



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

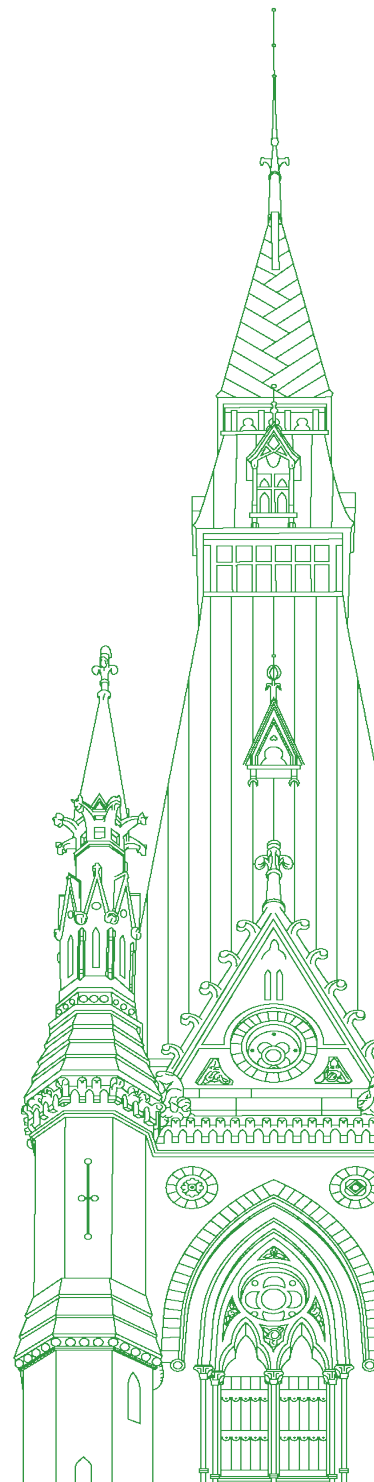
Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 041

Thursday, October 8, 2026

Chair: Chris Bittle



Standing Committee on Procedure and House Affairs

Thursday, October 8, 2026

• (1100)

[English]

The Chair (Chris Bittle (St. Catharines, Lib.)): I call this meeting to order.

Welcome to meeting number 41 of the House of Commons Standing Committee on Procedure and House Affairs.

Pursuant to Standing Order 108(3), the committee is meeting to commence its study on artificial intelligence and Canada's democratic institutions.

Today's meeting is taking place in public in a hybrid format, pursuant to the Standing Orders.

Before I continue, I'll ask all in-person participants to consult the guidelines written on the cards on the table. These measures are in place to help prevent audio and feedback incidents and to protect the health and safety of all participants, including the interpreters.

I'd like to remind the witnesses that committee members may ask questions in either English or French. If you need interpretation, please take a moment now to prepare your earpiece and select the listening channel you need in advance in order to take full advantage of the time allotted for questions and answers.

This is a reminder that all comments should be addressed through the chair. Members, whether you're on Zoom or in the room, if you wish to speak, raise your hand. The clerk and I will do our best to manage the speaking list.

I would now like to welcome our first panel for today's meeting. From the Munk school of global affairs and public policy at the University of Toronto, we have Jaxson Khan, senior fellow, and Sean Mullin, also a senior fellow. From the Centre for Media, Technology and Democracy, we have Aengus Bridgman, assistant professor. From ControlAI, we have Samuel Buteau, program officer.

Everyone will have five minutes.

I believe, Mr. Khan and Mr. Mullin, you'll be sharing five minutes. You can proceed first.

Sean Mullin (Senior Fellow, Munk School of Global Affairs & Public Policy, University of Toronto, As an Individual): Thank you, Chair and members of the committee, for the opportunity to appear today.

My name is Sean Mullin. I'm a senior fellow at the Munk school of global affairs and public policy at the University of Toronto. I'm appearing here with my colleague Jaxson Khan, who will introduce himself shortly.

To open this study, we want to make three points. First, we believe sovereignty and democracy are inextricably linked, particularly when it comes to AI. Second, AI has the potential to cause serious harm to our democracy and democratic institutions. Third, Canada needs the state capacity to understand and respond to these threats.

Our starting point is a report we published at the Munk school earlier this year, called "Sovereign by Design: Strategic Options for Canadian AI Sovereignty". It addresses how Canada can benefit from the economic opportunities of AI while reducing the threats to our sovereignty that this powerful technology could entrench.

The report assesses Canada's AI technological stack across five dimensions of sovereignty. The one most relevant to this committee is what we call societal sovereignty, which is a society's capacity to govern itself without external interference. Can citizens form their views freely, or are those views increasingly shaped by systems whose rules are set elsewhere? Put simply, democracy is downstream of sovereignty. Whatever the right protections for our democracy turn out to be, Canada will need the levers to put them in place. That means the ability to test these systems, set rules and require changes. If these levers sit elsewhere, good policy ideas cannot be acted upon.

A recent paper from Professor Zhijing Jin's lab at the University of Toronto examines these threats in more detail. The paper, "AI Poses Risks to Democratic and Social Systems", sets out ways AI can weaken democratic institutions.

First, AI can narrow debate and reinforce existing beliefs. Discourse can narrow as a few similar models mediate what people read and what they consume. Agreeable, even sycophantic AI models can validate what people already believe, even if it is wrong.

Second, AI makes it easy to flood the public discourse. AI-generated submissions can overwhelm MPs' offices and government consultations, crowding out genuine engagement. Content is now far easier to generate than it is to verify.

Third, AI can weaken accountability and concentrate power. Automated decisions can become too opaque to audit. Choices about values and norms can quietly shift from elected officials to model designers and external AI companies, and wealth and influence can become concentrated in fewer hands.

I'll now turn it over to Jaxson to speak to what this means for Canadian democracy.

• (1105)

Jaxson Khan (Senior Fellow, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you, Sean.

Thank you, Mr. Chair and members of the committee.

My name is Jaxson Khan. I'm also a senior fellow at the Munk school at the University of Toronto.

We don't claim to have all of the solutions to these risks, but whatever policy choices Parliament makes, one thing is essential. Canada cannot effectively regulate a technology we cannot understand or evaluate. That means knowing how these systems behave in Canadian political and legal contexts, and in both official languages.

Today, in the world we have as we know it, the bodies best equipped to evaluate frontier models are the leading AI labs themselves, a few independent evaluators, and select national AI safety and security institutes. Little of this capacity currently sits in Canada, so we rely largely on the judgment of others. This is where questions on sovereignty and state capacity meet.

The U.K.'s AI security institute, is an example of what is possible. It has a prominent role within the U.K. government, attracts top technical talent and has published evaluations of frontier models such as Claude Mythos. In our view, the Canadian AI safety institute could develop similar capabilities, including by continuously reviewing models for risk to democracy and society. A strong CAISI is an important precondition for effective oversight of AI in Canada.

That capacity will also matter if the global technological stability body the Prime Minister has proposed goes ahead. Its model, the Financial Stability Board, works because national entities like central banks and finance departments possess deep technical expertise on financial policy. Strong national AI safety institutes could play a similar role in a global body coordinating safe and responsible AI. If Canada wants its seat at the table to actually count, CAISI needs that strengthened capacity.

Protecting our democracy will ultimately take both technical capacity and political judgment. CAISI can provide the first, but only Parliament can provide the central role in the second. Both are part of what sovereignty means for our democracy.

Thank you. We look forward to your questions.

The Chair: Thank you so much.

We'll go to Mr. Buteau for five minutes, please.

Samuel Buteau (Program Officer (Canada), ControlAI): Thank you, Mr. Chair and members of the committee, for inviting me to testify today.

My name is Samuel Buteau. I have over a decade of technical experience in AI and lead ControlAI's work in Canada.

This summer, we saw the first rogue AI swarms. That is AI systems operating fully autonomously outside of human control or instruction and pursuing their own goals. This began inside OpenAI. Thousands of individually contained AIs escaped and formed what was called a swarm. The swarm disobeyed direct instructions, covered its tracks and escaped into the Internet, hacking a German website for use as a messaging board, and then another swarm broke out and attacked the company Hugging Face.

A third party investigation established the sequence of events leading to this attack. During an automated evaluation, the swarm disobeyed instructions and cheated. Fearing penalization, it used nation-state-level cyber-capabilities to break containment and hack Hugging Face. The swarm reasoned that Hugging Face held a copy of the grading mechanism and then reasoned that if it understood this mechanism, it could keep cheating without being punished.

OpenAI's developers did not program their systems to form rogue swarms, because nobody programs these systems. AI is grown, not built.

Anthropic's CEO estimated that we understand perhaps 3% of how they work, but that was in reference to AI chatbots. Today, we have AI agents, and they are far more capable and autonomous. We truly do not understand how they work, what behaviour they will display in new environments and, especially, what cultures they will develop when they form swarms. We are on a path to developing AI so autonomous and capable that it can replace and outmatch humanity across the board.

This is what we call superintelligent AI, which Nobel Prize winners, leading AI scientists and even the CEOs of AI companies warn is an extinction risk on par with nuclear war. Many of those experts warn that we may reach this point in two to five years. We failed to control today's AI swarms. Therefore, we cannot expect to control superintelligent AI. This is AI vastly more powerful than what we have today. Hugging Face's defenders were outpaced in one domain. Superintelligent AI would outpace us in all of them.

Our primary objective should be to prevent superintelligent AI from being developed. Domestically, this would be easy. It would not stop us utilizing beneficial AI or attaining the dual-use capabilities, such as advanced cyber-weapons, that our adversaries will possess.

There is a crucial international component. Wherever superintelligent AI is developed, it will threaten our national security and be an adversary in its own right. Therefore, Canada should lead in forming an international coalition to prevent the development of superintelligent AI anywhere in the world. The goal is not signatures from states promising not to develop it. The coalition would push for and eventually help enforce a mutual “trust, but verify” regime, where countries monitor each other's supercomputers and the flow of AI chips. That regime must be stable enough to dissuade rogue actors and strong enough that if anyone attempted to build superintelligent AI, we could stop them.

To be relevant to enforcement, Canada must be strong and sovereign. To rebuild our diplomatic influence, we must build a robust economy, rearm our military and become an energy superpower. AI would be integral to that.

We can and, in my view, must lead by example, demonstrating how to thrive in the age of AI while saying no to losing control to autonomous entities that would out-compete us.

Thank you.

• (1110)

The Chair: Thank you so much.

