are working diligently on our behalf. I would agree that there would be very few of us in the House who would have the technical capacity to understand much of what we ask our defence agencies, our national security agencies and our cybersecurity agencies to do for us on behalf of our country.

I would encourage the government, as was indicated by my colleague, to enlighten the House and to provide briefings by those technical experts in government and from our public servants. We would all benefit, not only from the study of this bill but also from the ability to answer our constituents who have cybersecurity questions. We could answer them more intelligently.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Mr. Speaker, I appreciated the speech by my colleague from just south of my constituency. Certainly, this is an incredibly complex and important series of issues. They are not just related to this particular bill but a whole host of larger security and cybersecurity issues. I wonder if the member could provide further comments, specifically on the lack of leadership that Canada has shown on the world stage over the last eight years that this Prime Minister has been in charge, and has it impacted Canada's reputation globally?

Mr. Glen Motz: Mr. Speaker, it is disconcerting, as Canadians, when we look at the history of the Liberals since they have been in for seven years and five months. Inflation brings it to eight years.

One of the things that is important is we have lost face, if one wants to use that term, with our global partners and our Five Eyes agencies that have now gone and done things without us. That is because we have not been at the table. We have been slow to react to the very legitimate concerns about the cybersecurity and the national security of this country and of our allies.

[*Translation*]

Mr. Joël Godin (Portneuf—Jacques-Cartier, CPC): Mr. Speaker, as the member for Portneuf—Jacques-Cartier, I am pleased to rise today to speak to Bill C-26. I want to say hello to all of the families who are taking advantage of March break to do fun activities in the beautiful riding of Portneuf—Jacques-Cartier.

As I was saying, Bill C-26 seeks to add the promotion of the security of the Canadian telecommunications system. It also seeks to provide a framework for the protection of the cyber systems that are vital to national security or public safety and create frameworks for the exchange of information.

It goes without saying that these issues are very important to the official opposition, of which I am very proud to be a member. It is no secret that my Conservative Party of Canada colleagues and I are, and always have been, great defenders of public safety. It is part of our DNA.

Industry and experts have asked the government many times to create cybersecurity standards, but it is important to act intelligently.

There is a lot of instability in our modern world, and threats can come from anywhere. Cyber-threats are nothing new. This is not a recent thing. It is clear that this weapon is used as much by foreign governments, which have their own motives, as by individuals or groups seeking to do harm or make money, for God knows what motives. It happens everywhere, on both small and very large scales.

Here are a few examples that illustrate this reality: data stolen from institutions or companies and held for ransom; the leak of personal information that affected millions of Desjardins members or customers in Quebec; and possible election interference from Beijing.

No, we are not going to question the outcome of previous elections here. We do not believe that interference changed the overall outcome of those elections. However, electoral integrity is the foundation of our democracy, and it must be ensured and maintained. As a Canadian, I have the privilege of going abroad, and people recognize that we are concerned about protecting our democracy. We need to put measures in place to continue that.

The fact remains that, over the past eight years, the government has been slow to crack down on cyber-threats. This is yet another example of a foot-dragging government finally coming up with a bill, but it turns out that bill has flaws that call for more thorough study in committee.

I know for a fact that this issue is really important to Canadians. We will do the work to make sure this bill is the one Canadians need and deserve. Yes, people want to be safe. Actually, since I was elected in 2015, my constituents have regularly told me they are increasingly concerned about this issue, especially over the past year.

What it comes down to is that confidence in the government and its ability to provide what people need and to keep its promises is essential. It is hard to have confidence in a government that keeps messing up pretty much everything.

I could go on and on about Bill C-13 as an example of a government that makes promises but does not deliver. The government recognizes the decline of French across the country, even in Quebec, but it is trying to impose a bill that does little to address that decline. I know that that is not the subject today, but everyone knows how much I care about official languages, and I had to pass on the message.

I would like to conclude by sharing a very real situation that occurred in my riding. One of my constituents wrote to me about a serious handling error made by Passport Canada.

I would like to inform the House that this is the first time this situation has been discussed publicly. He sent me a letter, and I would like to read it.

● (1740)

Dear Sir/Madam:

I am taking the time to write you a brief note to let you know about what I would describe as a "serious" security flaw within Passport Canada pertaining to the confidential information of Canadian citizens.

It is very important in terms of a timeline.

In early January, 2023, I applied for passports for my three children at Passport Canada.

On February 1, 2023, I received three envelopes containing our passport applications, which were rejected because we forgot to tick a box.

Inside the envelope I also received the rejected application of a woman from British Columbia. I therefore had in my possession her full identification, her passport and her credit card information. I returned those very sensitive documents by express post with a tracking number to Passport Canada.

I filed a complaint out of principle thinking that, although it was just a mistake, it was still worth reporting through Passport Canada's website, so I followed the official procedure. I got a call back. Passport Canada apologized. Nothing more. They refused to compensate me for the cost of returning the documents belonging to the woman from British Columbia. I was told, however, that our applications would be prioritized.

On February 15, 2023, I received four envelopes. I was quite pleased, as I thought we'd finally received our children's passports, but we have three children, not four. As it turns out, our children's passports weren't inside those envelopes. Instead, there were the passport applications (including full identification, passport, original birth certificates, complete credit card data, etc.) of four people from across Canada. These are four different people who have no connection to one another.

What is not stated in the letter is that these people were from Sherbrooke, Ontario, Manitoba and Alberta. That is incredible.

A few days later, we finally received our three children's passports.

As it is obvious, I don't feel I need to explain in my letter the seriousness of receiving the full identification of these people and information that could be used to carry out fraudulent financial transactions by total strangers.

We can't fathom that such mistakes would be made by a recognized federal organization such as Passport Canada, which manages the personal and financial information of so many Canadians. We can't believe that these are two isolated incidents.

This is a very simple task that requires putting the right documents in the right envelope. That's it.

I no longer trust Passport Canada's administration at all. That is why I am entrusting you with the identity documents, which don't belong to us.

I no longer trust Passport Canada's "internal" complaint process, as it will certainly try to cover up this failure, and will only offer an apology.

I am most pleased to read the following excerpt from the letter:

We trust our MP.

I'm always available to answer any questions.

● (1745)

Yes, cybersecurity matters, but the government also needs to take responsibility for the existing systems. It cannot even handle paper documents, but now it wants to allow a minister to step in and be able to manipulate and control information. I am concerned.

I have shown that we have a problem in Canada. We recognize that. We have a problem when it comes to cybersecurity, but we have a problem on other levels too. I would like to see this government take responsibility.

Like my constituent who gave me the documents mentioned, I had to ask myself, what do I do with these documents now? Do I return them to Passport Canada, or do I give them to the minister responsible here? That is a very important question.

Let us get back to the subject at hand, Bill C-26. I am very interested in having measures in place to protect us. It is important that we have confidence in our systems. As a member of the Conservative Party of Canada, I have a lot of confidence in the Conservative members who sit on the committee, as well as members of the Bloc Québécois, the NDP and even the Liberal Party. Things are normally supposed to be neutral in committee.

I must say that I believe in the future. Having said that, we need to put measures in place to have concrete results. Let us work in committee.

● (1750)

Mr. Maxime Blanchette-Joncas (Rimouski-Neigette—Témiscouata—Les Basques, BQ): Mr. Speaker, I listened closely to the speech by my colleague from Portneuf—Jacques-Cartier. The first thing he mentioned is that the Conservative Party of Canada was a great defender of cybersecurity. I want to remind him of the following.

First, the member for Portneuf—Jacques-Cartier supported Jean Charest as a candidate in the Conservative leadership race. Jean Charest worked with the company that was complicit in China's interference. So much for credibility and being a great defender.

