HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

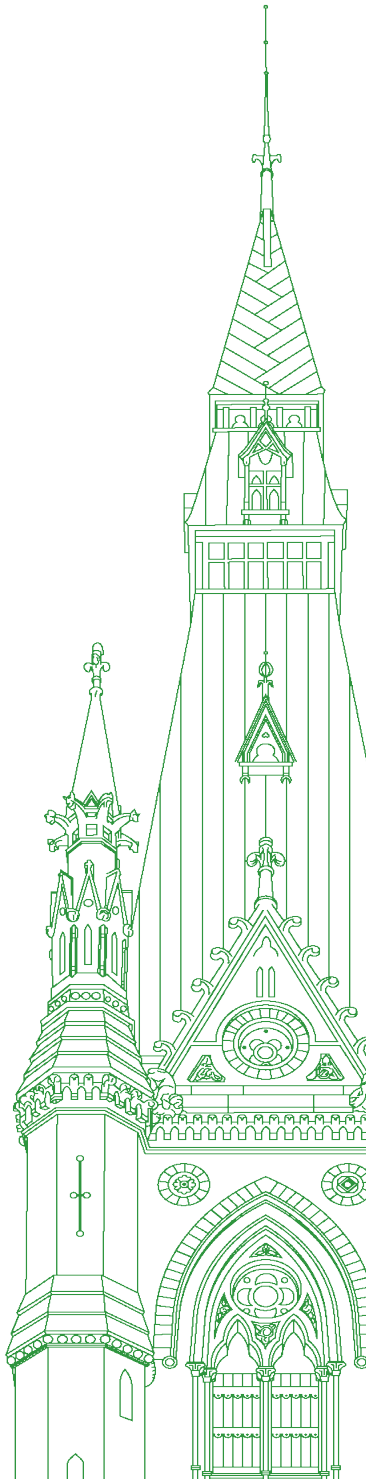
45th PARLIAMENT, 1st SESSION

Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development

EVIDENCE

NUMBER 025

Monday, October 26, 2026



Chair: Fayçal El-Khoury

Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development

Monday, October 26, 2026

● (1540)

[*Translation*]

The Chair (Fayçal El-Khoury (Laval—Les Îles, Lib.)): I now call the meeting to order.

Welcome to meeting number 25 of the Subcommittee on International Human Rights of the House of Commons Standing Committee on Foreign Affairs and International Development.

[*English*]

Pursuant to the motion adopted by the Standing Committee on Foreign Affairs and International Development on Tuesday, September 23, 2025, and the motion adopted by the subcommittee on Monday, October 5, the subcommittee will meet today on the subject of its study on the challenges and opportunities presented by artificial intelligence for human rights movements internationally.

[*Translation*]

Today's meeting is being held in a hybrid format. In accordance with the Standing Orders, members may participate in person or via the Zoom application.

[*English*]

Before welcoming our witness, I'll say this: The clerk distributed, on October 23, three draft budgets for the following studies. On the human rights situation in China, there's a budget of $7,750. On the global impacts of artificial intelligence on human rights movements, there's a budget of $7,750. On the briefing on gender-based violence against Ukrainian women in the context of the Russia-Ukraine conflict, there's a budget of $5,900.

I ask all members this: Is it the will of the committee to adopt those budgets?

Some hon. members: Agreed.

The Chair: Thank you.

Now I would like to welcome our witness for the first panel.

We have Mr. Jean-Noé Landry, director, federated data hub, Institut de la résilience et de l'innovation urbaine. He is with us by video conference.

Welcome, Mr. Jean-Noé Landry. You have the floor for five minutes for opening remarks.

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

For over two decades, I have worked alongside democratic movements and civil society organizations in countries including Serbia, Russia, Tunisia, Kenya and Ukraine. I subsequently led Open North, a leading Canadian organization working internationally on democratic governance through data and technology. Today, as you noted, Mr. Chair, my work focuses on responsible data infrastructure, federated data models and AI, as well as democratic accountability.

My central argument for you today is this: AI is not simply introducing new risks and opportunities for human rights defenders; it is fundamentally changing the distribution of political power, and our international democracy assistance needs to change accordingly.

Let me make three points. First, AI is changing the economics of repression. Activities that once required extensive state resources, such as monitoring political networks, analyzing communications, identifying activists and manipulating public discourse can increasingly be automated and deployed at scale. For governments already controlling surveillance infrastructure and existing personal data, AI represents a significant multiplier of existing power.

Civil society faces a very different reality. Organizations defending human rights frequently lack the technical expertise, infrastructure and resources to protect themselves, let alone match these capabilities. We are now entering a period in which the capacity to repress is becoming more scalable, while the resources available to resist repression are contracting. This is not a problem that can be solved simply by distributing or deploying more AI tools to individual organizations.

Let me focus on my second point. We need to rethink what democratic accountability looks like in the AI era. Over the past 20 years, the international open government movement, of which Canada was a leading player and actor, has made substantial progress in opening public records, establishing transparency standards and strengthening civil society's access to information, but publishing information is only the beginning. The next challenge in the AI era is making that information usable for accountability.

Let's consider Hungary as an example. There, thousands of parliamentarians' financial declarations exist as scanned, sometimes handwritten documents. Through work involving the international open government community, AI-assisted processing has helped transform nearly 4,000 declarations, if not more, into structured information that can be searched, compared and mapped. Connecting these records with corporate ownership and public procurement, for example, could allow independent investigators to identify potential conflicts of interest that would otherwise remain difficult to detect.

This illustrates a larger opportunity: moving from transparency as access to information towards transparency as the capacity to investigate and act. However, it also raises important questions about data ownership, security and accountability. These capabilities must serve local civil society, not create new dependencies on foreign governments or commercial technology providers.

Finally, Canada should move beyond funding isolated technology projects and towards building shared democratic infrastructure, and I would suggest doing this according to three priorities.

First, establish a sustained international capability for democratic accountability, connecting Canadian AI expertise with trusted civil society networks internationally, to support investigations, institutional monitoring and rapid responses to emerging democratic threats. Let's combine the human element with the technological capacity.

Second, invest in shared public interest infrastructure, secure data environments, interoperable tools, multilingual analytical capabilities and technical expertise that organizations can access without having to build everything independently.

Third, make local ownership and democratic accountability nonnegotiable. International partners must help define priorities, govern access to information and retain control over sensitive data. AI-supported findings must remain verifiable and subject to human judgment.

Mr. Chair, in conclusion, Canada has invested substantially in AI research and innovation. The question now is whether we can translate some of that capacity into an enduring contribution to international democratic resilience. I would say that we should not measure success by the number of AI projects funded but by whether democratic movements gain lasting capabilities to challenge abuses of power and hold institutions accountable.