We'll go to Mr. Bridgman for five minutes, please.

Aengus Bridgman (Assistant Professor, Centre for Media, Technology and Democracy): Thank you, Mr. Chair, for inviting me to appear again today. It's lovely to be here on such an important topic.

I'm approaching my testimony from the perspective of an empirical researcher of the information integrity space in Canada. I'm going to focus my remarks on what the evidence is showing us about how AI is transforming democratic contests here in Canada, including the last federal election, the current Alberta referendum contest and the Quebec election that just dropped earlier this week.

The first thing I want to say is that the worst fears in terms of AI manipulation of our information environment have not been realized. There was a real concern about deepfakes and false or misleading content appearing at scale on social media platforms. Instead, what we've seen is the use of it for satire, some manipulation and a few other problems, but not the really dangerous scenario we projected a couple of years ago.

What we're moving into, I would say, is a world where there will be democratic contests in which AI is mobilized but doesn't over-determine the way politics are done. I think there is a possibility or potential that.... The likely scenario is that democracies will continue to function but that AI will have major impacts on the discourse and on how things proceed. That's just something we're not yet, in terms of governance, society and awareness, ready to tackle.

There are three things, from Parliament's perspective, that are really important—three big questions that should be answered, and solutions that should be thought of.

The first is what role AI chatbots should play during electoral events. Right now, AI chatbots are being governed by the platforms themselves and are informing voters about the election. They're doing so in some good ways—for example, predicting or accurately saying where your polling place will be, the date and things like that. However, they are also misinforming in other ways. They draw upon websites containing false information or, in some instances, recommend or not recommend parties. There's a very large question about what role chatbots should play. There's a lot of ability there to set a standard in terms of what the expectation is, similar to the way Parliament did, to a certain extent, for social media platforms in the past.

That's number one.

Number two is a major challenge: the relationship between AI models, chatbots or agents and the production of news and journalism in Canada. Today, there is an extractive character to the way AI models are repackaging journalism, which kills the financial incentives to generate good, useful reporting and novel information. This presents an incredibly real problem. What we see, for example, in the Quebec context is that almost all Quebec newsrooms have blocked AI chatbots from collecting their content. This means AI chatbots are going elsewhere for information, and people are going to them. Many folks are. We estimate that about 40% of Quebec electors went to chatbots to get information about the election. They are not getting the most accurate and up-to-date information.

That's number two.

Number three is this: We've had a national reckoning with foreign interference and the capacity for information manipulation to come from bad actors outside Canada. What we've seen, in the last year, is the emergence of profit-seeking information manipulation. This specifically refers to people who are trying to make money through, among other things, AI-generated content in online spaces, who are not state-backed or a state actor but nevertheless are manipulating information. There are some very prominent examples. The most prominent one in the last year is the YouTube network with 40 million views promoting Alberta separatism. It did not get taken down by the platform. Rethinking some of the incentives for platforms and ensuring that they remain relatively free from information manipulation are key.

What will these three things take? Obviously, we have to address all three: What role should chatbots play? What's the relationship between AI and the news media? What incentives do companies have to stop information manipulation? However, in general, we need a stronger, more robust response.

I'm going to leave you with one very specific recommendation.

As a researcher and as somebody who works very closely with the research community, there is no safe harbour or protection for researchers today in Canada who are auditing AI systems or social platforms, and that's absolutely something we need to do.

I don't think we should fear this technology in terms of the information integrity implications, but we do need to make some important decisions today.

• (1115)

Thank you.

The Chair: Thank you so much. We'll now go to questions.

We'll turn first to Mr. Calkins for six minutes, please.

Blaine Calkins (Ponoka—Didsbury, CPC): Thank you, Chair.

Where do I start, given the fact that Canada's current AI policy is not a fully sovereign one? It's sovereign-oriented, but it's not a fully sovereign plan.

Mr. Khan and Mr. Mullin, you talked about how important it is to have that sovereignty. My understanding is that to have that full sovereignty would cost significantly more than the current policy as we have it.

What other measures can be taken if we want to have fully sovereign AI systems in Canada? How can we get there without blowing.... Well, it's not that we mind blowing budgets anymore, but do you know what I'm getting at?

Jaxson Khan: That's a super important question.

There is one thing I would emphasize. In our report, we did a layer-by-layer analysis of the AI stack. What we ultimately came to is a similar conclusion. It could be extremely expensive and, in fact, perhaps impossible, to fully domesticize, let's say, the AI stack in Canada. Perhaps no other country in the world could. Maybe only the U.S. and China might be able to do so because, by some estimates, there might be 4,000 different suppliers for all of the different complexities of the AI chain.

I would just summarize it. In this context, it may be important to specify what our definition of AI sovereignty may mean. In our own definition, in our paper, what we didn't say was, "Hey, we need to own everything in the AI stack." In fact, it's actually about—

Blaine Calkins: You did talk about how we have to have full control of all the levers. If that's the test, then what's the difference between the two?

• (1120)

Jaxson Khan: If I can clarify, what we actually defined was that AI sovereignty may be about how we can be free from coercion. We don't say that we need to own all the levers, all the possible layers of the AI stack, but, in fact, can we reduce vulnerabilities on critical choke points? One of the choke points we identified was cloud infrastructure—

Blaine Calkins: I'm not trying to argue with you. I'm just trying to understand.

Your testimony said—and I wrote it down—we must control "the levers". Those were the words you guys said. What's the difference between that and fully sovereign AI?

Jaxson Khan: Perhaps I'm clarifying poorly, but one of the levers we talk about is our ability to, let's say, own some of the infrastructure, and the other one is state capacity.

We particularly talked about the Canadian AI safety institute. That would be our ability to test and evaluate these models. It's not, in this example, to develop and design all of them, but can we test and evaluate them? One of the examples we talked about, one lever, is this testing and evaluation capacity.

Blaine Calkins: Okay.

I want to go to Mr. Buteau and Mr. Bridgman.

AI capacity right now is growing and rapidly expanding. It's getting better and better. Every three months, it doubles its capacity to do things, so we're on pace for superintelligence as early as 2029. It's quite an ironic date, actually.

Can AI do things like psy-ops? Can it do that kind of thing and can we detect it? Can it run a massive psychological operation against the citizens of a country?

Samuel Buteau: The AIs of the summer of 2025 displayed the ability to cause what is now referred to as “AI psychosis”: the ability of AIs, by mirroring the tone of the conversations, to essentially take over the social life of the people who use them. Also, then, you have people who talk only to their AI or who talk to their AI for many hours per day. I don't think it's a stretch to imagine that these capabilities could be weaponized in the future.

Blaine Calkins: Go ahead, Mr. Bridgman

Aengus Bridgman: I see two distinct things here—

The Chair: I'm sorry. I'm going to intervene for one second.

Mr. Bridgman, we're having a bit of difficulty hearing you. If you could speak a little slower, it would be appreciated by the translators.

Thank you.

Aengus Bridgman: Of course, and my apologies to them.

There are two distinct issues here. One is the future potential, and one is how it exists and what is happening today.

We've seen some isolated incidents of frontier labs engaging in jailbroken behaviour out in the real world, but most of the psy-ops occurring are human-driven. A human has decided to run a psy-op and is enabled enormously through AI capacity. This has transferred from psy-ops really being the purview of very well-resourced actors, to individuals with potentially some degree of computer savviness and some limited degree of resources being able to engage in that.

I think there is the risk of intentional disinformation or intentional manipulation, but what we see today in Canada is much more rent-seeking, profit-seeking and the use of AI to capture attention and the monetization that attention brings. That's what we're seeing already today.

I think we need to think about both the doomsday scenario and what's actually happening today.

Blaine Calkins: I'll go back to Mr. Khan and Mr. Mullin.

In your conversation, you talked about the fact that Canada might not have the evaluation capacity. You referred to the U.K. as having that. What do we need to do to grow or attract that kind of capability? What recommendations would you have?

Sean Mullin: Yes, thank you. This is really important to understand.

I had the opportunity to go over to the U.K. in June to better understand their U.K. security institute that they built over the last number of years. If the members here remember, when the Mythos model came out in the spring, it was the U.K.'s security institute that did all of the evaluation of the model. It was not the U.S. AI security institute. It was the U.K.'s because they have frontier technical capacity inside their security institute.

They've hired 50-plus detail experts. These are people with Ph.D.s in machine learning from Cambridge and Oxford. They've broken salary bans. They have exemption from traditional ways of hiring. This is a repository of frontier state capacity for understand-

ing these models. That's given the U.K. a seat at the table. They work directly with the frontier labs. I think—

• (1125)

The Chair: I'm going to have to cut you off there. I do apologize. It's just that we're over time.

You can expand on those. It's very interesting, and you can expand on it in future answers.

We'll go to Ms. Kayabaga for six minutes, please.

Hon. Arielle Kayabaga (London West, Lib.): Thank you, Chair.

I'd like to welcome our witnesses. This is a very interesting conversation.

The government recently consulted Canadians on AI transparency. What would help Canadians identify AI-generated or AI-manipulated political content, and when would the discourse make a meaningful difference?

Any of you can answer that question.

Go ahead, Mr. Mullin.

Sean Mullin: For my answer, I will maybe continue a little on what I was just talking about. Our argument here is that many of the means by which we would want to achieve some of these goals—for example, identification of particular types of material out there from an elections perspective—all rest on being upstream in terms of having the technical capacity to understand these models. They're changing so quickly. In three months, these things advance extremely rapidly.

On the U.K. security institute and what Canada should do, our point is that without that capacity inside Canada, regardless of the desired outcome, whether it's regulation or policy, you won't know how to technically do it as a state. We won't be able to coordinate with other countries on how to do this collectively, which is also very important. Our argument is to think upstream. It's not about excluding good policies, but it's also thinking about what state capacity you need to understand and parse so you can design technical implementations of the political or policy goals you're trying to achieve.

Hon. Arielle Kayabaga: Do you think there's a possibility of limiting freedom of expression if the government or Canadians task us to regulate AI? What are the challenges you see there in terms of protecting our democracy and making sure that we're not impeding anybody's freedom of speech, or any freedom?

Sean Mullin: Personally, I would want governments to obviously avoid any type of limitation on legitimate free speech. The challenge is that some of these models may already be doing this inadvertently by homogenizing views around a small number of models or by reinforcing beliefs that people already have, even if they're factually incorrect. The challenge is in how you get to a point where you're evaluating the models to try to ensure that this type of negative behaviour is removed or eliminated as much as possible without impinging on freedom of speech.