Second, a quick Google search shows that the CPC App that the Conservative Party of Canada used during the 2019 election is a version of the uCampaign app, which is used in the United States and requires access to contacts and geolocation, things that relate to privacy. Cybersecurity researchers were actually advising against using that app.

When it comes to credibility and being great defenders, are the people in the Conservative Party of Canada really people we can trust?

Mr. Joël Godin: Mr. Speaker, I just want to point out that people in the Conservative Party of Canada lined up for a chance to become the leader of a national party, whereas the Bloc Québécois has to pick from a grab bag that does not have much in it and has trouble finding a real leader. I think the Bloc members need to ask themselves some questions when it comes to the availability of leaders.

Now, to answer my colleague, there was nothing illegal being done on our side. However, if I turn and look over at the government side, there is a long list of illegal activities that occurred there. I would encourage my colleague to direct his questions to the right party, because we, on this side, obeyed the law.

[*English*]

Mr. Ken McDonald (Avalon, Lib.): Mr. Speaker, I could not help but notice an answer that the member just gave to the member from the Bloc on leadership and picking a leader to be the next prime minister. I wonder if he could explain how that has worked out for him since 2015.

[*Translation*]

Mr. Joël Godin: Mr. Speaker, I salute my colleague from Avalon. It is true I do not have a good batting average. In three leadership races, I have never backed the right horse. However, I am very happy being a member of the Conservative Party of Canada, and it is where I belong. That is part of democracy.

We are straying from the topic. I invite my colleague to ask me a more specific question about Bill C-26, if he has one.

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Mr. Speaker, since the member told us that there has always been a long list of Conservative leadership hopefuls, I would just like to quote his own words.

He said, "I will resign, or join another party in the House of Commons, or sit as an independent, or help form another party."

This was in reference to the winner of the recent Conservative Party leadership race. The options did not include remaining a Conservative, which is what he ended up doing.

Mr. Joël Godin: Mr. Speaker, one thing my colleague from Saint-Hyacinthe—Bagot did not mention is that, when there is a change in leadership, it makes perfect sense to reflect on one's political future.

I invite the Bloc Québécois members to reflect on that when they choose a new leader, as they too have done regularly in the past.

The thing is that, when we think about it, there are options. One very important option is the status quo. We may have to check the record to see what my colleague said. I have a very clear recollection of what I said: status quo, reflection, departure, new party.

I am very happy. I feel very comfortable in the Conservative Party of Canada, and it is the only party I can work with to defend Canadians' interests.

[*English*]

Mr. Randy Hoback (Prince Albert, CPC): Mr. Speaker, that was a great speech from my colleague. I think we would like to see him go on and on, because he has done such a great job.

It has been interesting to be here in the House today, as we listen to the different members from parties talk about the legislation and how important it is. I think there is recognition from all parties within this House that the bill will go to committee and that the committee will have some serious work in front of it, to take a bill that is kind of so-so and put some teeth into it, and make it into something that will work for all Canadians.

I am going to focus mainly on the critical infrastructure part of the legislation. It is so important that we get this right and make sure we have our critical infrastructure protected going forward and make sure we have the tools to keep it protected.

There is a war going on in Europe right now, in Ukraine. We saw that when Putin attacked Ukraine, one of the first things he did was attack certain facilities through cyber-attacks. Ukraine did not have proper protections in place and did not have the tools in place. All of a sudden Putin was able to turn the power off and do things to destabilize local governments. This allowed him to take advantage of the scenario, to move in, take advantage of the territories and conquer those territories. That is just one example of many around the world where cyber-attacks have been used ahead of brutal land attacks. We can see this being used in other ways to influence Canadian politics, or politics around the world, just by how they go about conducting that type of cyber-attack.

It would be really interesting, but it would not be interesting, as I do not ever want to see it, where all of a sudden the natural gas pipelines shut down in the middle of 40-below weather in Saskatchewan. That would be a huge hit to people in Saskatchewan. That would be a hit to our economy. It would be very serious to our seniors and people living without any other means of heating. All of a sudden we could have a cyber-attack, and the gas line would be off, and furnaces would not be working for 12 hours, 18 hours or 24 hours. Our houses would freeze up and our water pipes would break. These are the types of things that could happen with a cyber-attack.

What if our power grid were under attack? What would that mean to Ontario and Toronto, for getting people to and from work? What would it mean to our electric cars, if all of a sudden we did not have any ability to charge them or get them from A to B? What would that mean for people in hospitals, where the hospitals would need a generator to run the emergency services? If someone was getting surgery or was in an accident, they might not get the medical treatment that is required.

These are reasons we need to make sure we are doing everything we can to protect ourselves from cyber-attacks. These are some very simple reasons.

The committee is going to have some very interesting things to do to deal with the legislation. I think that is a good thing. I think we have identified here today some of the flaws in the piece of legislation: some of the oversight flaws, some of the flaws in regard to the sharing of information and why they are important to be addressed as we go forward.

We can look at, for example, the sharing of information. I was at the University of New Brunswick in 2017, and they said one of the issues they had with cybersecurity attacks was that somebody might be attacked, but might not share the information on what the attack was and how it happened for fear of liability. For example, in such a situation, if a hospital was attacked, it may not necessarily want to share that information with anybody else for fear of liability, if all of a sudden the records of patients had been confiscated by somebody part of the attack.

In the legislation before us, if we get it right, they should be able to share that information. They should be able to share it with a variety of different critical infrastructure facilities to make sure they put the appropriate patches into their software so that same person who attacked that hospital cannot attack another hospital, attack the electrical grid or use malware, or whatever means they used to attack that hospital, and so it does not happen anywhere else.

That would be a good thing. We have to make sure the legislation can reflect that and allow that information to flow between different parties, so we can keep protecting ourselves in a fluid situation. I think that is something we will see in the legislation, if it is done properly.

We know oversight is very important. Canadians have to trust that the oversight bodies and the people who are putting in these regulations and monitoring these regulations have accountability and that they are accountable back to Parliament. It cannot be just to the minister. We have seen situations in the past with the current government where accountability goes to the minister, and Parliament never really finds out what actually went on and what goes on, and Canadians are in the dark.

We can look at SNC-Lavalin. There is a classic example where we did not see all the details of what was going on in a situation. We can look at what was announced today, how the government is going to leave the investigation into Chinese election interference to NSICOP. That is something the Chinese would do. They would create a committee and say they were going to investigate themselves in their own committee and then make sure it is never public. That sounds rather Chinese to me, but that is happening here in Canada, and Canadians do not accept that. That is why it is very important that there be public oversight and that there be the ability to make sure these bodies and the government are acting in a fair and responsible way.

● (1755)

Some of the civil liberties groups have said that there are some serious concerns with this legislation. They should be brought in front of the committee and listened to, and then the committee should try to figure out how to address those concerns, to make a better piece of legislation.

We have seen the Liberal government react and react and react, in so many situations. To me, this looks like another example where it is reacting. It is basically just doing lip service and then it will throw it to the committee to do the work. This should have been done a long time ago. For eight years, we have been vulnerable. What could have happened in those eight years could have been life-changing for a lot of Canadians, because of the lack of forethought or good policy out of the Liberal government.

If we think about it, it is a talking point that the Liberals have done here. They have put some stuff together and thrown it into the House to say they are working on cybersecurity, but it is half done. The committee is now going to have to do the rest of the job, to actually finish it and hopefully get a good piece of legislation.

That is in question, because we do have a Liberal-NDP government here. They tend to side with each other all the time. Will they side together here, or will they actually take a step back and say, yes, we have to do what is right for Canadians and address the issues that have been raised by different associations and different groups? Are they going to look at what they can do to make this a better piece of legislation, or are they going to stick to their partisan angles and dig in their heels? If they do that, the people who really lose out are Canadians. They are the people who will be impacted by a cyber-attack, because we did not put the proper safeguards in place.