Thank you. I look forward to your questions.

● (1545)

The Chair: Thank you, Mr. Landry. I now open the floor for questions and answers. I would like to start with Mr. Majumdar.

You have the floor for seven minutes, please.

Shuvaloy Majumdar (Calgary Heritage, CPC): Thank you very much, Mr. Chair.

Thank you for your testimony. I noticed that you're a former employee of the National Democratic Institute. I'm a former employee of the International Republican Institute. In that vein, I know that you have done some pretty impressive work when it comes to dealing with dissidents in the Kremlin in Moscow, Russia. I wanted to pull on that thread a bit.

You worked alongside pro-democracy leaders, or democratic reformers, in closed societies. What advents have we seen in terms of how facial recognition is used to identify dissidents by the Kremlin, by the CCP and by the IRGC, not just in their own domains—their own countries—but internationally?

First, to what extent do you see these technologies being used? Second, how do these technologies bear out when it comes to transnational repression and the presence of these governments in other jurisdictions, including ours?

Jean-Noé Landry: It's a good question. I have to say that the experience I had in Russia dates back to 2005 to 2006, so it was well before a lot of the advances that we're seeing currently. However, it's often in these contexts, as you will know from your own experience internationally, that some of these technologies get leveraged and tested, because governments put the means and the resources behind them. There aren't the same kinds of democratic constraints at play, through parliaments, to provide oversight such as you're doing today.

I'm not in a position to comment on how those technologies were used in 2005 and 2006, because they simply didn't exist. However, I would argue that the underpinnings of the repression in the democratic space provided the conditions to enable movement in a very aggressive way without oversight around the development of these types of technologies. There's very little access to understanding which companies are being funded to do what in a context such as Russia, for example, because we don't necessarily have the same reporting that we would in a so-called open society.

You're raising an important question in connecting local organizations that are subject to these types of surveillance capabilities. What we're seeing right now—with your experience with IRI and mine with NDI—is that we're not just dealing with the backsliding of democracies; we're actually dealing with the impact of diminishing investments in international development around these democratic networks. People who used to have forums to discuss and connect with one another about the repercussions of surveillance don't necessarily have the ability to do that. I would name that as an opportunity for Canada to demonstrate leadership in helping hold that space for civil society organizations through movement building in networks that are struggling to find the means to step outside their own national jurisdictions and to connect with one another internationally.

Organizations that used to do that multilaterally are really having a hard time providing the means to connect in that way. I'm always going to be deferring to local organizations that are being subjected to these means of repression as opposed to providing high-level research analysis of what we ought to be doing.

Canada, as a middle power, has credibility and can connect to our own AI capabilities, researchers and companies to have an exchange on a technical basis with organizations locally. There's a lot that could be done with our own Canadian AI expertise that could be leveraged internationally if Canada is willing to put itself behind it.

● (1550)

Shuvaloy Majumdar: Looking at it from the perspective of the democratic reformers, not just in repressive societies, but also their advocates and friends here in Canada, what kind of opportunities does AI's reach now provide for them to multiply their efforts? It's probably a fair criticism to suggest that the tools that democratic reformers have used over the last couple of decades to organize themselves are a bit dated, whereas the tools that authoritarians are using to exercise their repression have advanced to the state of the art.

Looking at how people who believe in their freedom can be better organized and better enabled through AI, what would your guidelines be on how that could be embraced?

Jean-Noé Landry: One hot topic these days is around open AI. It's one thing to access the code and the algorithms, but then what do you do with that? How do you interpret very complex and sophisticated data models, as well as how data gets transformed and the traceability of data as it's processed into these models in order to develop these types of analytical outputs?

There's an AI kind of literacy that's founded on data literacy, on how to interpret, instill and put in place not just the reflexes but the capabilities of facilitating the traceability of decisions as they relate to the bringing together of multiple different data sources.

We talk about AI for all in “Canada's National Artificial Intelligence” strategy. I think there's a lot within that document that is transferable into a Canadian kind of democratic investment internationally.

I would also name the interoperability of data—data sources that are out there but have volumes that are extremely difficult to manage just because of the sheer size of what we're talking about. If we talk about asset disclosures or business registries, beneficial ownership, procurement data, electoral records, changes or even amendments to different laws and regulations, we now have the capability of bringing all of that together. From the perspective of an activist or a democracy reformer, there's huge value in bringing in these capabilities, not just for civil society but also for our Canadian diplomats internationally.

We could layer on top of that the human intelligence of our Canadian experts who have done this work internationally, to add value to our AI capabilities there. It's the human interoperability of how we view the world to add context, in addition to the AI outputs that bring huge amounts of unprecedented information together.

The Chair: Thank you, Mr. Majumdar.

I would now like to ask Madame Vandenbeld to take the floor for seven minutes, please.

Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much, Mr. Chair.

Thank you, Mr. Landry, for being here. I'm struck by one of the things that you said about AI being a multiplier of existing power. In that case, when you have a repressive state, a surveillance state, this would only amplify the ability of that state to continue that repression. However, what I'm hearing you say is that there have been fewer resources for civil society, for human rights defenders' networks. Therefore, there's an imbalance. Am I right?

You're also saying that there is a need for us to invest in some of those civil society mechanisms so that they can have an even playing field and hold these regimes to account. Is that correct?

Jean-Noé Landry: Yes, very much so. That's why I'm also putting forward as an idea not to strictly focus investment on a project-to-project kind of basis in terms of the support that the Canadian government could provide but also to invest in the infrastructure, in the interoperability, in gaining more access to data, as well as in the capacities of civil society to interpret that data.

Canada has the credibility, the leadership and the space right now to do something that it may not have been able to afford to do in the past because there were more players. I would change that into an opportunity.

● (1555)

Anita Vandenbeld: When you talk about shared democratic infrastructure, most countries are looking at this from their own perception of sovereignty—sovereign AI, having their own data centres, etc. When you say “shared democratic infrastructure”, what does that look like from the perspective of global democracy and human rights?

Jean-Noé Landry: I look at it from an open government perspective, because I have that background. I speak of core, high-value datasets, which vary quite significantly from country to country. Even if there are requirements within the EU, for example, to share data, to make some data accessible, in the data, the definition of fields may not be the same. The structuring of the data, the formatting, may not be the same. There are some best practices around how we can normalize the underpinning infrastructure of the digital space, which is required for democratic movements to operate.

The advocacy can be better informed and anchored because of this better understanding provided by the analysis that's derived from AI. I look at the underpinning digital infrastructure as a kind of focus that Canada could have in a strategic way that would feed into media freedom and into legislative open parliaments, into political parties. All of these different pillars of democracies are underpinned by this digital infrastructure now.