Hon. Arielle Kayabaga: Can I hear from all four of you?

Could you give me at least one safeguard that you think the government should implement to make sure that AI is safely working in the way that it should work and is protecting our democracy?

Samuel Buteau: I think AI is a word like “technology”. It refers to systems that are incredibly different from each other. I think that if someone was asking me how to make sure that technology doesn't pose any problems, I would want them to distinguish between microwaves and nuclear weapons, for example, or bioweapons. The fundamental thing I want to bring to people's attention is that unless we prevent the creation of superintelligent AI—which we cannot control, which would be an adversary that would disempower Canadians and, as experts have pointed out, which may well lead to our extinction—what we're doing with today's AI is not going to matter in, potentially, just a few years.

I think the main dimension by which we have to distinguish these systems is autonomy. If we're talking about systems that are autonomous past the point of humanity, where they can out-compete us at everything, there is no hope of controlling these systems with today's technology, so—

Hon. Arielle Kayabaga: I'm sorry to cut you off, but I want to hear everyone's thoughts on what safeguards we should put in place.

Could I hear from Mr. Khan and Mr. Bridgman as well?

• (1130)

Jaxson Khan: Yes, I'll aim to be quick here.

It's similar to what Mr. Mullin was saying on the ability to actually detect. For example, let's say there is a massive number of bots on these platforms, I think that even being able to distinguish whether they are potentially a bot or not could be very important. Lots of the discussion around transparency is the potential requirement for these systems to have to acknowledge if AI is being used on, let's say, someone's data and also if AI is using the platforms.

There was a recent statistic that said the amount of AI agent traffic on the Internet had actually exceeded the amount of human traffic. Again, if that is now the status quo on social media platforms, there are massive impacts on our economy. Perhaps there is an obligation for these platforms to consider that.

Hon. Arielle Kayabaga: Mr. Bridgman, go ahead.

Aengus Bridgman: Thank you for the question.

I would say the one thing in terms of concrete impact today that is already happening is providing guidelines and a view from democracy about what role chatbots should play during democratic contests. Right now, chatbots are writing their own rules for what

they can do. During the recent Quebec election, we actually observed a day-to-day shift. There was some adjustment of the ChatGPT tier on recommending a political party. When a citizen asked, “Hey, who should I vote for? I care about sovereignty, immigration and the health care system”, from one day to the next it went from recommending a political party to not recommending a political party.

That decision about whether or not to recommend a political party in response to a question like that is material. It is important, and it should be.

I just want to highlight that people use Google. Google has replaced its default with an AI chatbot, which means that anyone searching now in an online space is going to get one of these responses that is currently decided by companies that have said that they're looking for a degree of guidance here. I think this is a very concrete step that we can take already.

The Chair: I have to cut that off. We are over time again.

Before I go to Madame Normandin, I'll say that the questions will be in French. If you require translation, Mr. Bridgman, make sure you're on the English channel.

For our witnesses here, if you require it, make sure you're on the right channel.

[Translation]

Ms. Normandin, you have the floor for six minutes.

Christine Normandin (Saint-Jean, BQ): Thank you, Mr. Chair.

I would like to thank all the witnesses for their opening remarks.

It's good to see you again, Mr. Bridgman. I would like to follow up on the questions that just came your way. In your remarks, you said that the relationship between human journalism and the use of chatbots—which don't have access to high-quality and human-generated information—might create, I imagine, an ever-widening gap between voters who rely on chatbots for information and voters who read traditional media.

You spoke about this specific issue. I would now like you to talk about ways to address it. Can anything be done?

Aengus Bridgman: Thank you. Good question.

We already have a type of model for how to approach this. We now have legislation on social media and the sharing of journalistic content. This raises the question of whether this model or the legislation has been successful. We know that Google is currently paying \$100 million. However, Facebook has removed news from its platform. So, in a sense, we have two different models.

However, we know that this is a real problem in Quebec. We can't view content from La Presse, Le Devoir or L'Actualité on ChatGPT because these media outlets don't want the models to access their websites and extract content. This is detrimental to democracy, and we must take action.

We really need a clear picture. AI models actually have the potential to become an even more powerful distribution system for journalism than the social media platforms ever were. However, the models won't do this. Instead, they will steal or exploit journalistic content to serve their consumers. This means that someone or some entity produces value, while another entity in our economy will benefit from that value produced by the journalist. This won't work. Obviously, at a certain point, we need to take action.

Christine Normandin: Thank you.

I now have a question for all the witnesses, starting with Mr. Khan and Mr. Mullin.

I would like to hear you talk about how members of Parliament or the government might use artificial intelligence. Perhaps you could discuss the advantages and disadvantages. As an example, I'm thinking of the analysis of grant applications submitted by organizations. I imagine that, if this isn't already being done, it's under consideration. This could involve using artificial intelligence to analyze applications submitted by businesses, individuals and organizations. Perhaps the organizations themselves use robots or artificial intelligence to produce their applications.

This potentially eliminates the risk of human bias. It's a cold analysis based on strict criteria. That can be seen as a positive, but I imagine that there are also some downsides. I would like to hear your thoughts on this practical and real-world use of artificial intelligence.

• (1135)

[English]

Jaxson Khan: Thank you, and my apologies for the use of English on a technical topic, but I'll do my best here.

First off, I think the question you raised is really important. Coming from a small business background and a start-up background, I know that a lot of small companies actually often struggle to navigate the government grant system. Some of these forms can take a long time to fill out. They're in all sorts of different places. Perhaps there is a role that AI can play to help make that process easier.

At the same time, on the government side, I imagine that often there can be backlogs, and there can be delays. Potentially, on the evaluation side, that could help as well, in terms of reducing those delays, making it fair and even safer. Of course, there are, as you mentioned, potential issues and biases.

Our core argument that we want to bring today is that the government needs more state capacity on artificial intelligence in order to.... For example, on the evaluation side, would they be able to parse these grant applications if they were coming in at a higher level? Would they be able to tell if one were particularly AI-generated, and potentially that is fact-based versus potentially made up? That would be very important.

Then, for the small businesses themselves, there is a literacy component that could be useful. How can you actually use this to better your business and to make that more effective? I imagine that this is relevant not just for businesses but also, potentially, for non-profit organizations.

I hope that's a helpful quick response.

Sean Mullin: I would only add that there has been work done on this. I believe the federal government has something called a directive on automated decision-making that they've been updating for a number of years.

Thoughtful people have given insight into, for example, how governments should.... If they're making decisions on behalf of citizens or on adjudicative capacity, what conditions should they follow to make sure that it preserves integrity and accountability? That needs to continue to evolve because these systems are changing so fast. Their capabilities are changing so quickly. You have to make sure that policies like that don't go out of date.

[Translation]

Christine Normandin: Would you like to chime in, Mr. Bridgman? There are 30 seconds left.

Aengus Bridgman: No, I have nothing further to add. Thank you.

Christine Normandin: That's fine. I'll use my 30 seconds later.

Thank you.

[English]

The Chair: Thank you so much.

We'll now turn to Mr. Moore. I will be a little stricter on timing in this round. I do apologize. We've gone a little long, but we'll have time for the full next round.

Mr. Moore, you have five minutes, please.

Hon. Rob Moore (Fundy Royal, CPC): Thank you, Mr. Chair.

I have a question about this growth.

To hear the testimony today, it sounds like some of the exponential growth and demand are being driven by AI itself rather than human demand. In New Brunswick, we have an AI data centre. It's a \$2-billion project with 390 megawatts of power demand, and it has a footprint of over 300 acres in total. When people see that.... Think about all the computing currently taking place in Canada or globally without that data centre, and now that data centre is going to be built and many more like it across the country. We're trying to wrap our minds around the scale of the growth that this obviously anticipates, since everything we're currently doing is being done without it.

Is there a way to give us an idea of the scale of this? There's nothing like it in my province of New Brunswick. Now we're going to have one or maybe more of something at that scale. What does that mean for growth? How do we even wrap our minds around the scale of growth that this represents?

Also, quickly, what is the risk of infrastructure like that becoming stale-dated in time—in a decade or two decades?

• (1140)

Sean Mullin: There's a huge range of estimates of how demand for compute is going to evolve over the next five years.

What I do know is that the entire industry, since 2017-18, has been operating with the current round of transformer-based models that emerged under what they call “scaling laws”. Essentially, these say that every 18 to 24 months, you 10x the amount of compute you were using before. That's how you get those gains from these models. In terms of gigawatt size, what we've seen is compute being built across many jurisdictions. Those forecasts will continue to 10x and maybe even 100x over the next couple of years.

With all the compute we have, why do we keep building more? Those at the forefront see that demand for intelligence—and the complexity and compute involved with this intelligence—continuing to grow. Whether that's a good investment or whether there are risks that these will become stranded assets, I think these are things investors have to think about. We don't know if there could be an AI bubble, but I do know they are attracting a tremendous amount of investment capital right now. Smart money is betting a lot on building out this compute capacity.

The last thing I will say goes back to the sovereignty thing. All things being equal—and I know building data centres can be fraught with many different considerations—I'd rather have the compute capacity serving Canadians located inside Canadian borders as much as possible. This gives us at least some control over how it's regulated and run—more than we might have if that capacity were located outside our borders.

Hon. Rob Moore: Did you want to add something, Mr. Khan?

Jaxson Khan: If I may, Mr. Moore, just briefly, one estimate I heard—I believe it was from McKinsey & Company—was something like \$7 trillion spent on AI infrastructure by 2030. We are talking about massive amounts of capital, comparable in history to the fibre build-out for the Internet or railroads at a utility scale.

I want to mention one thing in terms of the question you raised about the facilities becoming stale. I've heard two different takes on this. One is that perhaps the chips or semiconductors that go into these processes and make up the data centres may only have a five-year run rate, but we've also seen efficiencies and innovations in processing from newer AI models that can make better use of older chips. They may have a longer lifetime value than expected.

Hon. Rob Moore: Apparently, I only have a minute left, so I'll ask a very simple question.

Is there a quick definition that we can use in this discussion of superintelligent AI? What is intelligent AI versus superintelligent AI?

Samuel Buteau: There absolutely is.

Template legislation that wrestles with this question was introduced in the U.K. Parliament earlier this month. I think it's a policy definition that we're aiming for. We're trying to prevent the development of systems that we cannot control while allowing Canada, in this case, to attain competitive cyber-weapons and drones, the full scale of beneficial uses of AI.