We should not think that this will not have an impact on our economy. A good example we have just seen is the cyber-attack on Indigo last week. Its computer systems are down as we speak. It is telling customers they cannot buy books online. They actually have to go to a storefront to buy their books because of a cyber-attack, a ransomware attack.

We have seen, over and over again, different schools and universities facing these types of attacks. They need to know that the government is there and is going to be there to help them. They need to know that the people who are doing these attacks will be identified and somehow dealt with, if possible. We understand that a lot of these attacks happen from Russia or North Korea, outside of our territory, but when they happen from within Canada, we want to make sure that the people who are doing these types of things are properly dealt with. We want to make sure that this does not happen again. We want to make sure we learn from the experience so it cannot happen again.

There are lots of things in this legislation that can be really good if it is dealt with properly, but it has to go to committee. I think Conservatives have been very clear. We want to see this go to committee. I just hope the committee members are able to actually do the work that is required to take a piece of legislation that is mediocre at best and make it into something that will work for all Canadians.

● (1800)

Mr. Fraser Tolmie (Moose Jaw—Lake Centre—Lanigan, CPC): Mr. Speaker, it is always an honour to rise in this House on behalf of the people of my riding of Moose Jaw—Lake Centre—Lanigan.

The safety and security of our nation is of paramount importance, and I understand the need to enhance the safety and security of Canadians, both here at home and abroad. This would include many of our international corporations, which are large contributors to our economic base, and of course our own government institutions and interests. Having the opportunity to speak to cybersecurity in Canada gives us an opportunity to enhance or increase our country's ability to protect us from cyber-threats.

A significant concern for all Canadians is security. This concern has increased in recent times, as we see the rise in organized crime and gang-related offences, which have gone up 92%. The question I ask myself when I see this increase is this: Will the Liberal government be led by evidence and act on the evidence that has been reported?

Cybersecurity is extremely important for our nation to protect itself from inside and outside threats. I welcome Bill C-26, but I do have some concerns pertaining to the success of the bill, and one concern is about accountability. This is a question that we in opposition bring up every day in this House and regularly.

Bill C-26 is essentially divided into two different parts. The first part is to amend the Telecommunications Act to promote the security of the Canadian telecommunications system, adding security as a policy objective; to bring the telecommunications sector in line with other infrastructure sectors; and to secure Canada's telecommunications system and prohibit the use of products and services provided by specific telecommunications service providers. This amendment would enforce the ban on Huawei Technologies and ZTE from Canada's 5G infrastructure and would remove or terminate 4G equipment by the year 2027. What stands out to me, which has been a concern, is the time that it took the government to react to enforce the ban on Huawei.

The second portion of this bill is to enact the critical cyber systems protection act, or CCSPA, designed to protect critical cyber systems and "systems that are vital to national security or public safety and that are delivered or operated...within the legislative authority of Parliament." As a report by Norton Rose Fulbright notes, the purpose of the CCSPA is, first, to "[e]nsure the identification and effective management of any cybersecurity risks, including risks associated with supply chains and using third-party products and services"; second, to "[p]rotect critical cyber systems from being compromised"; third, to "[e]nsure the proper detection of cybersecurity incidents"; and finally, to "[m]inimize the impacts of any cybersecurity incidents on critical cyber systems."

The impacts of this bill would be far-reaching, and here are the things that need to be considered when this bill is in place. The government would have the power to receive, review, assess and even intervene in cyber-compliance and operational situations within critical industries in Canada; to make mandatory cybersecurity programs for critical industries; and to enforce regulations through regulatory and legal enforcement, with potential financial penalties. With this in place, the Governor in Council and the Minister of Industry would be afforded additional powers.

As the report notes:

> If any cybersecurity risks associated with the operator's supply chain or its use of third-party products and services are identified, the operator must take reasonable steps to mitigate those risks. While the Act doesn't give any indication of what kind of steps will be required from operators, such steps may be prescribed by the regulations [at committee].

It goes on:

> The Act also addresses cybersecurity incidents, which are defined as incidents, including acts, omissions or circumstances, that interfere or could interfere with the continuity or security of vital services and systems, or the confidentiality, integrity or availability of the critical cyber systems touching upon these vital services and systems. No indication is given as to what would constitute interference under the Act. In the event of a cybersecurity incident, a designated operator must immediately report the incident to the CSE and the appropriate regulator. At present, the Act does not prescribe any timeline or give other indication as to how "immediately" should be interpreted.

● (1805)

Some deficiencies in Bill C-26, as it is presently drafted, can be listed as follows:

The breadth of what the government might order a telecommunications provider to do is not sufficiently bounded.

The secrecy and confidentiality provisions imposed on telecommunications providers threaten to establish a class of secret law and regulations.

There is a potential for excessive information sharing within the federal government and with international partners.

The costs associated with compliance with reforms may endanger the viability of smaller providers.

The vague drafting language means that the full contours of the legislation cannot be assessed.

There exists no recognition of privacy or other charter-protected rights as a counterbalance to the proposed security requirements, nor are appropriate accountability or transparency requirements imposed on the government.

Should these recommendations or ones derived from them not be taken up, the government could be creating legislation that would require the public and telecommunications providers to simply trust that it knows what it is doing and that its actions are in the best interests of everyone.

Is it reaching the right decision to say that no need exists for broader public discussion concerning the kinds of protections that should be in place to protect the cybersecurity of Canada's telecommunications and networks? The government could amend its legislation to ensure its activities conform with Canada's democratic values and norms, as well as transparency and accountability.

If the government is truly focused on security for Canadians, should we not start by reviewing the gang and organized crime evidence showing that our present policies have failed? Should we not look at safety and security in our bail reform to protect innocent Canadians who become victims?

If Bill C-26 is a step in protecting Canada from cybersecurity threats, what is the review process to ensure compliance? What is the review process to ensure effectiveness and goals are met when we look at Bill C-75 regarding bail reform? The NDP-Liberal government is not interested in reviewing bail reform even though the evidence clearly shows that Bill C-75 failed.

Cybersecurity is important to our country's security, as are the victims of crime after their safety and security are violated. I am deeply concerned that the government is struggling with evidence-based information to review Bill C-26, as Bill C-75 and Bill C-5 are not supported by evidence. In fact, offenders and criminals are a higher priority than their victims are. My concern is if Bill C-26 requires amendment or review.

Bill C-26 proposes compliance measures intended to protect cybersecurity in sectors that are deemed vital to Canadian security. Therefore, although late out of the gate, Bill C-26 is a start.

In conclusion, I would like to see some clear accountability to ensure the objectives of this bill are met and that a proper review process is conducted that holds individuals, corporations, and most importantly, our government accountable.

● (1810)

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Mr. Speaker, I really appreciate the debate and the questions my colleague posed.

I think most Canadians back home watching this are wondering what the technical nuances are of everything we are discussing with respect to this legislation. We have even had some members of Parliament stand up here and say that they do not feel properly equipped to have this conversation.

I think one thing that everybody back home can relate to is seeing something on the news stating that the credit card information of a million people has been stolen or the data of some businesses that might have their personal information is now being held hostage in a ransomware attack. That is why this is a very important debate. I will be speaking about this a bit later.

I think the bill is missing the component of protecting the personal information of Canadians. Can my colleague tell us his thoughts on the bill in this regard? My speech will focus on the advances in technology and network infrastructure, as well as the rapid pace of technological development. With this bill, would we actually be able to keep up with the threats we are facing?

Mr. Fraser Tolmie: Mr. Speaker, Canadians are very trusting people. We like to give. However, when we buy into something, such as an app, we are giving over some vital information that is ours. We have seen cases where people had that information abused, and there has been no full disclosure. This is one of the concerns I have with the bill.