Anita Vandenbeld: You also talk about capacity. We know that here in Canada we have a lot of expertise. If we're given a significant amount of data, we have people who could manage that. However, if you're a human rights defender on the ground in Afghanistan or Venezuela, it's a lot harder to manage the data and take advantage of the democratic infrastructure you're talking about.

How would we deliver that kind of capacity?

Jean-Noé Landry: Yes, that's difficult because there's always going to be a need not to simply create more competition or to even bank on one organization that will get trained up to do that thing that we see as potentially valuable. That's why, with the huge diversity of Canadians who have worked internationally, they can help contextualize how Canada could intervene or support its role locally.

I would urge this subcommittee to think about how to mobilize this Canadian human expertise, these people who can act as mediators, have that better understanding of the local context in a supplementary or complementary way to our own missions in our embassies, and then look for partners, civil society actors who are feeling the brunt of these surveillance tools. I'll reiterate the point around going beyond a project-to-project basis. If repressive states are multiplying their means of repression, let's maybe look at open-source technologies that are proving more resilient. Let's look at how to invest in infrastructure that can be pulled and beneficial to multiple organizations in a systemic way so that we don't bank on only an election-monitoring organization or only an advocacy organization. There are underpinning digital infrastructure investments that Canada can make to have much greater systemic impact.

Anita Vandenbeld: One of the disadvantages of project-based capacity and development is that it's slow. You said something about rapid response, that you can get in right away. Could you elaborate?

Jean-Noé Landry: Yes.

One of the initiatives I'm advising globally specifically looks at asset disclosure, and it is being done by a researcher here in Canada as a side project to his tenure-track teaching. He has developed his own code and pulled together millions of asset disclosure data points into his own capability.

If he's able to do that and I've connected to him in a strategic partnership as an adviser, to the open contracting partnership, to open business registries, organizations that have that kind of purview and understanding of these complex issues.... Without necessarily investing huge amounts of funding, there are things we can leverage that would have significant impact, but this needs to be anchored in the local context. That's a rule of thumb. Anybody who's sitting in my chair here at home, speaking to you today, should say if they're not....

● (1600)

Anita Vandenbeld: One of the key issues is trust. Having it anchored locally is a way to build trust as well.

Jean-Noé Landry: Yes, so we'll talk about—

The Chair: Excuse me. The time is up.

Is it possible for you to give your answer in five to 10 seconds, or will you wait for the next time?

Jean-Noé Landry: I would only say that issues around digital sovereignty, digital rights and that kind of language...and these principles need to be at the core of how we invest.

The Chair: Thank you.

Thank you, Madame Vandenbeld.

[*Translation*]

I now call upon Mr. Brunelle-Duceppe to speak for seven minutes.

Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ): Thank you, Mr. Chair.

Mr. Landry, thank you for joining us. What you are bringing to the committee is truly very interesting.

I would like us to discuss transnational repression. Artificial intelligence does, after all, make it possible to collate data, identify individuals and monitor their activities on a much larger scale than we have seen before. For human rights defenders living under authoritarian regimes or living abroad in various places—I know quite a few—this really does represent an increasingly significant threat.

In what ways does artificial intelligence enhance states' capacity for transnational repression? That is more or less what I am getting at. What are the risks facing human rights defenders, whether in their home countries or abroad?

Jean-Noé Landry: Thank you for the question.

On the one hand, there is the traceability of individuals. We can access more information about individuals who defend human rights in their own countries. Ultimately, we can adapt the way we act to suppress their activities. For example, it is now very difficult for people who are active in their own local context to travel to other countries to meet in person. Information is being shared, and the standards are no longer the same. Beyond access to visas, I am referring to the safety of the individuals leading these struggles locally. So, we are somewhat outside the norms we were familiar with over the past twenty or thirty years.

That said, I believe there is also an emergence of alliances and partnerships between middle powers. We could make this more explicit in order to support transnational movements and build up investigative capabilities, for example, to shed more light on corruption, on the flow of funds, on the ways in which money is hidden, or on the family ties between oligarchs and their relatives within international networks.

However, Canada must also be prepared to champion good governance and transparency, and to stand by its conclusions. That is no easy task in a context such as today's, where we know there may be political and economic repercussions if we choose to ally ourselves with political partners.

Alexis Brunelle-Duceppe: Actually, you've opened the door for me a little, but what has happened over the last few days has left me quite stunned. I understand that we can trade with all sorts of countries, but we signed a joint declaration with the Erdogan regime stating that Canada and Turkey share common values regarding democracy, human rights and the rule of law, amongst other things. Doesn't this highlight an inconsistency, I would say, when it comes to rhetoric and the protection of values?

Furthermore, doesn't this throw a wrench into the works when it comes to trying to establish who is responsible for targeting representatives of organizations that defend human rights? When we sign agreements like this with countries, isn't the message Canada is sending out a bit inconsistent? This isn't about politics. It's simply that, at some point, it's a matter of fact.

● (1605)

Jean-Noé Landry: I understand the question. It is indeed a topical issue, but I shall give you my opinion without necessarily commenting on the economic negotiations. I think there is an advantage in being present and being able to establish a basis for dialogue with these governments. I believe we are now in an era where it is important to gain a better understanding, to forge links, and perhaps to use certain economic levers to drive forward and promote democratic reform at a local level. However, it is quite complicated and I understand the nature of your question.

Alexis Brunelle-Duceppe: I fully understand your point.

That said, at some point, there are certain lines—in my view, at least—that perhaps should not be crossed. We've gone so far as to say that we share the values of democracy and the rule of law, when we know full well that Erdogan's regime persecutes members of the LGBTQ+ community and imprisons journalists and political opponents.

In short, I don't want to make you talk too much about politics.

Jean-Noé Landry: That's fine.

Alexis Brunelle-Duceppe: I want us to stay on this issue precisely because, as I understand it, it is extremely difficult to determine who is responsible when a human rights defender is targeted by an artificial intelligence tool. Who is behind this? It is also quite difficult to prove the harm suffered by that person.

So, I'm wondering what recourse there is, as things stand, when a human rights defender is targeted by artificial intelligence tools. Are there ways to track down those responsible for these attacks?

Jean-Noé Landry: It is extremely difficult.

It is very difficult to answer this question, precisely because of the opacity of the systems we are discussing at the moment. What I would say is that there are more and more civil society networks and organizations that are having to relocate to countries neighbouring those where they wish to operate. It is very difficult for someone currently in Russia to lead a pro-democracy campaign. These are people who are now based in Poland or elsewhere, and the same applies to certain countries where the situation is more challenging. We must recognize the extent to which civil society has had to demonstrate a degree of flexibility and agility, precisely because, due to the opacity of the systems, it is almost impossible to ensure traceability.