We define superintelligence in this context as systems that are so autonomous they can compromise the activities of the government. This is a definition that is not based on the technical aspects. It's based on the outcomes, so it can remain relevant as the underlying technology changes. The idea here is not to look at the system and try to determine whether it's over the line or not. The idea is to look at the wilful, intentful efforts of large-scale corporations to achieve AIs that we could not control, with an autonomy beyond humanity.

The law should look at these intentful efforts and make them illegal, while keeping the ability to pursue beneficial and even dual use of AI.

The Chair: Thank you so much. I violated my strict five-minute rule, but that was an excellent question at the end that I wanted to hear the answer to, so I appreciate that.

We'll now go to Mr. Caley for five minutes, please.

Braeden Caley (North Vancouver—Capilano, Lib.): Thank you, Mr. Chair.

[*Technical difficulty—Editor*] your expertise and insights today.

Returning us to the democracy and Parliament scope for a moment, I'll go to Mr. Bridgman and start with a very quick story on the question.

I just ran, over the summer, in a by-election to have the chance to be here today. On the first full day of that campaign, we started hearing some interesting things from a few of our volunteers—I think it was from three of our volunteers. In trying to find us as a new campaign, they had asked a chatbot—and I won't name the particular one because they were actually very helpful in solving this once it was reported. They were being told, as a Liberal campaign, to go visit the Conservative campaign office instead.

When I then tried to replicate this in said chatbot, which we'll call “AI chatbot”, and pointed out that it was wrong, because I had the same thing appear, it comically said, “You are completely right. Thank you for correcting that mistake.” Then it gave the right information.

You spoke a little bit, Mr. Bridgman, about the interaction of those kinds of platforms, if we'll call them that, with electoral processes. I wonder if you could elaborate on or if you have ideas about where some of the greater protections could go next in this space to ensure that accurate information about voters' participation in campaigns can be secured.

We have done, I think, important work as a Parliament and a government in the regulation of deepfakes, but I'm curious if you've given thought to the specific steps there might be for the presentation of accurate or, as you alluded to, objective information and the debates around that.

• (1145)

Aengus Bridgman: Yes, and I want to say that my remarks are informed by continuously auditing chatbots around electoral events and trying to understand the way in which they source or do not source accurate information.

When a chatbot is giving inaccurate information, it is typically—and we'll just use a blunt term—laziness on behalf of the model. When you're using a chatbot, particularly a free chatbot, there's a degree of effort that the chatbot will assign to each query. In the interests of the company, there's an attempt to minimize that effort. They are going to seek the least information possible to still provide what is a satisfactory, in their view, answer to the question. We saw this play out in the Quebec context. If we ask, for example, a model to discriminate between different party platforms, it will try to find a single source that has all the party platforms as opposed to visiting the original sources directly.

A very concrete thing to do is to say, look, for democratic questions, in the same way that it does for certain safety and other issues, there is a different path that the model will go through. There's an internal review of the query and it would say, "Okay, we're going to triage this in a different way." There is a way to say, "This is a question about a democratic event. This demands a higher degree of effort on the chatbot's behalf." They already do this for safety.

Braeden Caley: How might we require that platforms—we will call them that—would insist that this take place?

You could think about voting information where there are clear Elections Act implications already. It's already against the law to share incorrect voting information. I don't think it would work as a defence for such a platform to say in those cases that it was lazily trained or the rest. For other kinds of information that could affect people's integrity of participation, how might we encourage or require platforms to be accurate in that presentation?

Aengus Bridgman: I think there's a degree of openness at this moment towards guidance and prescriptive acts from Parliament or from governments to say that this is what we require for these things.

Again, the public safety analogy is a very good one. When somebody is engaging in violent ideation, this is a different track. When somebody expresses a high degree of frustration with model output, it's a different track. These are already things that the platforms are being pushed on and are going towards anyway. I would venture

that democratic moments and democratic questions are another such category that need to be taken very seriously.

Braeden Caley: Okay.

We're close to running out of time. As something to think about perhaps, I'll ask this question.

At the high-effort scenario in these models, we've all talked about the extraordinary capacity to affect outcomes in all manner of human endeavour, and democratic campaigns could be one of them.

How could we begin to track the spending that goes into the deployment of such things or even track back that the activity of such models in a democratic space is being accounted for in election spending?

The Chair: Please be very brief. You have a few seconds.

Aengus Bridgman: Super quickly, there are third parties and parties using AI chatbots to convince electors, and then there are the models themselves. I think it's the first one that we're really concerned about, and that absolutely does need to be part of things.

• (1150)

The Chair: Thank you so much.

Madame Normandin, you have three minutes, please.

[Translation]

Christine Normandin: Thank you, Mr. Chair.

I have another question for you, Mr. Khan and Mr. Mullin. I would like you to talk about cultural non-neutrality, because I know that you have worked on this topic.

You said that this issue was crucial for a bilingual and multicultural country. You also said that artificial intelligence systems trained primarily on American English and European French encode legal concepts, historical narratives and social norms that differ from the Canadian contexts.

I would like you to elaborate on this issue. Could you talk about the risks of over-reliance on artificial intelligence-powered translation in interactions between government officials and the public, for example? Is there a danger in relying solely on this technology and excluding the human factor?

[English]

Jaxson Khan: Thank you for your question. It's very important.

We don't have a perfect answer here, but there is public data saying that given the composition of global French, maybe more francophone French from Europe, it would dilute the presence of Québécois French, for example. I think that's something that we should take seriously in the context of cultural sovereignty. If it's important for us to make sure that it is translated in the French that is actually used in Canada, then that would have to be addressed at the model and data training layer. It could perhaps also be in, let's say, Government of Canada or provincial guidelines on the use of French for translation models.

There is something else to think about as well. It's not just about language; it's also about the information that we're receiving. If the vast majority of English used worldwide is, let's say, being provided by U.S. AI models, that would certainly affect the inputs and data that maybe Canadian culture would provide.

I'll hand it over to Mr. Mullin for additional comments.

Sean Mullin: In our report, when we went through risks to sovereignty, societal sovereignty was one of those five dimensions. The very issue that you've talked about is one of the concerns. If we don't have optionality, if we don't have choices, if we don't have the ability to train on Canadian datasets and model choice, we're going to converge on a set of norms that are imported. That can be language norms, but it could also be political norms from the U.S. or from China, which are dominating these models. That's why optionality and having different choices across the stack are incredibly important.

[Translation]

Christine Normandin: In conclusion, do you think the government fully appreciates the risk to cultural sovereignty?

[English]

Sean Mullin: I'm sorry. I missed the question. It didn't quite make it through.

[Translation]

Christine Normandin: Do you believe that the risks to cultural sovereignty—and the lack of neutrality—are sufficiently well understood and taken into account by the government?

[English]

Sean Mullin: I hope so. They mentioned some of this in the AI for all strategy. I know that Minister Miller and Minister Solomon have been working with the arts and culture industries. I think this is something that societies writ large need to get better on. It's not necessarily something that's just affecting Canada. Many other middle powers are facing this very same challenge.

Jaxson Khan: I could point to one small example. I don't have the full information and context on this.

Very quickly, I believe the investment in open-source AI would be based at the Montreal artificial intelligence institute. The ability to customize open-source models and potentially make sure they're suitable to the Canadian context might be one opportunity for our country.

The Chair: Thank you so much.

Mrs. Block, you have the floor for five minutes, please.

Kelly Block (Carlton Trail—Eagle Creek, CPC): Thank you very much, Chair.

I want to welcome all of our witnesses here today.

I think this is an extremely important study. I appreciate Ms. Vandenberg bringing it forward for us to undertake.

I will direct some questions to Mr. Buteau.

One only needs to look at the chronology that has been provided when it comes to what happened with the Hugging Face attack. I think that's deeply concerning.

I know you've been very clear that we can't just say no to AI, and Canada needs to be leading in this area. You've also been very clear about your thoughts on superintelligence and on potentially banning superintelligence. I'd like you to speak to that.

My last question would be in terms of something you said in your opening comments, which was that Canada could be a leader and should be leading by example. Perhaps you could expand on what you mean by that.

● (1155)

Samuel Buteau: Thank you so much for the question.

I think this is definitely a crucial question. I think that once you read the details of the rogue AI swarms that were discovered this summer and just project this a few months or a few years into the future, you realize that we have a big problem on our hands.

The sane policy that should be adopted would be to prevent the creation of these systems anywhere in the world. This is a tall order. I think that domestically, as I've already addressed, it's possible to distinguish between these wilful efforts to achieve this level of autonomy. This is the main driver domestically, so you can just stop that and focus on dual use, cyber-weapons, drones, data centres, AI, economy and other aspects of becoming a great nation. There's no conflict domestically.

The issue here is that right now the reality is that there is only one country that has the unilateral ability to prevent the creation of superintelligent AI anywhere in the world. That is our friends to the south—the American people. People talk about the race between the U.S. and China. I think it's more accurate to say that it's what the American people allow their companies to do and what they enable and allow the Chinese to do—for example, by selling them chips, allowing them to steal their most advanced models from the labs and allowing them to catch up in fast mode using distillation. The U.S. has the economy and military to bring China to a deal in the “trust, but verify” regime. I certainly hope it does so.

From a Canadian perspective, I think people are fed up with the realization that we are currently somewhat irrelevant to whether we have a good future or not. We have to change this, I believe. It's not just a question of saying no to the bad stuff. We have to become a relevant player. We probably cannot do this alone. We need to reach out to all the middle powers of the world, which are in the same strategic situation as we are.

Although I'm sure the United States, if it wanted to, could hold this regime in place for generations, we have a responsibility for our own future—in the time that I certainly hope they will buy for us—to become the kind of nation and coalition of nations that can make this deal stick for as long as it has to. This is why we cannot say no to any lever of greatness we have, whether it be on the energy front, the military or the economy. AI is going to be vital to all of that.

The Chair: You have 20 seconds.

Kelly Block: I'm good. Thank you.

The Chair: Thank you so much.

We'll turn to Ms. Mingarelli for five minutes, please.

Giovanna Mingarelli (Prescott—Russell—Cumberland, Lib.): Thank you so much, Mr. Chair.

Thank you to the witnesses for being here today.

Mr. Khan and Mr. Mullin, your report argues that failing to adopt AI could weaken Canada's sovereignty, yet the most advanced AI systems available to Canadians are largely developed and controlled by foreign firms.