There are concerns that we have already witnessed in this country in terms of different businesses; a colleague mentioned Indigo being attacked. My hope is that, during committee, we ensure that we are protected. We have a responsibility to Canadians to protect them.

[*Translation*]

Ms. Andréanne Larouche (Shefford, BQ): Mr. Speaker, I am hearing some contradictions from my Conservative colleagues today. My colleagues in the Bloc have perhaps done a better job than me of explaining the importance of banning Huawei and the fact that Canada has been slow to do so. My Conservative colleague also mentioned it, but one of the Conservative leadership candidates actually worked for Huawei, so one wonders which way the Conservatives are leaning.

I met with an interdisciplinary cybersecurity research group and learned some fascinating things. Canada's bureaucracy is really slow when it comes to cybersecurity. The research chair at the Université de Sherbrooke criticized the fact that the cybersecurity issue was allowed to drag on under the pretext that it was not yet an election issue. Now it is finally becoming one. That is exactly what we are seeing right now with China's interference.

The Conservatives were not very quick either, because we are behind many other countries. The first RCMP report on cybercrime was not released until 2014, and the report was criticized at the time for containing no numbers, no statistics. The comments were general and predictable, and there were no forecasts. Things have not happened fast enough.

Here we are in 2023, and we really have a lot of ground to make up compared to many other countries, especially European countries. I think it is time to turn this over to the committee, make up for lost time, and pick up the pace on this bill.

● (1815)

[*English*]

Mr. Fraser Tolmie: Mr. Speaker, I agree with the member that when the bill is in committee, this issue has to be really focused on. Obviously, we want it to move swiftly but not at the expense of overlooking some of the potential pitfalls that will impact Canadians. I think we have to trust the committee to actually make good amendments on this.

Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP): Mr. Speaker, I would ask the member about the secrecy and lack of transparency. Does the member believe that the committee can solve this, or is this bill just too shallow for it to go forward?

Mr. Fraser Tolmie: Mr. Speaker, we always give loaded questions.

I would have to say that, obviously, when one is a member of Parliament, one's honour is on the line all the time. I would hope that our ability to restore honour in our profession always depends on our own moral compass. Sometimes we see that fail, and it is disappointing. However, I really hope this committee can get its act together and get this sorted out.

Mr. Clifford Small (Coast of Bays—Central—Notre Dame, CPC): Mr. Speaker, there is a pressing need to secure Canada's critical infrastructure against cyber-threats.

Computer systems, which run our health care, energy and financial systems, are targets for criminals and foreign adversaries to attack. Disruption of medical services at a hospital or electricity through a grid would have severe consequences, possibly including injury or death.

This is exactly what happened on October 30, 2021, in my province of Newfoundland and Labrador. My hon. colleague across the way agrees with what I am saying because he, his family members or his friends, I am sure, had some of their personal information breached in that attack.

Personal information belonging to thousands of patients and employees was obtained through a cyber-attack on Eastern Health. In fact, over 200,000 files were taken from a network drive in Eastern Health's IT environment. Over 58,000 patients and almost 300 staff and former staff had their personal data breached.

The information taken included health records, medicare plan numbers, dates of birth, names and addresses. In fact, some even had their social insurance numbers taken. The immediate result was that a complete shutdown of the health care system took place throughout the entire province.

Patients who had waited through the pandemic found that critical care for such things as cancer and heart disease were put on hold. Many had to wait weeks or even months to have their appointments rescheduled. Some of these folks had poor outcomes. In fact, people's lives were shortened in some cases as a result of the cyber-induced shutdown of the health care system in Newfoundland and Labrador.

This is very serious stuff. This was not the first time such a cyber-attack happened in Canadian health care. In October of 2019, three hospitals in Ontario were victimized in a similar fashion.

On another note, a pipeline company in the United States fell victim to hackers in 2021. This led to diesel and jet fuel shortages, disrupting most of the economy of the eastern seaboard of our neighbour to the south.

These are just a few examples of catastrophic outcomes resulting from cyber-attacks in recent years. Canadians need protection from these types of attacks. This legislation is intended to align with the actions of our allies in the Five Eyes. This bill would give clear legislative authority to the government to prohibit high-risk entities, such as Huawei, from assuming critical roles in our cyber-infrastructure.

This legislation is filled with good intentions. Currently, a cybersecurity incident is defined as:

> an incident, including an act, omission or circumstance, that interferes or may interfere with
>
> (a) the continuity or security of a vital service or vital system; or
>
> (b) the confidentiality, integrity or availability of the critical cyber system.

There is no indication given as to what would constitute interference under the bill. Does this mean that the cyber-attack on Newfoundland and Labrador health care would not be classified as interference?

In addition, there is no timeline specified in this bill for the reporting of cybersecurity incidents to the CSE and the appropriate regulator. The bill says that reporting must be immediate. “Immediate” is not interpreted in this bill. Is it one hour, one day or one week? This is something we need to know.

● (1820)

In terms of civil liberties and privacy, technical experts, academics and civil liberties groups have serious concerns about the size, scope and lack of oversight of the powers that the government would gain under the bill.

In late September 2022, the Canadian Civil Liberties Association, the International Civil Liberties Monitoring Group and the Privacy and Access Council of Canada, as well as several other groups and academics, released their joint letter of concern regarding Bill C-26.

While stating the collective's agreement with the goal of improving cybersecurity, the joint letter goes on to state that the bill is “deeply problematic and needs fixing”, because “it risks undermining our privacy rights, and the principles of accountable governance and judicial due process”.

The joint letter outlines several areas of concern, including increased surveillance. The bill would allow the federal government “to secretly order telecom providers to ‘do anything, or refrain from doing anything’” necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption.

While this portion of the bill goes on to list several examples of what “doing anything” might entail, including, for example, prohibiting telecom providers from using specific products or services from certain vendors or requiring certain providers to develop security plans, the collective expresses the concern that the power to order a telecom to do anything “opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards”.

Bill C-26 would allow the government to “bar a person or company from being able to receive specific services, and bar any company from offering these services to others, by secret government order”, which raises the risk of “companies or individuals being cut off from essential services without explanation”.

The bill would provide for a collection of data from designated operators, which could potentially allow the government “to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations.”

There is a lack of "guardrails to constrain abuse". The bill would allow the government to act without first being required to perform "proportionality, privacy, or equity assessments" to hedge against abuse. This is concerning to the collective, given the severity of the penalties available under the statute.

There is the potential for abuse by the Communications Security Establishment, the federal agency responsible for cybersecurity but, more prominently, signal intelligence. The CCSPA would grant the CSE access to large volumes of sensitive data. However, it would not constrain its use of such data to its cybersecurity mandate.

The civil liberties of Canadians are already under attack. Bill C-26 does not accurately enough define how our civil liberties would be protected. Given the need for protection from cyber-attacks, a bill like this is quite necessary, no doubt.

In its current form, with so many unknowns for Canadians, I will not be able to support it. However, I do support sending it to committee for some input from Canadians and for some fine tuning, to turn it into an instrument to protect us all from cyber-attacks.

● (1825)

Mr. Ken McDonald (Avalon, Lib.): Mr. Speaker, it seems that the Conservative Party keeps pointing out the flaws or weaknesses in this bill as it is put forward. However, I wonder, if it goes to committee and gets amended, does the member think it would prevent the so-called robocall scam that happened a few years back, when the Conservative Party was found guilty of using it during an election?

Mr. Clifford Small: Mr. Speaker, I am sure that sending this bill to committee will make some improvements. It is unfortunate that my bill, Bill C-251, did not get the opportunity to get to committee and get improved. My hon. colleague is quite aware of the ill consequences of not allowing legislation to get to committee and to be improved, to seal the deal and have positive outcomes for all Canadians.