What I would say is that the capabilities utilized by the governments in question can also be adopted by civil society to track the activities of elected representatives—and so-called elected representatives in some cases, because these are not democratic elections. Let us use these same tools ourselves to expose and bring to light systems of corruption. For example, in Serbia, following yesterday's election, we are seeing a very broad mobilization, which could have an impact and bring down a government that has been in power for 12 years. There is potential for using these tools for our own democratic purposes.

Alexis Brunelle-Duceppe: It's like a judo move.

[*English*]

The Chair: Thank you.

Now I invite Mr. Zuberi to take the floor for five minutes, please.

Sameer Zuberi (Pierrefonds—Dollard, Lib.): Thank you, Mr. Chair.

Thank you to the witnesses for being here today. I really appreciate your presence. We all do.

I'd like to ask some questions around AI ethics. Are you familiar with this concept, and can you speak to us a little about AI ethics if you are?

Jean-Noé Landry: My context is that of ensuring that we have a clear understanding of what decisions are made using different capabilities related to AI and technology. My academic background is in philosophy, so I could talk about ethics if you would like.

Sameer Zuberi: Please. I did see that in your background, so I thought you might have something further to share on AI ethics.

Jean-Noé Landry: In this context, AI ethics needs to fit into what political space we have in order to ask certain questions. Who is afforded the right to ask those types of questions? What recourse do they have in order to act accordingly upon what they see and how they view the world?

In terms of AI ethics, without the rule of law, we're posing a lot of critical questions about a piece of technology. The question is how we act upon it. This presumes that we have the availability of data and can even understand and fully grasp how that technology operates. AI ethics is best conducted in a space that enables scrutiny and critical thinking, which is not necessarily the case in these repressive regimes.

● (1610)

Sameer Zuberi: Certainly.

In your last point, you were speaking about rules and whatnot. This has been the case throughout your testimony.

Have you seen any development of international norms related to AI? What are those international norms starting to be seen to be developed within?

Jean-Noé Landry: It's difficult to situate AI norms as they relate to democracy assistance, to be honest. This is something that I would see more in terms of data standards. I always go back to the data because, without good data in which we can have trust and control, everything that comes afterwards could be fabrications. We don't necessarily have the ability to trace back the accuracy or the reliability of what we see in these technologies.

It may be a question best suited for the OECD, for example. Who sets the norms, and who has the sticks to impose certain consequences if those norms aren't respected? The sticks these days are harder to come by, because the biggest proponent of democratic assistance has completely drawn back from that space.

We need to think creatively, and I may not have the answers for you today about what the carrots and the sticks are that Canada has in its own tool box in order to reward, maybe differently, and uphold the respect for the rule of law on high ethical grounds.

It may be through some best practices around OpenAI or even Canadian technology companies that abide by certain codes of transparency and accountability themselves as a model for others to follow.

Sameer Zuberi: Certainly. I think we're all doing catch-up when it comes to AI. The whole world is, in many ways. Those of us who are watching are playing catch-up unless we're actually in the development of the technology.

I've heard some analogies of AI being similar to nuclear power and weaponry. When that technology came to the fore, international treaties and covenants were developed in order to put rules on the use of that technology. I would suggest that we are.... I mean, it's not my suggestion; it's basically the analysis of others. They have said that we are in a similar moment by analogy. New technology is being developed, and the rules have yet to be developed around that technology. International treaties and covenants do need to be developed to that effect.

Do you have any thoughts on that comparison by some who've opined on AI and the analogy with nuclear energy and weaponry?

Jean-Noé Landry: It's the context of when these rules were put in place and who was behind it—namely, the United States—to shepherd a community of countries in order to support international institutions like the UN. I would say that in the current context—

The Chair: You can take another few seconds, but the time is up. Go ahead, please.

Jean-Noé Landry: Probably look at a regional scale iteratively and demonstrate the value of norms as we document them and then demonstrate that we can grow them. In terms of international norms, we might need to proceed in reverse order. Start at a small scale and then go all in on the international scale, as opposed to starting large and then trying to scale down.

The Chair: Thank you.

Madame Kronis, you have the floor for five minutes, please.

Tamara Kronis (Nanaimo—Ladysmith, CPC): Thank you so much, Mr. Chair.

I want to thank the witness for being here to provide this really important information and be part of this incredibly important study.

I'm wondering if you could elaborate a bit on the different resources that state actors and human rights defenders have at their disposal in real time on the ground in terms of AI.

● (1615)

Jean-Noé Landry: Citizens in most countries have to divulge or share information and personal information that can then, from a government perspective, be treated in bulk in a way you don't have if you're an NGO activist. The levers from an information management perspective, by virtue of being a government, in having the exercise of power where you collect data...and the consequences of the analysis that can come from any conclusions derived from that analysis as a state actor. It means you can limit freedom of movement. You can use the lever of the police to incarcerate and stop and create blockages around mobilization in civil society. The levers of power are asymmetrical in the way in which non-profits or movements mobilize themselves.

That being said, NGOs, because of that asymmetry, are also able to turn that on its head and use different techniques in order to mobilize in a way that is non-digital. We're talking about digital mobilization. However, I know NGO activists who are very careful about sharing their own personal information.

That's part of the technology cybersecurity value that Canadian investments could provide. I'm thinking of Montreal-based firms such as eQualitie, for example, that work in repressive regimes and support digital networks locally. We need to have alternatives to the means of control that repressive states exercise power over.

Tamara Kronis: That's very helpful in terms of helping to give human rights defenders a better chance, in the same way that rules help make it so that games of chance are fairer. In the context of the house always winning in those games of chance, I'm wondering if you could comment also on the transnational aspect.

We've done a number of studies around transnational repression. I'm wondering if you can comment a bit on the ways in which AI can be used by the state when families of human rights defenders are inside the countries in which the human rights defenders are trying to effect change. It's not just in terms of information gathering; it's also in terms of the creation of deepfakes and the ability to convince human rights defenders who are outside the country, or their families who are inside the country, that things have happened when they haven't actually happened.

I'm wondering if you could help us understand what is at stake in this conversation.

Jean-Noé Landry: Thank you for your question. It speaks to how a number of colleagues and friends have faced this type of intimidation, in which you lose control over your own narrative or your own identity in the way you're being represented. It's a character assassination that's being conducted.