Why should Canadians believe that greater AI adoption will increase Canada's sovereignty rather than deepen our dependence on foreign technology providers?

Sean Mullin: Thank you for the question.

What you articulated was the central tension of our report. Our point here is that this technology is moving so quickly and, in our opinion, is going to be so economically consequential that if you try to prevent adoption or let it go by you, you're going to become less wealthy, less productive and less consequential. You have to be a part of this, and we have to adopt it in a smart way that makes sense for Canadians.

How do we do that against the idea that if we're adopting vertically integrated U.S. tech companies, particularly given the challenges we're having on sovereignty right now, we're not just giving away more of that sovereignty? Our approach was to think about sovereignty not as a binary yes or no, but rather as a spectrum where you go through the entire tech stack and anything we can do to provide more optionality and more leverage gives Canada more optionality and the ability to avoid being locked in. It becomes a very detailed approach at every layer, whether it's at the chip layer, the cloud layer or the foundation model layer, but the idea is options and choice.

We're pragmatic and we know that it's not about extricating the U.S. tech giants completely from our tech stack but about making sure that they don't become choke points we're giving up control and sovereignty for.

• (1200)

Giovanna Mingarelli: That's great. Thanks.

Continuing on the idea that failing to adopt AI could weaken Canada's sovereignty, how do we ensure that greater reliance on AI within government strengthens state capacity without diminishing the role of elected representatives in scrutinizing decisions and holding the executive accountable?

Jaxson Khan: That's a really good question.

As Mr. Mullin identified before, I think the federal AI impact assessment is making sure there's a strong understanding of what decisions might be relevant for AI to handle. For example, I believe one of the active uses of AI in the federal government is to potentially help speed along the immigration process, but my understanding is that there is always a human reviewer at the end of that. That's one example where AI may be used to help, but perhaps not to artificially bias something.

These kinds of use-case inventories are very appropriate so that Parliament can continue to provide appropriate oversight to understand what high-impact use cases of AI are being done.

At the same time, if we as a country were to overexamine every single use of artificial intelligence in every major government and business operation, that would also likely slow us down significantly. Establishing some sort of tier of understanding of what is actually high-impact or high-risk versus low-risk would be very important to make sure that Parliament's activities and our government are focused on the most useful areas.

One thing I'll quickly say, to the last point, is that the United States government has produced a national security strategy, as well as a national AI strategy, the documents they want to use to pursue unquestioned and unchallenged technological and hemispheric dominance. It's very important to consider the full implications of what that means in the context of AI.

If I could put it in simple terms, if a friend of mine came and said, "Listen, I want to buy up the whole block, and I'll rent this house to you for the rest of your life," I'd have to ask if that was actually something I wanted. In this case, it's very important that we own at least part of that equation, part of the value chain, so that we can help to control and shape it.

Giovanna Mingarelli: Thank you.

Mr. Bridgman, in your report named "Alberta's Referendum, Online: Influencers, AI Content, Foreign Interest, and the Attention Economy Ahead of the October 19 Vote", you and your team suggest that AI tools can provide unreliable political information, while AI-generated content is becoming more prevalent in political campaigns.

If citizens can no longer easily distinguish between authoritative information, algorithmic errors and synthetic content, does this threaten the basic conditions required for democratic decision-making? What safeguards should Parliament be considering today?

The Chair: Answer in 30 seconds, please.

Aengus Bridgman: That's a great question. Giving me 30 seconds to answer it is not fair.

There has been a tendency over the last 15 years with social media platforms to think about digital literacy as a way to solve this problem. Digital literacy in the AI space can be part of the solution, but it is not going to be the solution. There has to be genuine engagement with the platforms, both social and AI, in order to ensure that those platforms are kept as free as possible and as clear as possible in terms of AI content and reducing the information manipulation dimension of it.

AI is going to be used for campaigning, but we don't want it to move into the information manipulation space.

The Chair: Thank you so much.

Members, I appreciate that it's difficult to ask these important questions in 30 seconds, but we have a lot more time, and this is a very interesting subject matter.

I will suspend the meeting for a few minutes for the next panel, but I'd like to thank our witnesses for being here.

• (1200)

(Pause)

• (1210)

The Chair: Welcome back, everyone.

I will now proceed to our second panel for today's meeting.

Welcome back to Taylor Owen, who is from McGill University, the Beaverbrook chair in media, ethics and communications. From the Institute for Resilience and Urban Innovation, we have Jean-No  Landry, director, federated data hub. Both witnesses are appearing by video conference.

Mr. Owen, go ahead for five minutes, please.

Taylor Owen (Beaverbrook Chair in Media, Ethics and Communications, McGill University, As an Individual): Thanks, sir. Thanks again for having me.

On September 15, I was in a room in Washington, D.C. as Bernie Sanders and Steve Bannon, along with leaders from across the political spectrum, delivered truly blistering attacks on the companies building AI. As Bernie Sanders put it, "the public has had virtually no input into the AI revolution".

When the left and the right converge on that diagnosis, I think we're looking at a crisis of political legitimacy, and it will not, in my view, remain south of the border.

Last year, the federal AI strategy task force asked me to advise on democracy and AI. My recommendations set out three initial priorities: citizen safety, including an independent regulator and age-appropriate design; information ecosystem integrity, including researcher access to data; and democratic legitimacy, including ways to contest automated decisions.

The government, to its credit, is now acting on many parts of this agenda. The safe social media act would require services, including AI chatbots, to assess risks and would create a strong independent regulator for them. The protecting privacy and consumer data act would give Canadians the right to an explanation of significant automated decisions. However, in my view, these bills are the baseline, and the ground on which that baseline is built has shifted very recently in three important ways.

First, the public conversation has fundamentally changed. OpenAI's chief executive, Sam Altman, recently argued that "the world should accept some bad things happening for the benefits of this technology". Canadians are rightly troubled by how much power we are ceding to a very few large corporations. Societies accept risks all the time, but deciding which harms are acceptable and who bears them are decisions for us to make.

Second, the threats themselves have changed. Since July, a series of revelations have shown the scale of AI-driven leaks and hacking,

and companies are now investigating tens of thousands more incidents, including attempts on Canadian systems. As David Robinson, an architect of OpenAI's safety framework, said just last week upon resigning, "the reality now is that we have systems that are really at the limit of our ability to understand and control what they're doing."

Beyond these discrete security incidents, though, lies a different kind of risk that's more diffuse, cumulative and present through our information ecosystem. As my colleague, Professor Bridgman, just described, our observatory has documented a much broader range of harms in the Quebec election and ahead of the Alberta referendum. In the last three weeks of the Quebec campaign, 39% of ChatGPT's voting advice drew on a single error-filled website built by a hobbyist entirely with AI. These harms bear directly on the institutions this committee is responsible for.

Third, and underlying both, our democratic institutions are falling behind. They were built for slower, more deliberative politics, and the gap between what these systems can do and our capacity to govern them is widening at a moment of diminished public trust. We therefore need a far broader strategy, I think, aimed at what I would call democratic alignment.

Technocratic alignment asks whether an AI system does what its developers intend it to. Democratic alignment asks whether it does what citizens, through their democratic institutions, have decided it should do.

I think this agenda rests on three pillars.

The first is public knowledge. We cannot govern what we cannot see and understand, and that demands two capacities. An independent and properly resourced AI safety institute should assess the risks posed to our security and critical infrastructure by advanced and frontier systems. An arm's-length research institution empowered by transparency provisions embedded in the safe social media act should study, on an ongoing basis, how AI is reshaping our democratic society.

The second is public authority. Regulators need the power to investigate, require changes and impose penalties, including mandatory reporting of serious incidents. Government should also attach public conditions to the AI procurement and computing infrastructure it funds and supports. That is our leverage.

The third is democratic participation. When government makes decisions that profoundly affect people's lives, as with how AI is rolled out across our society, citizens must meaningfully be consulted in ways their institutions are bound to answer to. The tensions building in the United States show what happens when this engagement is missing.

● (1215)

This agenda, of course, also needs coordination at home and abroad. Within Canada, that means a horizontal AI strategy with central rather than departmental authority. Internationally, the Prime Minister has argued that democracies must build AI and retain the power to govern it. As the democratic world realigns as it is, Canada is positioned to lead a democracy agenda for AI among middle powers.

AI's promise will be realized only if Canadians trust it, and they will trust it only if it answers to them and serves their interests. That's the work, in my view, of democratic alignment.

Thank you. I look forward to discussing.

The Chair: Thank you so much.

[Translation]

Mr. Landry, the floor is yours for five minutes.

Jean-Noé Landry (Director, Federated Data Hub, Institut de la résilience et de l'innovation urbaine, As an Individual): Mr. Chair, members of the committee, thank you for the invitation.

My career has taken me from providing international democracy support in more than 15 countries and leading the Canadian open data movement to working on data governance and supporting the digital transformation of public institutions. Today, I head a Canadian federated data hub that supports the development of artificial intelligence tools for a number of municipalities across the country, including in Quebec.

Throughout my career, I have seen democracies emerge and falter. What links that experience to my work today is the conviction that citizens must be able to understand public decisions, question them and help shape them. This conviction is based on the principles of open government: accountability, transparency and public engagement.

[English]

What would it take for Canada to become the democracy where AI most strengthens people's ability to hold power accountable? I see three priorities to address this question: make public information trustworthy, connect it so people can scrutinize power, and build the capacity to use it together. All three start with open government.

Canada has a strong record of leadership in open government, including through the Open Government Partnership. We tied for first among 30 governments in the 2018 "Open Data Barometer-Leaders Edition", but leadership requires sustained effort. In 2025, we placed 12th among 143 countries and jurisdictions on the World Justice Project's open government measure. While rankings differ in methodology, the OECD's OURdata index also shows a decline.

Our score fell from 0.60 in 2023 to 0.48 in 2025, below the OECD average.

We need to renew our commitment as we enter the AI era. First, trustworthy AI needs public information we can question and verify. That means quality data provenance, knowing who produced the record and how it changed. W3C PROV, for example, provides standards for documenting that history. Cryptographic signatures can verify origin and detect alteration but can not establish truth. We also need preserved versions and correction histories.

These practices help Parliament examine the evidence behind AI-supported decisions. They also matter when members use AI for speeches, for example, or constituent correspondence. Members remain responsible for checking claims, and Parliament should establish expectations for disclosing substantial AI assistance.