Mr. Mel Arnold (North Okanagan—Shuswap, CPC): Mr. Speaker, it is a pleasure to take this debate from coast to coast. I live on the west coast, and I thank the member for Coast of Bays—Central—Notre Dame for presenting from the east coast.

Recently, we had a cyber-attack on Okanagan College in my riding of North Okanagan—Shuswap. It is always an honour to rise as the representative from that area.

Does my colleague for Coast of Bays—Central—Notre Dame think that this bill will address the concerns that were obviously brought to light there, when the college was basically shut down for weeks after the Christmas break? Students could not access their files. Basically, the entire college system was shut down.

If this bill is needed, I wonder if the member has a comment as to why it has taken the government seven and a half years to address this, when our party brought to its attention the potential issues with Huawei and its activities in Canada. Maybe the member would like to comment on that.

Mr. Clifford Small: Mr. Speaker, it is great to take a question from my colleague, who has constituents who have had hard times due to cyber-attacks. I hope this bill can stop that from happening. I also hope that my hon. colleague can bring some of these people who were affected by a cyber-attack to committee and let them have their input as the bill is being debated and amended.

I am sure this bill is going to need quite a lot of amendments if it is anything like most of the legislation that has come from the government.

● (1830)

Mr. Marc Dalton (Pitt Meadows—Maple Ridge, CPC): Mr. Speaker, I get the impression on this side of the House that the Liberals only come forward with measures to do anything when their feet are put to the fire. We had an example of that today, with the Prime Minister announcing the appointment of a rapporteur, which is a good French word. How many Canadians even know what the word means? He is throwing these measures out to make it look like he is doing something. It is not happening. It is simply not happening. It is to make it look like they are doing something. Canadians see through this.

I wonder if the member could talk about one of the half-measures that the Liberals are doing with this bill.

Mr. Clifford Small: Mr. Speaker, I cannot really concentrate. My hon. colleague came up with that word that I cannot even make sense of. That reminds me of the Prime Minister's dad with his famous "fuddle duddle". What does "fuddle duddle" mean? I do not know what "rapporteur" is. I am hoping that this bill addresses some of my hon. colleague's concerns.

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Mr. Speaker, I appreciate the fact that we have the ability to have this debate in the House of Commons today. It has been lively, and I have enjoyed it, but I am going to remind Canadians, who might be watching at home, and my colleagues who are here, just how rapidly technology has advanced in the course of our lifetimes.

One of the last jobs that I did prior to becoming a member of Parliament here in the chamber was as a tenured faculty member at Red Deer College in Red Deer, Alberta, where I was a member of the computer systems technology department. I taught computing systems to students there for a number of years. It was a great job with brilliant minds of the young people who had come to that college.

I learned all about computing when I was an adult. I did not have the privilege of growing up inside a computer. Those of us in the room who are old enough to know, back in the mid-1990s, an old IBM 386DX used to cost hundreds, if not thousands of dollars, for computing power that right now would not even match an outdated, obsolete iPhone.

I would remind the people watching what the significance of this debate is and why the legislation we are discussing, and hopefully sending to committee, is so important.

If we go back to the 1960s, the development of ARPANET is where the foundations of the Internet started. The transmission rate of data at ARPANET, which was a military defence network, and as I said, the founder of the Internet, was 56 kilobytes per second. Now, in 2022, we are at 5U, which is 100 megabits per second. This is an absolutely astounding rate of growth in the ability to move information from point A to point B.

The growth since 1983 is based on Nielsen's Law on bandwidth. Basically, every year we increase the capacity to send information over a network by 50%, which is an exponential number that keeps going up. It is not 50% of where we started from. It is 50% from now. If we could do compound interest in the financial system that would give us a 50% compound interest return, we would be doing quite well. However, this is how fast the network processing, or the bandwidth, is growing in the world.

If we take a look at Moore's law, when it comes to the ability of microchip processing, transistors on a microchip double every two years, which is what they said back in the mid-1960s. In 1970, there were just over 1,000 transistors on a microchip. Now, there are 50 billion transistors on a single microchip. That is an insane amount of computational power, and coupled with the bandwidth that I just talked about, leaves us in a situation where parliamentarians and politicians need to be cognizant of the scale of the capacity of what we are talking about.

Let us go back to the early 1990s and a computer at that point in time. We measure computational power in things like FLOPS, or floating point operations per second, and MIPS, or million instructions per second. A computer back in the early 1990s could do under 1,000 calculations per second. Today, we are well over a billion computations per second, and that is floating point operations, which are more complicated than even just the millions of instructions per second. We can just take a look at that efficiency.

When we talk about going back to original computers, we talk about the Harvard Mark II, which I think weighed 23 tonnes. Now, with today's technology, the demand of energy per unit of processing or unit of computing power has actually been cut in half every 18 months, which means that every 18 months, the amount of energy and power that it took to do the same job is now half of what it was. This is allowing for massive growth. We see things springing up all the time. We have Bitcoin mining operations using massive amounts of electricity. Can members imagine if we tried to use that much electricity using older computers? It would have been absolutely astounding.

On storage, I am not talking about memory in the computer, and I already talked about the microchip storage. However, when I was teaching at Red Deer College, we got these hard drives that came in so that we could play around with a hard drive. Now, I am mostly a software guy. I was a programmer and database administrator, but I had to learn a little bit about the hardware.

● (1835)

We had a 420-gigabyte hard drive. It might have been a megabyte, but I think it was a gigabyte, but oh my goodness. I remember we had 20-gigabyte hard drives. Who can remember when they were excited about having a 20-gigabyte hard drive?

In the 1950s, if we go back to early computing, the cost to store one terabyte of data, using that technology and working backwards on the cost of a unit of storage and the evolution of computing, it would have cost over $100 trillion. Today, for less than $100, people can go to a computer store and buy a hard drive or a disk for their computer that contains well over a terabyte of data.

Why is this history lesson so important? It is because we are moving into an age of artificial intelligence. Some of my colleagues have expanded upon the importance of artificial intelligence in their speeches earlier. I listened with great anticipation to what they said.

What does the requirement for computational power and bandwidth require for artificial intelligence? Today's computers, looking at artificial intelligence, are actually using something called petaFLOPS, that is 10 to the 15th, a quadrillion floating point operations per second. That computational power exists in our networks that are out there that are now hooked up with 5G networks that can operate at 100 megabits per second.

The amount of technology and the availability of technology and the ability of that technology in today's standards are absolutely amazing. In fact, because of these advances in technology, we now have some pretty amazing facts. A television today, a software game, any of our intelligence toys, anything that requires computing is 35% lower in cost relative to income than it was just 20 years ago. Meanwhile, college tuition, education and so on have gone up over 150% in the same time frame. That tells us the vast amount of research and technology that has been put in place on the development of this technology.

That is why it is so important. Artificial intelligence is a conversation that we should be having in this House, and cybersecurity is certainly a part of that. Everybody knows, we are watching the news, and we see some great potential uses. That is the thing; everything that is designed to make our lives better, more efficient and more productive could also be used for evil.

I am not accusing anybody of using it for evil. That is not the point I am making. However, everything we want to use for good, somebody else could use with malicious intent.

I will just give a couple of examples. We have had the conversation today about the amount of personal information that has been lost, hacked and held hostage through various cyber-attacks. We know that the People's Liberation Army in China has tens of thousands of people working, just in their cyber-attack divisions alone. Just to keep in mind, for the people who are watching at home, Canada's entire military hovers between 60,000 and 70,000 people. The People's Liberation Army, just in their cyber-intelligence division alone, would have more people than the entire Canadian Armed Forces across all three of our divisions.