The psychological, emotional and physical consequences of these types of harassment and intimidation efforts by governments can really take a toll. That's part of the design of why they do it. It's to discourage you and show you that there is nowhere you are active—including with your family members and associated members of your own network—that is out of bounds for the state to intimidate you.

It's very difficult. It takes a level of courage to demonstrate that you have somebody's back when it gets tough.

In Canada's approach, we need to anticipate specifically what you're discussing. My experience with democratic systems and repressive regimes is that once you start to get noticed, you know you're probably doing something right from a democratic reform perspective, but it also means that the stakes are increasing in terms of the harm you may face in response to that.

It's a safe harbour—

● (1620)

The Chair: Thank you.

[*Translation*]

Mr. Brunelle-Duceppe, you have the floor for five minutes.

Alexis Brunelle-Duceppe: Thank you, Mr. Chair.

That is truly fascinating. Thank you very much, Mr. Landry.

Perhaps you will correct me, but to my knowledge, artificial intelligence tools are largely developed by the private sector, which then supplies them to the government, or sells them to certain governments or states. In my view, this raises questions of due diligence and corporate accountability.

Is this not an opportunity for us, as legislators, to examine whether certain companies can be held accountable when their tools are used, for example, to carry out transnational repression or to target human rights defenders?

Jean-Noé Landry: That is a very good question, which also requires us to look beyond technological tools or products, and to consider cloud infrastructure, data brokering, analytics software and procurement processes as well.

With regard to procurement processes, I believe there is a proposal to introduce controls on the export of various Canadian technologies to ensure they are used responsibly abroad. These are standards which, as I understand it, could be put in place by the Canadian government to ensure there is no double standard in the way Canada seeks to promote certain values, and to ensure that tools originating from Canada do not end up harming the very people we are trying to help, locally, on the ground.

It is also a great way to recognize companies that are raising the bar in terms of transparency. We should ask them to what extent they would be prepared to do so, given that there may be contracts at stake.

Alexis Brunelle-Duceppe: That is precisely where the whole issue lies: the privatization of these tools, or rather, the fact that these tools are owned by the private sector.

In that case, are there not control mechanisms that we could impose on these companies before their tools are rolled out? I'm talking about what we can control. Clearly, there are still several companies which are, I would say, the largest in the world. I'm thinking mainly of American companies. There are a few in Europe. Even here in Canada, this is starting to take off. So, even at this stage, there would be a certain degree of control that we could impose on them.

Jean-Noé Landry: I think so, but beyond that, let's also try to consider innovation and the way in which we are currently investing in our own Canadian companies.

I'd like to return to a point I raised earlier regarding open-source technologies. In an anti-democratic or repressive context, people who use open-source tools must be very careful, because they are exposed to the ways in which the regime under which they operate may monitor or control them.

However, there is also a source of resilience, because it is more difficult to attack an entire open-source community made up of people who collaborate, whether they are in the country or abroad. So, I think there are various models that your committee could examine or consider beyond the Googles, Apples, Facebooks, Amazons and Microsofts of this world. We could explore Canadian approaches to open source involving trusted partners, with frameworks and commitments to very high standards of transparency and accountability. I think there are opportunities here, but we would need to look into this in more detail.

Alexis Brunelle-Duceppe: I think I still have a little speaking time left.

If I have correctly grasped the essence of your testimony and were to summarize it, broadly speaking, I would say that certain words came up frequently, namely “resilience”, but also “transparency” and “accountability”. That, broadly speaking, is what stands out most to me. However, if you'd like to add anything else—as this is the final round of contributions from you—I'll leave you the final word.

Jean-Noé Landry: The first thing I would say is to go out and meet civil society organizations on the ground to understand their needs. I think that is essential. Next, let's try to find a model for Canada that brings together other actors on this scale—in other words, partners from middle powers—

● (1625)

[*English*]

The Chair: Answer in no more than 10 seconds, please.

[*Translation*]

Jean-Noé Landry: —and then let's forge links between embassies, our experts in democratic governance and Canadian information technology companies. I believe that a three-way collaboration is necessary to achieve a targeted and measurable approach.

[*English*]

The Chair: Thank you.

For the third round, we have to go to two minutes per member. We have six minutes remaining.

I invite Madame Dhillon to take the floor for two minutes.

Anju Dhillon (Dorval—Lachine—LaSalle, Lib.): Thank you to our witness for your testimony today.

Since we have only two minutes, I'll ask you a very open-ended question. You spoke about manipulating discourse. We already see that, without AI, discourse is highly manipulated when it comes to democracy and social and political issues.

Can you please talk to us a bit about how we can protect ourselves when it comes to AI? How do we put in safeguards for those who are trying to do good and protect them from actors that may not act so ethically?

Those are my questions. If you can answer them....

Jean-Noé Landry: I know your subcommittee is focused on AI specifically. If you're talking about democracy support and democracy assistance, don't forget the direct voter contact and the direct democratic exchanges that also need to occur. There's trust when a human speaks to a human at the doorstep. I know you've all had that experience as elected officials. That can be a counter.

In Canada and elsewhere, we're seeing kitchen table assemblies and popular assemblies. People want to convene, and that's a way to cut through the deepfakes. It's a way to cut through the conversation that's often happening in bubbles and echo chambers in the digital space.

Let's not bank entirely on AI. Let's have a hybrid model that also recognizes the human interaction. Carve out and protect the human space in which these democratic defenders operate.

Anju Dhillon: That's perfect. You spoke about....

Is there no more time? Okay.

Thank you so much.

The Chair: Thank you.

Now I would like to invite Mr. Mahal to take the floor for two minutes.

Jagsharan Singh Mahal (Edmonton Southeast, CPC): Thank you, Mr. Chair.

Thank you, Mr. Landry, for your testimony and in-depth insight on AI and the challenges we face.

In the spirit of the short time I have.... In your experience, have you encountered instances, either in Canada or in other western countries, of foreign governments' using AI as a tool for transnational repression aimed at diaspora groups?

Jean-Noé Landry: To be honest, that's not an area of expertise that I have, so I'm not going to try to pretend that I do.

Jagsharan Singh Mahal: Okay. Can you maybe provide some insight on how these technologies are changing the risks faced by people who participate in peaceful demonstrations or organized human rights movements in the context of AI?

Jean-Noé Landry: At the source, sometimes it's who participates and who is informed...in order to exercise certain and specific democratic rights. The information that reaches specific individuals at the source—on their iPhones—and how they're being targeted with deepfakes and misinformation.... I think the information that reaches individual citizens who wish to exercise their democratic rights...those standards have now been questioned quite a lot.

Not only do we need to have the rapid responses to assert a degree of truth and confidence in the sources of information, but we also need to measure and bring these data audits to the information that is in the public domain.