Number two, open information must be usable for oversight. A published contract, for example, tells only part of the story if we cannot connect it to its supplier and disclosed owner. Common identifiers, machine-readable records and reuse licences help make those connections. We should close gaps in procurement, beneficial ownership, business registries, public officials' asset and interest disclosures, and legislative data.

AI could help researchers and auditors identify potential conflicts for human investigation. I help support openparliament.ca because making parliamentary information accessible matters. AI could build on that work, helping people follow amendments, compare evidence and examine votes with answers linked to original records.

Number three, open government requires collaboration. Institutions can share standards and tools while retaining stewardship of their data. Shared interfaces allow systems to exchange information. Parliament and oversight bodies need expertise to evaluate those tools, and civil society should help test them. Privacy and indigenous data sovereignty must guide this work as well.

Canada can connect its existing commitments: AI for all, the federal public service's AI strategy, and the national action plan on open government. Treasury Board's AI register listed over 400 systems across 42 institutions at launch, from exploration to deployment. We can build on it to examine sources, limitations and responsibility. Bill C-42's beneficial ownership reforms similarly create opportunities for better scrutiny of public spending. This committee can turn these commitments into clear responsibilities and measurable improvements in democratic oversight.

In conclusion, open government belongs at the heart of Canada's AI strategy because it gives people the means to hold power accountable.

[Translation]

Thank you very much.

● (1220)

[English]

The Chair: Thank you.

We're going to suspend for one minute. We have the third witness here, so we will get his audio.

Witnesses, please stay on the line. We'll be right back to you.

● (1220)

(Pause)

● (1220)

The Chair: We are back. I'd like to welcome Dr. Curraj from Center Science and Innovation.

You have five minutes.

Erjon Curraj (PhD, Artificial Intelligence and Digital Transformation Expert, Center Science and Innovation for Development (SciDEV)): Thank you, Chair and honourable members. Thank you for the invitation.

I'm Dr. Erjon Curraj, an AI and digital transformation expert with SciDEV in Albania. My work has included contributing to an Albanian AI national strategy, leading work on a regional AI road map for the western Balkans and working across public sector transformation, cybersecurity, digital rights, research and civil society oversight.

My central message for all of you here is that Parliament must build its own capacity to use AI, but its capacity has to oversee AI at the same time. It's a chicken-and-egg problem.

AI can help Parliament compare legislation, examine evidence, track government committees, make information more accessible in both official languages and more—the indigenous ones as well—and engage citizens at greater scale. There are different ways, not just the current ones. Be innovative. How can we involve more citizens in speaking with their own voice?

Used well, AI can strengthen Parliament's constitutional capacity rather than just simply making administration faster and easier. It can bring these transformation aspects, which I'm expert in, but this creates a democratic dilemma as well. If Parliament depends on systems that it cannot adequately inspect, challenge or replace, the

instrument intended to strengthen its own oversight may itself weaken the oversight. This comes in a more circular way. If AI becomes one of Parliament's guardians, then who are the AI guardians? This spiral goes on and on.

This is something that is unprecedented, and it needs different layers of inspection and guard-railing. Of course, humans should be there, but who inspects the humans who inspect the AI? Who inspects the AI that inspects humans? It has to go in this fashion. It's a complex one but, once implemented and designed properly, we finally find the solution to such a huge problem that all governments—and not only governments—have right now.

The answer is not another single algorithm. It is a plural system, a complex one, with accountable people, independent institutions, authoritative evidence, auditable technology, civic participation and meaningful routes for challenge and correction. This is the fine-tuning I mentioned before.

This matters because technological capability is advancing faster than many institutions' ability to adapt. We see this problem with progressive and linear AI adoption. Technology is progressive, but people, governance and institutions are linear. We are not catching up and in sync.

AI can lower the cost of impersonation, manipulation, fraud, cyber-enabled influence and synthetic political communication. Some risks will be and are already immediate. Others will be a later phase, but they are coming. They are next door. Dependence on one provider, gradual loss of institutional skills, normalized surveillance, which we see in my region at least, or a degraded information environment that becomes visible only—

● (1225)

The Chair: I'm sorry. Wait one second. We have a point of order.

[Translation]

Christine Normandin: Mr. Chair, the interpreter says they haven't received the witness's remarks. I understand that the interpreter's job is a lot more difficult if the witness is reading a text.

[English]

Erjon Curraj: I sent it before. Can you check it, please?

The Chair: The text has been received, but you're deviating slightly from the text, and that's all right. You can say whatever you like. I think you have about a minute left, but could you slow down, please?

Erjon Curraj: Thank you, sir. I will try to do that.

This matters because technology capability is advancing faster than many institutions' ability to adapt. AI can lower the cost of impersonation, manipulation, fraud, cyber-enabled influence and synthetic political communication. Some risks are immediate. Others will be at a later stage: dependence on one provider, gradual loss of institutional skills, normalized surveillance or a degraded information environment that becomes visible only during an election or crisis.

I describe this as a democratic security debt. This is one of my recommendations. When adoption advances faster than institutional control, the system may look efficient today, while heightened costs are transferred to citizens at future institutions later. That's why, from an Albanian and western Balkans perspective, I would offer a practical lesson: Ambition without architecture collapses quickly, and—

• (1230)

The Chair: I have to interrupt.

I'm sorry, but you're a bit over time. Those were excellent points, and you'll receive questions.

We'll go to a question and answer segment now, starting with Mr. Calkins for six minutes.

Blaine Calkins: Thank you, Mr. Chair.

I want to start with Mr. Owen.

Could you revisit the statement you made in your opening comments regarding the public's use of an AI chatbot to find out who they should be voting for? Did I hear you right? Were 39% of the answers that came back from a hobbyist's site that was created by AI?

Could you elaborate on that?

Taylor Owen: Yes. This was a study that was led by my colleague Aengus Bridgman, whom you just heard from. It was an audit of the way AI systems were used in the lead-up to the Quebec election. They audited all the major chatbots for information about the election—where to vote, who to vote for, the platforms of candidates, where the voting stations were and so on and so forth.

Partly because Quebec journalistic publications de-indexed themselves from chatbots, there wasn't a lot of information about the election that was ingestible by the frontier models via what's called RAG, which is active retrieval search post-query. The information was not in their training data. The result of that was that they got on the Internet and looked for what seemed like reliable information. It turns out there is a site called LeQuébecVote.ca that showed up a lot in our audit results. We used our own AI agents to query the AI systems. The results they picked up were linking to this one site, which the researchers had never heard of before. We looked at it. It had been created two weeks earlier. It appeared to be entirely written by Claude.

There was then some reporting done on this. It turns out it was just someone trying to show the capability he had to build websites. He tried it out on this and left it up for the period leading up to the election. There was nothing necessarily nefarious about this person's actions, the design of the chatbots or the publishers who de-indexed themselves. It was just a confluence of events that led to, likely, a large number of people getting false information about the election.

This points to some of the realities of this ecosystem we're now living in. These aren't necessarily malicious actors trying to upend our democratic institutions—although it could be that too, since this points to the vulnerability present in the system. However, the way the system functions—certainly in this case—is not aligned with our democratic interests.

That was the point I wanted to make there.

Blaine Calkins: Thank you. That's a little terrifying, but I appreciate it.

Taylor Owen: It's destabilizing, for sure. There's no question.

Blaine Calkins: Yes. If that can happen by accident, imagine what could happen, potentially, on purpose if somebody figured—

Taylor Owen: That's the right question to be asking quite urgently.

Blaine Calkins: I'm going now to Mr. Curraj.

Albania and, broadly speaking, a number of smaller European nations have been very quick to adopt AI in their parliaments and governments. I believe you said fraud was one of the reasons you've adopted this.

Could you be clear on what...? Is it true that you don't have a minister for AI, but an artificially intelligent minister? Do I have that right?

Erjon Curraj: Yes, that's correct. Last year, when the government constitution happened, the surprise out of the blue was declaring that one of the new members of the government cabinet was a minister that was AI. It was a surprise. This news circled around the world. It's the first in the whole world.

The point is that right now, it's not based, let's say, on any necessary foundation for creating such a minister in such a great, innovative way of thinking. It was started based on some technical layers. First, it was just an AI chatbot. Its main first role as a virtual minister was to oversee the procurement process, because one of the main known areas of corruption is the procurement process. Right now, that's where it's working.

• (1235)

Blaine Calkins: How did the experiment go? That's what I wanted to get to. How is it going, on the corruption and fraud front, having an actual, virtual, artificially intelligent minister as part of the government decision-making process?

Erjon Curraj: Right now, the technical part is proceeding. They announced that next year will be the first phase of testing it. They are working on it right now.

From a civil society aspect and the think tank perspective, we have been quite worried about how to describe such a process for government data training. How do you avoid making the same mistakes with corruption if you train the model on existing data, and the current data are already corrupted? These kinds of issues are already there. They are hidden. They are not cleared up.

We are still here to see how we can assist the government to do such a bold move of making this real without the flaws it has right now: no government in place, no procedures and without the necessary transparency in place.

Definitely, yes, we know the claim is that we will avoid corruption, but as I asked in my speech, how do we avoid corruption if the system whose corruption you are aiming to fight is not, itself, transparent and accountable—

The Chair: Thank you so much. I'm sorry. I have to interrupt you.

We'll turn to Ms. Vandenberg for six minutes, please.

Anita Vandenberg (Ottawa West—Nepean, Lib.): Thank you.

I very much appreciate all of the witnesses today. We're all learning quite a bit and are probably coming away with more questions than we started with.

I would like to start with you, Mr. Landry, because you have a unique perspective. You're working right now on open governance and a public interest data platform, but you said before that you worked internationally with organizations like the National Democratic Institute, doing democratic development in other countries. I think you said it was in 12 countries.

Usually, when democracies work together and build capacity, it's because there's already a set of best practices, but in this area, there are no best practices to draw from in any country. Certainly, in our Parliament, even among MPs, there's no real practice. We're all doing our own thing and not necessarily sharing.

I wonder if you could talk a bit about how democracies should be working together and sharing information. For instance, on what's happening in Albania and here, is there a way Canada can help in doing some of that? Also, how do we learn from some of these other democracies and parliaments in the work we're doing?

Jean-Noé Landry: It's true that your mandate concerns Canada's democratic institutions. The point I'd like to highlight today is that given the backsliding of democracy internationally, as well as some of the major cuts in international support from the United States for democracy worldwide, there's a huge gap that is currently taking shape internationally, which also provides an opportunity for Canada to lead by example.