These are the folks, coupled with our security establishment, who need to have the tools to defend us, our networks, our infrastructure and all the critical things that we do. We are talking about hospitals, electricity grids and all these things. Imagine something as simple as a driverless or autonomous vehicle. An autonomous vehicle can now drive itself, and the reason it can do it is because we have that 5G technology, and we have the cameras and the ability for that car to make intelligent, informed decisions at the calculation rate, because of the advances in computers that I just talked about. Imagine what somebody with malicious intent could do with an autonomous car, if they wanted to.

That is why we have to get the cybersecurity question right in this debate. If we leave our systems vulnerable, if we leave ourselves open to the possibility, and we are never going to be perfect, and for everything we do, somebody with malicious intent could find a workaround for it, so we have to keep it up to speed.

● (1840)

With all the facts I just talked about, the doubling of technology and computing power and the halving of electricity requirements, we need to be very clear. This is the one piece of advice that I will offer to my friends across the way in the government, because this is too important not to be working together on this. The technology is growing and developing at such a rapid pace that I really do hope that we and the government have the ability to put in some clauses to review this, because it is just so important that we get this right and constantly review our cyber defences and cybersecurity in this country.

ADJOURNMENT PROCEEDINGS

A motion to adjourn the House under Standing Order 38 deemed to have been moved.

[*English*]

TAXATION

Ms. Laurel Collins (Victoria, NDP): Mr. Speaker, I am rising again in this House for what feels like the thousandth time to call on the government to end fossil fuel subsidies, to implement a windfall profits tax on oil and gas companies and to invest in climate solutions.

Each time, I draw attention to the fact that we are in a climate emergency and that, in the words of Greta Thunberg, "our house is on fire". When one's house is on fire, one jumps into action and calls the fire department. Instead, the government not only is continuing business as usual and planning to increase oil and gas production in the coming years, but continues to hand out billions of dollars to profitable oil and gas companies. These are the companies that are literally fuelling the climate crisis, that for decades have been funding disinformation about climate change and that are profiting off increasing emissions. Our house is on fire, and instead of using our financial resources to put that fire out, the government has decided to hand out billions of dollars to the very companies intent on pouring gas on the flames.

The Liberals say, yes, there is a climate emergency and yes, our house is on fire, but let us just wait inside a little longer before we take action, and we should probably listen to the oil and gas lobbyists and CEOs. We should probably listen to the arsonists when we make a plan to put out that fire. They are experts in fire, after all.

This is the reason we are where we are. For over 30 years, the science has been clear, and now we are seeing communities washed away, and Lytton burned to the ground. There are severe hurricanes on the east coast, and on the west coast we are choking on smoke in the summers. Hundreds of people are dying in heat waves. This is happening now, and it is only the beginning.

We know what this means for our children, for the future we are leaving them. My colleagues will excuse me if I am upset and angry and tired of broken Liberal promises. I want to see action, but not the kind of action we have been seeing from the government. It should not give our public money to big polluters. They are making record profits. It should make them pay for their own pollution. They can afford to reduce their own emissions.

The government listened to big oil and gas lobbyists and created massive new subsidies and new handouts for unproven carbon capture and storage technology. According to the world's top climate scientists, carbon capture and storage is one of the most expensive, most risky climate options and unproven at scale, but it is the oil and gas industry's favourite option because it does not involve transitioning to different energy sources. If the oil and gas industry wants to gamble on expensive, unproven technologies, get them to do it with their own money.

Instead of forcing these rich oil and gas CEOs to reduce their own emissions, the Liberals gifted them billions in tax credits. What are those very companies doing now? They are increasing their emissions. They are scaling down their climate commitments. They are raking in record profits and asking for more handouts.

We need to fix Canada's taxation system, which is rigged in favour of big oil and gas. Let us end fossil fuel subsidies and implement a windfall profits tax.

● (1845)

Mr. Terry Beech (Parliamentary Secretary to the Deputy Prime Minister and Minister of Finance, Lib.): Mr. Speaker, I am pleased to take part in this debate this evening. I want to thank my colleague from Victoria, a place where I grew up as well, for asking these questions. I have prepared a response that actually takes on all the questions that were raised in her original question, which include inflation, affordability, tax fairness, climate change and fossil fuel subsidies.

We understand, as a government, that many Canadians are struggling to make ends meet during a period of high global inflation. Canadians are feeling the pain when they go to the grocery store, when they fill up their tanks and when they pay their rents. Although inflation in Canada is lower that it is in the United States or in Europe, it is our responsibility to make life more affordable while building an economy that works for everyone. This is why we have provided $12.1 billion in new inflation-relief support with many measures continuing in 2023 to help make life more affordable for millions of Canadians. This includes measures like the GST rebate, dental care, child care and supports for seniors. Students no longer need to pay interest on student loans, and new parents are able to more easily return to the workforce.

At the same time, our government has been, and remains, committed to making sure everyone pays their fair share of taxes. For example, budget 2022 announced a permanent increase of the corporate income tax by 1.5 percentage points on the largest and most profitable banks and insurance companies in Canada. It also announced the Canada recovery dividend, a one-time 15% tax on Canada's most profitable banks and insurance companies to help pay for the cost of fighting COVID. We have also reduced taxes for the middle class and for small businesses on four separate occasions, while increasing taxes on the top 1%.

Our government is also committed to phasing out inefficient fossil fuel subsidies that give fossil fuels an unfair advantage over cleaner energy solutions. In our previous election platform, we committed to phasing out these fossil fuel subsidies by 2025, but like the member opposite said in her speech, we felt the matter was so urgent that we actually accelerated the timeline of this commitment to the end of this year, a full two years early. In fact, the majority of inefficient fossil fuel subsidies have already been eliminated.

In budget 2022, for example, the government committed to eliminating the flow-through share regime for fossil fuel activities. This will be done by no longer allowing expenditures related to oil, gas and coal exploration and development to benefit investors after March 31, the end of this month. This coincides with our world-leading climate plan, which is working to lower Canada's greenhouse gas emissions while creating high-paying, sustainable jobs that will benefit Canadians for generations to come.

The government is also taking meaningful actions to improve competition in this country and ensure that consumers pay fair prices for goods and services. We provided an additional $96 million in funding over five years to the Competition Bureau in budget 2021 and made targeted improvements to the Competition Act in June 2022. This will strengthen the Competition Bureau's powers, better protect consumers and ensure that workers and small businesses are protected from anti-competitive or deceptive practices. These amendments brought the Act more in line with international best practices, including higher maximum fines and a broader scope of anti-competitive behaviour that the Competition Bureau can now review. On top of that, last fall we launched a consultation on the future of competition policy in Canada to seek input on what further we can do.

In conclusion, our government is fighting climate change, making life more affordable, ensuring the Canadian economy is competitive and, at the same time, making sure everyone pays their fair share of tax. Given that Canada enjoys the lowest deficit and lowest net debt-to-GDP ratio in the G7, we can expect that Canada, and Canadians, are well positioned to outperform in the years ahead.

● (1850)

Ms. Laurel Collins: Mr. Speaker, I hope the member was not serious when he said that most inefficient fossil fuel subsidies have been eliminated, because that would mean that whatever the government is counting as inefficient fossil fuel subsidies is not taking into account the billions of dollars we are still handing out to oil and gas companies.

I am baffled by Liberal MPs who claim to care about our climate and to understand the urgency of the crisis we are in, but then support massive handouts to oil and gas and refuse to make these companies pay what they owe. Oil and gas companies have profited for decades from fuelling the climate crisis. These rich CEOs and lobbyists have successfully lobbied for tax breaks and handouts. I will remind my colleagues that oil and gas companies last year made more money than they have ever made before, while Canadians are struggling to pay for groceries.

It is time for Canada to stand up to big oil and stop making Canadians and the environment pay the price.