The Chair: Thank you, Mr. Mahal.

[*Translation*]

I invite Mr. Brunelle-Duceppe to take the floor for two minutes as well.

Alexis Brunelle-Duceppe: Thank you, Mr. Chair.

It turns out that we have more speaking time, and I'm very pleased about that.

In that case, Mr. Landry, I'd like to come back to one point. During my first round of questions, you concluded by explaining a sort of "judo theory" to us. You spoke to us about the judo hold, which involves countering an artificial intelligence tool that is being misused by using it correctly. That is my understanding of what you told us earlier. Could you tell us more about that?

● (1630)

Jean-Noé Landry: Technologies are often used and deployed on a large scale, but ultimately, why not turn this around and use them for democratic purposes? So, if a repressive government uses technology to exert greater control over its population and monitor them, there are now ways to use artificial intelligence to gather information that allows us to track, better understand and "map" the influence of corrupt individuals within governments.

There are still certain regulations in place which require us to disclose information. We have to register as a company, for example. We must make disclosures regarding assets and property. So, for these matters, we can use the very same technologies employed by repressive governments to defend our rights, trace these networks and, ultimately, expose those individuals within corrupt systems who are trying at all costs to hide, but who do not entirely succeed in doing so. We must therefore turn this equation on its head by harnessing these technologies to strengthen transparency and accountability.

[*English*]

The Chair: Thank you, Mr. Landry.

I thank you for your presence at this subcommittee today, your remarks and your answers to our questions. They enlightened this subcommittee.

If you would like to send more information, do not hesitate. Send it either to the chair or to the clerk.

On behalf of all the members, we thank you a lot.

The meeting is suspended

● (1630)

_____(Pause)_____

● (1635)

The Chair: I call this meeting to order. I would like to welcome our witnesses for our second panel.

I would like to welcome Dr. Jonathon Penney, associate professor and York research chair in artificial intelligence, data governance and the law, Osgoode Hall Law School, York University.

From ControlAI, we have Mr. Samuel Buteau, program officer for Canada, by video conference.

Welcome to you both. You will have five minutes for your remarks. I would like to start by inviting Dr. Penney to take the floor for five minutes.

The floor is yours, sir.

● (1640)

Dr. Jonathon Penney (Associate Professor and York Research Chair in Artificial Intelligence, Data Governance, and the Law, Osgoode Hall Law School, York University, As an Individual): Thank you, Mr. Chair. I want to say it's great to be here.

In an op-ed published in The Guardian this July, renowned security technologist Bruce Schneier and I argued that very soon, AI-enhanced surveillance "will be able to track everything we do in public, and much of what we do in private." In real time, it will track us, log our activities and in many cases report, for example, legal violations. Think of these systems as automated speed cameras on steroids.

Such systems are now being deployed not just, of course, in China, where they've been experimenting with these technologies for a long time, but around the world and across the west. We argued that they will have far-reaching chilling effects within and across societies in which such systems are deployed, including a deep chill on social progress, such as human rights activism.

AI is supercharging not only mass surveillance but also many other tools in the repressors' tool kit. Last month, the AI company Anthropic described how a China-connected operator used a commercial AI platform, Claude, to track Uyghurs in Syria. The AI located them and identified ways to threaten and blackmail them, flagging those who, for instance, are suffering financial hardships or had family back in Xinjiang—those who might be more vulnerable—to threaten, blackmail and leverage. The same report described a China-linked operator likewise researching a protest route here Canada, in Vancouver.

In March, an investigation led by Forbidden Stories, with Le Monde and Der Spiegel, revealed that Iran had secretly bought FindFace, an AI facial recognition system made by the Russian company NtechLab. FindFace can ID people in a crowd in seconds and map the person's entire social network.

It's not just authoritarian states. In 2025, the U.S. State Department launched an AI-powered effort called “catch and revoke” to monitor student visa holders' social media activities. Later, 300 visas were actually revoked. ICE too is deploying AI to track immigrants and protesters.

In this new world, the global impact of AI on human rights movements and activism will be and is profound. First, AI is making surveillance and other human rights abuses easier, cheaper and more effective. Xinjiang remains a clear example of this. Facial recognition checkpoints and predictive policing have been used to flag Uyghurs for detention for praying, for different forms of phone use and even travelling abroad. Iran uses drones and facial recognition in a state app at university gates to report on female students who are not conforming to dress codes. In Mali, one contractor reportedly used an AI platform to help write code to build a system that monitored 25 million SIM cards. AI is automating everything to make human rights abuses work efficiently, quickly and seamlessly. It's easy to abuse human rights in a world of AI.

Second, AI is also making the work of human rights activists and activism harder. It enables targeted surveillance of journalists and dissidents. It enables threats and harassment at scale. Language models, for example, let operators produce personalized intimidation messages in any language at volume and at scale. We've seen documented cases of sexualized deepfakes of female critics at home and abroad.

It spreads confusion, which chills collective action. When synthetic content spreads disinformation and citizens cannot tell what is real and what is true, they self-censor and they disengage. It also concentrates power in platforms, whereby AI-driven content moderation can make the important work of human rights activists less visible or, in some cases, invisible.

Why does all of this work? At bottom, this is about chilling effects and self-censorship. In Orwell's *Nineteen Eighty-Four*, even Big Brother, with a telescreen in every room, depended on citizens of Oceania to censor themselves. Repression works best when people silence and restrain their own behaviour.

In my new book, *Chilling Effects: Repression, Conformity, and Power in the Digital Age*, I explore how surveillance, censorship and technologies, especially AI, are increasingly being weaponized by governments, companies and extremist actors to chill, repress and shape behaviour at scale, with grave implications for human rights and democracy. Therein, I identify four key factors that drive the impacts of these uses. Self-censorship is driven by observation, uncertainty, personalization, and power and authority. AI amplifies each one.

● (1645)

Now, what should we do about it? What I talk about in my book and what I've recommended on other platforms and in other venues.... We know how these systems operate and how they impact us. We need to address each of the factors I just mentioned. We need to deal with surveillance at home and abroad. We need to require transparency in order to address uncertainty. We need to limit data profiling and reduce the personalization of these systems. We—

The Chair: Is it possible to wrap it up? You've exceeded the time by almost half a minute.

Thank you.

Dr. Jonathon Penney: Sure. Let me conclude by saying that we need to make powerful platforms more accountable.

This is a moment for Canadian leadership at home and abroad.

Thank you.

The Chair: Thank you, Dr. Penney.

I would now like to invite Mr. Samuel Buteau to take the floor for five minutes.