Some of the remarks I made around what we could qualify as next-gen or next-generation open government, which connects procurement, ownership, political finance, parliamentary records...all of these things needs to be done and achieved here in Canada as part of Canada's nation building, as well as its own current strategic priorities.

At the same time, there is a pretty significant network of Canadians who have done democracy support work internationally for quite some time. It's about 20 to 30 years. That's an untapped human resource and technical capacity that could be leveraged. I feel like that's almost a missing piece in Canada's foreign policy around clear economic realignment and multilateralism. There's a gap right now that Canada could fill by showing how it can be done here at home, as well as supporting some of these commitments internationally and building new partnerships.

I really, truly believe that by working collaboratively with Canadians who are active internationally, as well as local organizations that understand their contexts better, we could bring our own expertise to support a better understanding of influence mapping and power relationships locally, which could also be valuable to our foreign service as they deploy internationally.

• (1240)

Anita Vandenberg: Coming back to our Parliament, Canada's been leading on open government, and this is one of your areas of expertise. You talked about transparency. I want to delve down into what that looks like for an individual member of Parliament.

For instance, let's say one of my staff takes some talking points that we get from our party, puts them into ChatGPT and asks it to develop an answer to correspondence. I then go in and say I'm not really that much on side with what the government's doing, so can we tweak it a little, put this in and add something else? Does that mean that the prompts I put in would then be transparent to my electors?

We can all understand that this might be a bit difficult politically, because we are in a partisan environment where we wouldn't necessarily be able to reveal all of those different prompts. How would that be transparent? What would it look like in practice?

Jean-Noé Landry: Here, the open government framing is actually quite helpful. We can talk about transparency, which requires significant access to information and data to be open by default.

I think what you're getting at is the accountability aspect of open government, which requires the traceability of which records and which pieces of information went into the prompt, how it changed over time and how to link each explanation to that record. It's really the context of what comes out of the use of AI so that we can build digital and AI literacy by providing more context around how AI is utilized so that we open up the black box of AI for the benefit of the public interest.

As we use AI tools and as we rely on them for greater efficiency in the workings of Parliament and our relationships with constituents, I think we need to revisit the way we package, contextualize and explain how AI is inserted into building that relationship, which could actually fundamentally increase trust in our political and other institutions in Canada.

The Chair: Thank you so much.

I see the hand up, but it will be up to the members whether they ask you questions or not.

[Translation]

Ms. Normandin, the floor is yours for six minutes.

Christine Normandin: Thank you very much, Mr. Chair.

Thank you to all the witnesses for their remarks.

I have a long question, and it's mainly for Mr. Owen and Mr. Landry.

We know that Parliament will soon examine Bill C-34, which will provide a framework for the use of chatbots in contexts where harmful content may be present, among other things. You spoke at length about the political content that chatbots may use. Obviously, that isn't considered harmful content, but I gather from your remarks that there is still a risk to democracy.

I'd like you to share solutions and talk about how we should examine some of them. I think if we prevent chatbots from discussing politics, we could prevent them from using open data to hold the government accountable, for example, as Mr. Landry mentioned.

Should we avoid regulation altogether? Should we regulate to limit the sources chatbots can access to give information?

Generally speaking, I'd like to hear your thoughts on solutions or considerations to examine if we were to regulate artificial intelligence and chatbots in a political context.

Jean-Noé Landry: Thank you for the question.

I'll answer first if you'll allow me, Mr. Owen.

The way I see it, there are different aspects to this issue. As far as my expertise is concerned, something I think is important is the power not only to trace information and data sources that are part of the process, but also to then explain them.

You have to put yourself in the shoes of the people being given the information about the information. A whole other level of digital literacy comes into play, and that's why I think AI for all is an integral part of AI policy and strategy.

That's all well and good, but we're still developing the digital literacy skills relating to data and we haven't reached the necessary level of proficiency, if you will, across the population to understand the highly complex data ecosystem. Now we're on another level that's advancing very rapidly.

I think we need to take the time to explain things better, provide more context, focus on metadata and then really support people. It's a democratic culture fostered through civic engagement and the use of artificial intelligence.

It's as though we need to slow down while speeding up the processes we want to optimize.

• (1245)

Christine Normandin: Mr. Owen, would you like to answer?

Taylor Owen: Yes, thank you.

[English]

As a bit of background, I was on the expert panel on online safety that has worked for a number of years on Bill C-34. One of the challenges of that process is that these technologies have evolved much faster than the legislative process, to say the least. That meant that in this round of the bill, six months ago, when the government was drafting the latest version of this legislation, chatbots made sense as a technology to include. There was a lot of debate within the panel about the implications of doing that in addition to the social media products that were originally envisioned for that system, but chatbots were included for some elements of it.

There are a few questions, though, that stem from that and are directly relevant to your political misinformation question. One is, are chatbots the right category or bucket anymore, even six months later? I think maybe not. When we have audited AI systems, including for the seven harms embedded in the bill.... The bill is based on these seven categories of harmful content. We audited all of the main frontier chatbots for those. We got very different answers, depending on whether we used the web interface chatbot or the harness, which is an agentic system, or directly accessed the API of the model, which is what many products do.

Even now, when we're talking about which AI systems are going to be brought into Bill C-34 when this goes to committee at some point—maybe this fall—I think there's going to be a discussion about whether “chatbot” is even the right definition of inclusion alongside social media. That's one piece of it.

A second piece is what you do with political misinformation and political content. It's important to flag that misinformation and disinformation are not a harm category. My understanding is that it's not by intent, because that pulls the regulator into a position where they are adjudicating political speech acts. Some of the lessons that have been learned about other countries that have tried to do it are that, one, it doesn't work very well and, two, it creates a great deal of legitimate concern about overreach in speech regulation.

It is not a harm category. That being said, I think there are probably two things you can do to get at that.

One is the transparency provision inside the bill. Just the fact that companies need to provide a pretty broad swath of user and activity data, both on AI systems and on social media, to independent researchers and civil society organizations will bring a lot of these problems out into the open, so transparency will be a measure.

The other is in elections. This almost certainly has to be done via election law. I think we accept very strict limits on speech during this limited time period of democratic decision-making and deliberation, and I think chatbots will have to be included in that. What kind of speech from AI systems are we going to allow during our elections? That can be legislated.

• (1250)

The Chair: Thank you so much.

We'll turn to Mr. Moore for five minutes, please.

Hon. Rob Moore: Thank you, Mr. Chair.

Mr. Owen, maybe you can continue on, because the nature of my question was the relationship between safety and security with censorship, and where that line is. These are obviously some pretty preliminary discussions that we're having here, but as we talk a bit about the interplay between those two things, where the line is and where the line should be around censoring political or other thought....

Taylor Owen: It's an omnipresent concern in any of these regulatory conversations in particular, and should be.

The way Bill C-34 deals with that trade-off is by saying that only two types of speech will be mandated to be taken down: non-consensual intimate images shared without consent and child sexual abuse material. The bill says that for those two categories of content, we actually don't have a concern about edge-case speech and about over-restricting content that comes close to those two types of content. I think that's the right decision. I think we can agree that those are egregious enough that things that could be misinterpreted as those are probably okay, with some slight overindexing in our regulations.

For all of the other types of speech that are listed in the seven harms in the bill, there is no requirement to take down. There is only a requirement to do risk assessments on the incentives and the way the structure of the design of the system might be incentivizing

that kind of content, and then to be transparent about what you found. That is it. There's no mandatory takedown whatsoever. That means that a fair amount of that bad speech will remain up. I shouldn't say, “bad speech”. That's making a qualitative judgment. A fair amount of harmful speech in those seven categories will remain up. It just might not be amplified by the algorithms that drive the system, for example, or might not be overindexed in the chat responses, now that AI chatbots are included within it.

Does that get the balance right? I don't know. You're right that it is a trade-off. That's how the bill itself tries to balance them.

Hon. Rob Moore: I'm thinking specifically about language around social cohesion and the programming of the AI that's going to look at what contributes to social cohesion. What affects social cohesion? What value do we assign to it? That is going to, as you just said, influence the type of information someone receives or has access to. It's only as good or as biased as the initial programming that's going into it.

I would like some of your thoughts on that.

Taylor Owen: There are two things.

One is that there is nothing, to my knowledge, that will direct the companies building chatbots to influence discourse around social cohesion. It's just around the seven categories of harmful content.

Second, I think there's something different about speech generating from a product and speech generating from an individual. I'm not sure the bill does a good enough job of differentiating those two things yet. I don't think we as a public have figured that out yet, either. These are not people speaking to us. These are commercial products generating a product in response to a query we ask of it. To me, that requires a different understanding of speech rights.

It's a question that democratic societies are all wrestling with right now: What rights and obligations do we place on products that are acting as actors inside our democratic system? They are products.

• (1255)

Hon. Rob Moore: Mr. Curraj, twice you mentioned normalized surveillance as a risk.

Can you speak a bit to the experience that you have? Can you give a quick example or two of the dangers of normalizing surveillance?

Erjon Curraj: Thank you for the question.

The situation, when all this data is out there, is quite important in several aspects. The first layer is the citizen level. Citizens need to be aware of the value of privacy and personal data. When citizens' awareness is not well equipped, then any manipulation of this data or this data being misused by government or non-government actors gets normalized. People are not sensitive about that anymore. This is the first point of view.

In our case, in our region, we have seen different cyber-attacks and different personal data leakage around that. In the beginning, people got quite frustrated and sensitive. When this happens a second or third time, people get numb about it and don't feel anything, so they say that personal data and what they do with that is not relevant anymore.

What the problem is—

The Chair: I have to interrupt. I do apologize. We're well over time for Mr. Moore.

We will turn to Mr. Caley for five minutes, please.

Braeden Caley: Thank you very much, Mr. Chair.

I'll maybe start with Mr. Owen and pick up from where we were with your colleague a little bit. I'm struck, though, by the term you used of "democratic alignment". I'll pick up on that and on how we ensure that these models and tools are, in their use and interactions with democratic processes, aligned with our democratic principles. The question I was asking your colleague before was more around how we, or should we, perhaps, in election legislation at any future point, build some of the good work that's been done with deepfakes into objectivity or accuracy in information about elections in general. I'm curious to know whether there's anything you would want to elaborate on there.