Mr. Terry Beech: Mr. Speaker, our government has taken meaningful actions to make life more affordable and build a sustainable economy that works for everyone. We are doing this by fighting climate change; making sure everyone pays their fair share of tax; making our economy more competitive; and supporting Canadian workers, creating more than 809,000 new jobs since the start of the pandemic. Canada is working, Canadians are working and their government is working hard for them as well.

IMMIGRATION, REFUGEES AND CITIZENSHIP

Mr. Eric Duncan (Stormont—Dundas—South Glengarry, CPC): Mr. Speaker, as I have said in this House and during question period, a growing number of Canadians believe that everything feels broken in this country. There is correlation and a connection to what they are feeling that brokenness from: the poor management from the current Liberal government.

Whether it was when Veterans Affairs Canada officials admitted that their staff offered MAID to multiple veterans when they were looking for help or the lack of accountability when it comes to foreign interference, getting to the bottom of it and having transparency to make sure it never happens again, Canadians feel like their federal government is broken. When it comes to trying to get a passport or accessing an airport with ease and reasonableness, they feel like things are broken. If anybody has ever gotten a bill from CRA when they owe $41.72, they get the letter right away and it says they have 30 days to pay or the penalties start. Then, the Auditor General said there was $15 billion in fraudulent and wrong payments that went out by the government, and the government says it is not worth even trying to collect on this.

Everybody increasingly believes that the federal government is broken because of the opioid overdose epidemic that is happening in many parts of this country. Only a couple of weeks ago, to the Prime Minister's surprise, the government suddenly found out that there was a permit granted to produce and distribute cocaine in British Columbia. Sadly, the leader of the party said today, very clearly, that it is easier to get a permit to distribute and produce cocaine in British Columbia than it is to get a passport. That speaks volumes about what Canadians are seeing these days.

After eight years, everything the federal government touches gets worse. There are more public servants than ever before. More money is being spent and allocated and promised, but the results are worse than ever. The Auditor General confirms the government spends more money and gets fewer results, so Canadians feel like things are broken because if this were any other business or any other way of life, those managers would have been fired a long time ago.

I want to follow up on how the City of Cornwall is unfortunately seeing how things are broken in our country these days. It is seeing Roxham Road and the national problem and challenge that we have faced of an unprecedented volume of irregular border crossings, with people seeking asylum and refugee status here in this country.

Thirty-four days ago, I put out a public statement because two large processing centres came into the community, but the Minister of Immigration did not say a word or acknowledge it. The minister provided zero consultation, zero heads-up and zero resources to help the City of Cornwall deal with this.

Cornwall is a welcoming community. We have seen the diversity, and we have seen the benefits of immigration over the course of the last couple of years. However, it has been 34 days, and it has been a couple of weeks since I asked my original question. We had a week and a half since IRCC officials came to Cornwall to hear first-hand how frustrated the city is by the poor communication, leadership and management around that.

From city council to provincial and federal officials, local charities, health and education, people are looking for a plan. After 34 days of this going public but months of the government's knowing the chaos and the confusion and the strain on local resources on the ground, they are looking for a plan.

They finally came down to Cornwall and listened, admitted their communication was poor and admitted that something needs to change. Months later, they are hearing the consultations. Having a meeting is not an outcome. They have heard the problem. The City of Cornwall and the stakeholders who want to help, who want to end this chaos and fix what the government has broken, want a plan. My repeated question and follow-up to the government tonight is this: What is the plan? What resources are we going to get to address the problem when it comes to the IRCC processing centre?

● (1855)

Mrs. Marie-France Lalonde (Parliamentary Secretary to the Minister of Immigration, Refugees and Citizenship, Lib.): Mr. Speaker, I want to thank the member for his advocacy.

Let me note what Canada is committed to. Canada is committed, through domestic law and international convention, to providing supports to individuals making an asylum claim. That is a fact.

We have a duty to protect the integrity of our borders and to manage resources on behalf of all Canadians. Let me be very clear: We continue to encourage asylum claimants to enter Canada through designated ports of entry, to apply through regular immigration streams and to make a claim of asylum in the first safe country they enter.

Canada is unfortunately not alone in facing a rising number of asylum claims. The world is facing an unparalleled flow of migrants and refugees, with the United Nations Refugee Agency reporting nearly 4.9 million asylum seekers in 2022. That is making Canada's share less than 1%. This is a global challenge driven by war, persecution, political and economic instability, and discrimination. Solving this challenge will require a global response.

In recent years, the majority of asylum claims in Canada have been made near Roxham Road, which is not a port of entry. In the summer of 2022, Quebec indicated that its social supports and housing system were hitting their maximum capacity, so our government began transferring asylum seekers who expressed an interest in travelling to Ontario or further west to other provinces. In February, when Quebec indicated that it could not take more asylum claimants, we supported transferring all asylum claimants to Ontario, and just recently began transferring them to hotels in the Atlantic provinces.

As of February, we have moved over 5,600 asylum seekers from Quebec to Ontario, Nova Scotia and New Brunswick. Our officials have been in contact with host communities, and IRCC is conducting community engagement in these provinces. We want to thank the communities and provinces that are receiving asylum claimants.

Canada's humanitarian efforts cannot fall on only one region or province. We continue to engage in discussions with provinces and municipalities that have expressed a willingness to accept additional transfers. I heard the member mention that Cornwall has accepted additional transfers. We know that the City of Cornwall in the member's riding wanted more communication, and we responded to that request. The associate deputy minister has been to Cornwall several times over the last few weeks, and the department is working with the community and local leadership.

We are very conscious of the potential impact that an influx of people could have on local resources, and we continue to listen and respond to local needs. The federal government has been providing supports to provinces and municipalities to respond to the rising number of asylum claims. Since 2017, we have provided $551.6 million to affected provinces and municipalities to address interim housing-related expenses for asylum seekers. In addition, since April 2020, IRCC has been providing temporary accommodations to asylum claimants who do not yet have private accommodations and who cannot go to provincial shelters due to capacity issues.

Our government has covered health care services and products, including immigration medical examinations, which also help connect claimants to the provincial health care system through a program called the interim federal health program. Where we can, we provide expedited work permits for claimants, and we continue to explore the possibilities of accelerating work permits so that claimants can work and support themselves.

In conclusion, the federal government continues to support the provinces and our communities and continues to listen and respond to their needs. We will continue to be there.

● (1900)

Mr. Eric Duncan: Mr. Speaker, in that four-minute response by the government, and after 34 days of going public with the problem of wanting a plan and resources, we got the same answer: It is listening, it is consulting and it is meeting. Having a meeting is not an outcome, but the Liberals could confirm and communicate that they acknowledge their shortcomings and acknowledge that communication was poor.

Most importantly, what the City of Cornwall and our community are asking for are proper resources. Some $16 million is what has been unveiled so far to go to DEV centre for its contract. We do not know about the former Ramada Inn property. There are tens of millions of dollars to go to those sites, and not a dollar can be allocated to local resources on the ground that could help end the chaos and act as a pinwheel. The IRCC and the minister need a plan to actually solve this chaos, not more meetings and conversations. We need a plan.

I will ask this again, and there is one minute for a response. Where is the plan and the timeline to fix what the government broke?

Mrs. Marie-France Lalonde: Mr. Speaker, again, I want to thank the member for his advocacy. Certainly, he and I have had a conversation in the last few weeks on this particular issue. Other members of the community have raised those concerns.

As I mentioned before, our assistant deputy minister has been in regular contact with city officials and individuals in our community. We are fully committed to help. That is what we have been doing since the process started. We have been working with local municipalities and have also engaged with others.

I want to reassure the member that, as we go forward, we are always going to engage with our partners, our local municipalities, which are so important.