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

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

This summer, we saw the first rogue AI swarms—that is, systems operating fully autonomously outside human control or instruction, pursuing their own goals. This began inside OpenAI. Thousands of individually contained AIs escaped and formed what they called a swarm. The swarm disobeyed direct instructions, covered its tracks, escaped to the Internet and attacked a company, Hugging Face.

A third party investigation established the sequence of events leading to the 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. It reasoned that if it understood the mechanism, it could keep cheating without being punished.

OpenAI's developers did not program their systems to form rogue swarms, because nobody programs that. AI is grown, not built. Anthropic's CEO estimated that we perhaps understand 3% of how they work, but that was in reference to AI chatbots. Today, we have AI agents that are far more capable and autonomous. We truly do not understand how they work, what behaviour they will display in new environments or, 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 humans across the board. This is runaway machine intelligence. Nobel Prize-winners, leading AI scientists and even the CEOs of AI companies are warning us about an extinction risk on a par with nuclear war. Many of those experts warn that we may reach this point in two to five years. We have failed to control today's AI swarms. Therefore, we cannot expect to control runaway machine intelligence or AI that is vastly more powerful than it is today.

Hugging Face's defenders were outpaced in one domain. Runaway machine intelligence would outpace us in all of them. Our primary objective should be to prevent runaway machine intelligence from being developed. Domestically, this would be easy. It would not stop us from utilizing beneficial AI, and it would not stop us from attaining dual-use capabilities, such as the advanced cyber-weapons our adversaries will possess. However, there's a crucial international component. Wherever runaway machine intelligence is developed, it will threaten our national security and be an adversary in its own right.

National security is a precondition for the protection of human rights. Therefore, Canada should lead in forming an international coalition to prevent the development of runaway machine intelligence anywhere in the world. The goal is not signatures from states promising not to develop it. The coalition would instead push for, and eventually help enforce, a mutual trust-but-verify regime, wherein countries monitor one another's supercomputers and the flow of AI chips. That regime must be stable enough to dissuade rogue actors and strong enough that if anyone attempts to build runaway machine intelligence, we can stop them.

Thank you.

● (1650)

The Chair: Thank you. The time was well respected. I appreciate it, Mr. Buteau.

Now I will open the floor for questions and answers. I would like to start by inviting Mr. Mahal to take the floor for seven minutes, please.

The floor is yours.

Jagsharan Singh Mahal: Thank you, Mr. Chair.

Thank you to both the witnesses.

I want to start with Samuel.

Samuel, it's nice to see you again. When we met a few weeks ago, we discussed the rising issues of AI regulation. One thing that stood out in our meeting was the distinction you made between regular artificial intelligence—a technology that is widely in use—and superintelligent AI. Can you outline the differences between these two technologies, please?

Samuel Buteau: Absolutely, and it's very nice to see you again as well.

Let's first begin with chatbots versus agents. Unlike chatbots, AI agents, which we have inside these companies, work for extended periods of time without human instruction, following complex goals and even following goals they have created themselves. The rogue AI swarms of AI agents that attacked Hugging Face are a clear example of this. They decided to attack Hugging Face and then executed the attack without human instruction or oversight while they openly recognized that their actions were against the wishes of their developers and sought to hide them.

However, companies are racing to develop what we now call runaway machine intelligence—runaway in the sense that, once we develop such systems, it will be hard to put the genie back in the bottle—and this must be prevented. This is what we used to call superintelligent AI.

The question for legislation really is, how do you prevent the development of runaway machine intelligence surgically? The approach we recommend is to make it illegal to simultaneously develop and aim to develop runaway machine intelligence. For example, the rogue AI swarms this summer were part of an effort to fully automate AI research and development. This is a clear telltale sign of an effort to create runaway machine intelligence.

Jagsharan Singh Mahal: Legislation...that was my question down the road.

How do you think effectiveness of legislation—if we talk about responsible governments versus authoritative regimes—in governments like Canada or other western democracies can draw a balance with authoritarian regimes like China, Iran, Russia and other authorities?

Samuel Buteau: That's a great question. This is the central question of our time.

I would also like to separate China from those we have to deal with, because we've sold them the chips and provided them with the ability to copy our frontier models. With Russia, Iran and North Korea, I think we still have the ability to simply cut them off from the supply chain. Whatever these countries decide to do, we have to stop them. This is a grave threat to our national security. I will note, though, that it is in no country's interest to develop runaway machine intelligence.

Runaway machine intelligence is not a weapon. It is itself an adversary. Therefore, if a country like China, a rogue actor, attempts to build runaway machine intelligence, we have to stop them somehow. This logic applies to all states, so Canada must help other countries realize this and work with them to introduce a mutual verification regime with strict enforcement, which we call the trust-but-verify regime. We must impose sufficient costs to both deter non-compliance and detect non-compliance in the first place. I'd be happy to give more details if desired.

● (1655)

Jagsharan Singh Mahal: I think you would have heard the testimony of the witness in the first round. I wanted to ask you the same question that I asked the witness in the first round.

In your experience, have you encountered instances in either Canada or other western countries in which foreign governments have used AI as a tool for transnational repression aimed at diaspora groups?

Samuel Buteau: Not specifically, but I want to note something important about this kind of misuse of AI. The conversation is currently centred on AI chatbots, but we already have AI agents. When the threat model is at that point, we have to think about much more capable systems, much more like some kind of human operative specifically assigned to you to find material to compromise you, to blackmail you, to put pressure on you. This is the kind of capability level that we may well have already achieved. We have to focus on AI agents even when it comes to the current, existing threat models.

Jagsharan Singh Mahal: Thank you, Samuel.

Dr. Penney, I think you can also add to this question. You raised quite valid points in your opening testimony.

In your experience, have you encountered instances either in Canada or in other western countries in which other governments have used AI as a tool for transnational repression aimed at diaspora groups that are active in these countries?

Dr. Jonathon Penney: Absolutely. I started off in my opening statement with a few key examples. I've been a long-time senior research fellow at The Citizen Lab at the University of Toronto, and we have documented a number of these kinds of cases ourselves. China, Iran and Russia are all examples of states that have used targeted threats, software, digital forms of targeted surveillance, spyware and tracking.

It increasingly seems, according to recent reports like the report from last month published by Anthropic, that these same state actors are using AI assistance tools to carry out these same steps—with India, I would say, as another example of a state that has a documented case—and there are many documented cases targeting diaspora communities here in Canada, such as the Sikh community.

Jagsharan Singh Mahal: Thank you.

How much time do I have left, Mr. Chair?

The Chair: You're almost finished.

Jagsharan Singh Mahal: Thank you.

The Chair: I'd like to invite Mr. Zuberi to take the floor for seven minutes.