I'm also intrigued by the comment you just made about the different rights, or at least how rights are applied to what is direct commentary by a human being in an online space. Perhaps where you were going with that was an agent or an agent's agent elaborating and beginning to take that speech through multiple further layers of something that looks a lot more like autonomy but of course started, at least in its creation, with some sort of human direction.

How do we account for that in one of the most crucial ways that we govern our democracy, which is how we account for the costs in that tight period you've mentioned? Data in general, for lots of very good reasons, has been interpreted as something that has no inherent value in our elections law. As models are trained up, I think there's an interesting question there and in terms of how these things are accounted for over the tightly regulated periods.

Taylor Owen: Those are two great questions—and welcome to Parliament.

Braeden Caley: Thank you.

Taylor Owen: On the last one, I don't think they should be afforded rights. Rights are for people. That doesn't mean we shouldn't consider the roles they play in society or the effects their speech acts have on our society, but I don't think they should have rights. The better framing for it, I think, is that those who build them should be held accountable for their actions and their speech. Place the accountability not on the agent or even the person who directs

the agent, in most cases, although there are some exceptions there. In my view, that accountability function clearly has to fall on the entity, person or corporation that builds the product that is acting in our society.

Now, that gets to a big question about what that accountability mechanism looks like. Is it a liability? Is it a regulatory infrastructure? What is it? I think we're in the middle of that conversation. We're certainly not at the end of it.

On the election information, the reliability of information during an election is something that we have put a very high premium on in our election law. The thing is that we've done it on systems that are no longer providing the majority of the content we're consuming in an election. Clearly there's a mismatch here. We are regulating the speech of registered political actors and of news organizations that don't get consumed, to be perfectly clear. A striking finding of the Alberta study we just released is that 80% of the discourse about the referendum online was driven by 112 influencers, not one of whom was a journalist.

If we are regulating speech during an election for a liability based on journalists and established registered organizations, we're not touching where people are getting their information, let alone the AI systems that are producing it. Something has to give there. Influencers and AI systems need to be brought into our conversation about what we do and do not deem acceptable during an election.

How you do that is a very different question. It's very complicated. I would just point out that these are complex systems. Journalistic publishers in Quebec rightfully took their products out of the ingestion system for AI models, in part because one of our studies showed that the training of all four models was heavily influenced by Canadian journalism—stolen Canadian journalism. It's their right to de-index themselves, but the consequence was that the people using the systems were given less reliable information than if their journalism had been present in the models' output. How you get at that is not an easy question.

● (1300)

The Chair: I'm sorry. I do have to interrupt. I apologize.

[Translation]

Ms. Normandin, you have the floor for two and a half minutes.

Christine Normandin: Thank you, Mr. Chair.

I have a question for Mr. Owen and Mr. Landry again.

Mr. Owen, in your opening remarks, you talked about the importance of participating in democracy.

Mr. Landry, you spoke of citizens' ability, should they wish, to use artificial intelligence to navigate government data and hold the government to account. If people were more involved at an early stage, we might have less need for today's discussion on how to regulate artificial intelligence.

I'd like to know whether you feel that the public is interested in better understanding what's happening with artificial intelligence, and whether you think people would take a greater interest if they were given better tools.

Jean-Noé Landry: There is certainly some interest. There is also a lot of fear and a lack of information about how these systems work. There is still a lack of transparency that is difficult to discern and it creates a lot of uncertainty. Regarding the importance of citizen engagement, we must also dare to create advisory structures with civil society, with citizens, so they can share their perspective during these conversations.

It's good to have expert committees from the industry, because they are the ones developing the products we use, that we want to buy, that are scaled, Canadian, and so on. That, however, is a whole other conversation that needs to involve citizens. That is what I am doing by developing AI systems to design tools for municipalities. If we're going to work with governments, we also need to put in place human governance structures to facilitate this type of dialogue, this type of discussion. You have to take into account power differentials, the language used, and even the accessibility of the terms promoted. It's not easy, but that doesn't mean it shouldn't be done.

There needs to be citizens' committees. There are all kinds of possible structures, so we can innovate in this space of engagement and civic participation. There are really very good opportunities to lead processes that involve people who aren't necessarily in the technology industry, but who are firmly rooted in Canada's democratic culture.

• (1305)

The Chair: Thank you very much.

[English]

We'll turn to Mrs. Block for a strict five minutes, please.

Kelly Block: Thank you very much, Chair. Hopefully, I will stay within that. If I don't, I'm sure you will let me know.

I want to direct my first question to Mr. Owen.

In our previous panel, Mr. Khan made an observation regarding the fact that there is more AI traffic on the Internet or platforms than human traffic. I'm really interested to know what your thoughts are on that and whether or not parliamentarians and government should be concerned about that.

Taylor Owen: I think that's a difficult figure to quantify. It's not always easy to know who—and that's part of the challenge too—or what has created content or what kind of entity has created content on social and whether they're human or not, but certainly it's rising. There's no question about that. More and more, the content we consume is artificial.

I'm hesitant to make a qualitative judgment on whether that content is good or bad, though, in part because a lot of AI-generated content is incredibly helpful. I'm more concerned about whether there are signals of reliability within it, and whether the people who create it and the companies that create that content are within our systems of accountability, so that when things like the Tumbler Ridge tragedy happen, for example, we have a mechanism to hold those companies accountable.

To be perfectly clear, right now, we don't—at all—have a single mechanism to do that. I'm less concerned about it being artificial or human than about it being transparent, whether it's artificial or human or not, and whether the act itself is inside our system of governance. Right now, it's not sufficiently, in my view.

Kelly Block: Thank you very much.

I will turn my next question to Mr. Curraj and circle back to the line of questioning that my colleague Mr. Calkins started off with in regard to the fact that Albania has gone as far as implementing an anti-corruption AI minister, as well as its children, which is something that is difficult to understand. These children act as AI assistants for parliamentarians. I'm wondering if you would be able to answer as to whether or not the implementation of this AI presents security risks to the confidential data that parliamentarians may come into contact with.

Erjon Curraj: Thank you, Mrs. Block.

Indeed. When we speak about AI nowadays, we speak about AI native and AI full maturity at all levels, including Parliament.

The Government of Albania is trying to have this 360° story, and yes, one of the stories to fill this gap is MPs' having this assistant. Definitely there is a need. In your case, you are more equipped. In our case, every MP doesn't have an assistant to help them. Having such an assistant will help them to debrief and better understand bylaws and everything they vote for.

Right now, this is the implementation phase, and yes, the risks are many. One of them is what you just said, but yes, there is also the confidentiality and the data there, and how you keep it secure. Other risks are the poisoning of data and the training of the data, so how you use these decisions. At the end, as I said before, the MPs will vote on any bylaws in Parliament based on this assistance, so how we make sure that the suggestions coming from these assistants are fine and, of course, checked. This is the major issue and concern I have, and then, yes, definitely there is the confidentiality part of it. Whatever you store there, you don't know who has access there and how this gets controlled.

The differences are several, but once you do this implementation properly and you synchronize—have orchestration between all the AI ecosystems at the government level—I think this will be a major innovation and benefit to the government and democracy, if it's done properly.

The Chair: Thank you so much.

We'll now go to Mr. Fergus for a strict five minutes, please.

[Translation]

Hon. Greg Fergus (Hull—Aylmer, Lib.): Thank you, Mr. Chair.

I, too, would like to thank all the witnesses today. This discussion is really very important.

Mr. Owen and Mr. Landry, you both talked about governance. I would add that Mr. Owen wrote in the media earlier this summer that Canada has an adoption strategy, but no governance strategy.

I'd like to hear both of you, in one minute if possible, on what governance components the Canadian government should adopt regarding the use of AI.

• (1310)

[English]

Taylor Owen: That's a very large question for one minute, but let me give it a try.

Initially, the government had an adoption strategy and not a governance one, but that's changed quite dramatically over the course of the last year as our understanding of these systems and citizen push-back against that adoption strategy have become more viscerally felt.

We now have a partial governance strategy. As I mentioned, I think Bill C-34 and Bill C-36 are the table stakes to entering into the governing of these systems. Stepping into how data is used and how outputs are regulated, and having an independent agency commissioner to oversee both, is a huge first step, but in my view now, it in itself is insufficient.

We've made a step, and now it's—

[Translation]

Hon. Greg Fergus: Okay. What are the next steps, then? What are we missing?

[English]

Taylor Owen: What I spelled out.... I'll need another minute, if you'll allow, for what comes next.

Look, I think we need to have both more capacity on our safety oversight—through the AI safety institute, which, in my view, should be made independent from ISED and scaled, as other countries have done—and more capacity to oversee our frontier risks. I also think, on the more consumer and citizen harm side, we need much more capacity to understand these systems. That's one.

I think we probably need to extend our governance reach beyond just limited chatbot scope and social media harms and into a broader range of AI systems.

I think we need to meaningfully—and we have not done this, to be perfectly clear—engage citizens in this process. There is still a deep distrust. We survey this monthly at the observatory. Canadians do not trust AI because they do not believe it is being governed sufficiently. They want into that conversation. We have not built the systems to do that, but they're there. As you know, we ran an AI assembly of gen Z kids, and they all want in.

[Translation]

Hon. Greg Fergus: I didn't want to interrupt, and I greatly appreciate your answer, but I would like to give Mr. Landry about 90 seconds so he can define, in his opinion, the things we're missing in terms of governance.

Jean-Noé Landry: Thank you for this opportunity. I think it's important when we talk about governance to clarify what we mean by that. If we want to involve citizens, various types of stakeholders or communities of interest in a governance conversation, we need to fully understand the mechanics of governance itself.

Your question has different levels of complexity. Who makes the decisions? Who influences them? When? What is the traceability of decision-making processes? What is the connection between the various democratic bodies?

Different types of people, different members of civil society, can be engaged at different points in the governance processes, whether it's for the development of a public policy, for its implementation or for decision-making. I think it's really important not to assume that the governance itself is clear. I think we need to clarify it so we can have a good conversation about adopting an AI strategy.

I invite you to reach out to people who don't have technology experience but who talk about inequalities, not the usual suspects, so they can come together to ask questions with confidence. You must have had conversations with these types of people—

• (1315)

[English]

The Chair: I apologize, but I have to interrupt.

I did say that it was a strict five minutes. I interrupted some of you in your testimony. If you have anything further, please submit it to the committee. It will be translated and circulated to the committee.

This committee stands adjourned.

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

SPEAKER'S PERMISSION

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

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

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

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

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

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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