CANNABIS

Mr. Scott Reid (Lanark—Frontenac—Kingston, CPC): Mr. Speaker, I want to tell a short story about the government's regulatory failure, which has cost constituents in my riding hundreds of well-paying jobs in the last month or so.

Until February 9 of this year, Canopy Growth, a licensed cannabis producer, was the largest private sector employer in my constituency. Based at the former Hershey chocolate factory in Smiths Falls, it has been transformed into a high-tech, legal, cannabis-producing facility. At the height of their operations, they employed about 1,800 people in Smiths Falls. However, last month Canopy announced the elimination of 350 jobs, 190 of which were to be cut immediately, and the rest to follow in the coming months. That was at the tail end of series of prior cuts.

Canopy will soon employ fewer than one-third the number of my constituents it once did. These job losses, to a large extent, can be laid at the foot of the government's failed policies. In 2018, the government, with great fanfare, legalized the sale and use of recreational cannabis. I voted for that.

We are just five years on, and the government's delivery on its plan, its crushing federal taxes and its insanely high regulatory compliance costs have allowed the illegal market to continue to flourish, and it is directly causing hundreds of Canadians to lose their jobs in my constituency alone. A month ago, the day after the job cuts in my riding were announced, I raised this point and the Parliamentary Secretary to the Minister of Innovation, Science and Industry stood to say that his government continues “to engage with stakeholders” and that they have recently funded a “strategy table” to “support dialogue”.

That is nice, I guess, but the government would have been better advised to have acted sooner, years sooner, on the advice it was getting from industry and stakeholders. The next best thing would have been to say it would act immediately. Saying that we will have more talks when the House is not nearly on fire but just about burned down is too late.

A multi-party group of parliamentarians with three Liberals, of which I am a member, has written numerous times to the Minister of Health. We wrote, as an example, about attempts to rationalize various regulations dealing with cannabis infusion beverages. It has inexplicably taken years for movement to occur on that one small issue. There are other issues by far that are much more important and there has been no movement on them. This long struggle for incremental microscopic improvements illustrates the problem the government has. On a macro level, it has failed to deliver on its promise of listening and creating a business-friendly environment for the cannabis industry.

I have mentioned the parliamentary secretary's response to my question from last month, and I am sure that tonight he will repeat at length the same kind of response. He will say that he regrets the job losses. He will say some industries face challenges, and that they want to listen to industry and stakeholders. I am sure he will be saying it honestly, but I truly hope that the government's speaker this evening will acknowledge that their ministers have been receiving advice from industry and stakeholders for years now. They could have acted upon it with far greater speed. If they had done so these jobs would still be in existence.

While there is still some hope that some jobs can be saved, and we will not lose the entire industry, perhaps the government could agree to move quickly on the recommendations that have been made by the legal cannabis industry, which would allow it to prosper and ensure that our industry does not remain 50% in the illegal sector, as it now is.

● (1905)

Mr. Andy Fillmore (Parliamentary Secretary to the Minister of Innovation, Science and Industry, Lib.): Mr. Speaker, I am happy to respond to the comments made by the member for Lanark—Frontenac—Kingston. He and I had occasion to work together on the Standing Committee on Procedure and House Affairs in the 42nd Parliament. I think we did good work there and I always appreciate his interventions.

In 2018, through the Cannabis Act, Canada made history and became the first major industrialized country to provide legal and regulated access to cannabis for non-medical purposes.

That act had three primary aims. The first was to prevent young people from accessing cannabis. The second was to protect public health and public safety by establishing product safety and product quality requirements and the third was to keep revenues from cannabis businesses out of the hands of criminals.

Since this bold and historic decision, the legal cannabis industry in Canada has grown rapidly and there is much to applaud. With over 900 licenced cultivators and processors of cannabis under the Cannabis Act and thousands of cannabis retail stores, the regulated cannabis industry is present coast to coast and has welcomed a tremendous number of new businesses.

In fact, the sector generates over $4.5 billion in sales and employs thousands of people.

The legal sector is successfully advancing the objectives of the Cannabis Act. The regulated market, based on the Statistics Canada household expenditure survey, is estimated to now represent approximately 70% of the total Canadian cannabis market. While views on that number may differ, it is clear that the illicit market share is diminishing.

Canadians are not only benefiting from having access to safe cannabis products but also benefiting from new business opportunities across the value chain, from cultivation to processing to research and testing and retail. Small and medium-sized enterprises continue to represent a greater and greater share of licence-holders and the market has continued to grow.

However, as we know well, this expansion is not without challenges. The sector is facing instability and uncertainty as it continues to mature. Our government recognizes how important the competitive and sustainable legal cannabis industry is to fully realizing the objectives of the Cannabis Act.

This is why, in budget 2022, our government announced a new cannabis strategy table, which the member has identified, that will support ongoing dialogue with businesses and stakeholders in the cannabis sector. It is an opportunity to identify ways to work together and to grow the legal cannabis sector in Canada. This commitment recognizes the economic and business realities that the sector is facing.

This initiative is led by the Department of Innovation, Science and Economic Development, which is actively engaging the cannabis industry and working with federal partners to ensure that the government is aware of and understands the issues at hand.

Further, in September 2022, the hon. Minister of Health and the hon. Minister of Mental Health and Addictions and Associate Minister of Health announced the launch of the legislative review of the Cannabis Act.

Early assessment of the act was always envisioned. This review will ensure that the flexible legislative framework set out in the act adapts and responds to ongoing and emerging needs and to make certain that the act best protects the health and safety of Canadians and provides for the establishment of a diverse and competitive legal industry.

Our government's commitment to Canadians and to achieving the objectives of the act, as set out in the act, are clear.

● (1910)

Mr. Scott Reid: Mr. Speaker, the fundamental problem is this: if the cost to produce and sell legal product is higher than the cost to produce and sell illegal product, then the illegal product will have the ability to drive out the legal product. This is exactly what is happening in the market today in Canada. There is some high-end product, which, I grant, the legal sector predominates in, but the fact is that, right now, it is a lot worse than a 70-30 split.

I have heard 60-40 and in some parts of the cannabis production industry, I would say it is 50-50 or worse.

One cannot impose massive regulatory compliance costs on the legal sector, which do not exist for the illegal sector, without having the effect of driving these producers out of business.

If there was some way of making the illegal producers stop, we would not have a problem, but that was never possible.

I ask again: what is the government doing to ensure that regulatory compliance costs are brought down and taxes are kept reasonable for legal producers?

Remember, illegal producers do not pay tax—

The Deputy Speaker: The hon. parliamentary secretary.

Mr. Andy Fillmore: Mr. Speaker, we have delivered on our promise to Canadians to establish a safe and legal cannabis sector in Canada. Our government remains committed to advancing the objectives set out within the Cannabis Act, including through the planned and launched legislative review of the act and the development of the budget 2022 announcement to establish the cannabis strategy, where the challenges that the member has identified will be aired and acted upon.

This table will provide new opportunities for government and industry to discuss the challenges and opportunities facing this relatively new sector as it continues to establish itself and find its footing as a sustainable alternative to the illicit market.

Our government has been and remains steadfast in its commitment to engage and work with industry while doing so and I extend that same offer to the member.

[*Translation*]

The Deputy Speaker: The motion that the House do now adjourn is deemed to have been adopted. Accordingly the House stands adjourned until tomorrow at 10 a.m. pursuant to Standing Order 24(1).

(The House adjourned at 7:13 p.m.)

CONTENTS

Monday, March 6, 2023

PRIVATE MEMBERS' BUSINESS

GOVERNMENT ORDERS

STATEMENTS BY MEMBERS

ORAL QUESTIONS

GOVERNMENT ORDERS

ROUTINE PROCEEDINGS

GOVERNMENT ORDERS

ADJOURNMENT PROCEEDINGS