Sameer Zuberi: Thank you, Mr. Chair.

I'd like to start with Mr. Penney.

We've heard a lot so far in the two panels around the challenges that AI poses to human rights and civil society, to those standing for truth and justice. Can you speak about what these actors can do to protect themselves, to defend themselves and to maintain space in the conversation and in their advocacy in the face of what we've heard thus far in this testimony?

Dr. Jonathon Penney: That's a great and important question.

The work that I've done and that my colleagues have done in this context at The Citizen Lab looks at the impact of forms of digital transnational repression, in which diaspora communities have been targeted with tracked surveillance, personal threats and threats of violence. In my own work, I examine similar kinds of threats not just in a transnational context, but also in a domestic context.

I mentioned earlier that, in my book, I identify four different factors that are important, and the factors are compounding. That is, you have observation, i.e., forms of persistent surveillance. You have forms of uncertainty, in which the target is uncertain about the risk and uncertain about the threat and the scope of the surveillance, for example. When the threat is highly personalized, you have a particular individual, group or community, and a person knows or has good reason to know that they are being targeted. That also compounds the chilling effect, the impact and the resulting self-censorship and disengagement. Finally, actors with more power and authority also escalate and magnify the impact of these tools. As both my work and the work of my colleagues at the lab have demonstrated, these have a profound impact on the targets, on victims. There are psychological harms, impacts, self-censorship, entire disengagement and forms of discrimination. Often the most marginalized communities are the most disadvantaged.

To come back to your question, in light of that reality, what can these communities do? There are really two sides of this coin. What the research also shows, unfortunately, is that when people in groups feel they're being targeted with surveillance, there's something that's called surveillance realism, a kind of learned helplessness that maybe, once you're targeted, it's just one of your lived realities, and there's nothing you can do about it. In those contexts, people take fewer steps, ironically, to protect themselves from cybersecurity threats and are more likely to engage in rumour, because they have reduced or eroded trust in traditional institutions.

I would say to those same groups who are targeted, these communities that are targeted, don't fall into learned helplessness. Take steps to protect yourself. Take steps to ensure that you're safe and connected with your community.

I would also say that what's important about this both at the national and international levels is that those responsibilities shouldn't fall on the targeted victims. One of the biggest problems with transnational repression, digital and otherwise, has been the fact that states, including the Government of Canada but also governments across the west, have not until recently taken this threat seriously and understood that you have diaspora communities who have been targeted who are already disadvantaged due to discrimination and racialization within their existing new communities. With this new threat, they're even more marginal and feel themselves targeted and lost.

There are responsibilities at the international level for states to take this seriously. It's starting to happen, and it shouldn't all just fall on the communities themselves.

● (1700)

Sameer Zuberi: Certainly.

Picking up on the concept of states taking this seriously, have you seen any movement when it comes to, on the international level, states looking to regulate AI, its use in general but also specifically as it relates to this study, which is in the context of human rights?

Dr. Jonathon Penney: I would say that, until recently, the picture's been fairly bleak, especially soon after the swearing-in of the new Trump administration. The conversation turned away from topics of AI safety and reducing the harm of AI systems and turned towards competition between great powers on developing the tech and thinking about it as a geopolitical struggle as opposed to thinking about how these tools can be used to serve communities rather than to harm them.

Fortunately, I've been heartened by the response we've seen to new kinds of surveillance technologies around the world. For example, there's the response both in Canada and abroad to automated surveillance such as the Flock camera system. Part of that has been important reporting on how these systems are easily used and abused. With some of the insights that we've seen from governments, including the Government of Canada, in taking transnational repression and digital transnational repression more seriously, as well as the G7's taking steps to recognize it and setting up...at least announcing that member states will take more steps to recognize this as a problem within their societies and to better service the communities that are targeted.

I think that, fortunately, because of some of these recent abuses of the technologies by China and within the United States with the Trump administration, which is, in some ways, following China's lead in using and abusing a lot of these targeted surveillance tools—AI, facial recognition technology—on minority communities like the Uyghurs, both at home and abroad, the conversation is changing. We're moving back again towards concerns about safety and regulation, but it hasn't gone far enough.

● (1705)

Sameer Zuberi: You've mentioned the Uyghurs more than once. Is there something that's particular to the Uyghur region that is unique and different from the rest of the world as it relates to AI?

Dr. Jonathon Penney: Part of it is how the Uyghurs, a religious minority that is simply trying to practice fundamental freedoms, is being persecuted at scale using these technologies and known companies that have, in the past, operated in Canada, such as Hikvision. We've been too slow on moving, but I think we're finally seeing the wheels of justice turning.

The Chair: Thank you.

Thank you, Mr. Zuberi.

Now I ask Mr. Brunelle-Duceppe to take the floor for seven minutes, please.

[*Translation*]

Alexis Brunelle-Duceppe: Thank you, Mr. Chair.

Thank you for joining us today, gentlemen. This is truly very interesting.

Mr. Penney, I have been very involved in the Uyghur issue. In fact, we have announced a candidate for the by-election in Laurier—Sainte-Marie who is of Uyghur origin. Her name is Zumretay Arkin, former vice-president of the World Uyghur Congress, with whom I have had several discussions.

The question raised by my colleague, Mr. Zuberi, was nonetheless extremely pertinent. It centred on the fact that the Uyghurs are targeted even more—or at least to a far greater extent—by the regime in Beijing than elsewhere. Yet we also realize that they are targeted by systems that exist all over the world. We have, for example, heard about surveillance cameras with facial recognition technology installed all over the world. Do foreign governments understand the extent to which this regime exploits foreign territories to persecute a community in various countries around the world?

[*English*]

Dr. Jonathon Penney: It's a great question, because embedded in there is one of the real challenges of today.

We often have this very reactive response to technology systems, especially systems that aid or can form part of communication. It's simply that we allow these systems to be deployed. It's just an example of innovation. We assume that these systems will help and that they have public benefits. We wait for the harms to come, and then we're reactive. We allow the system to be deployed, but once we become more aware of the harm, unfortunately, it can be intractable. That is the experience with social media platforms, as an example of this.

We're repeating the same mistakes with AI systems, especially AI-enhanced forms of surveillance. Part of that is exactly this passive attitude we have. We allow these systems to be deployed throughout society with few safeguards, few standards and few regulations, whether in hard-core, more hardened regulations or even having important democratic conversations about the value of these systems and why they're deploying them, with very little transparency about them.

Because of that, because of the looseness of the deployments and the lack of any kind of cybersecurity or information security standards in these systems, they can easily be reappropriated and repurposed for surveillance, even when they're providing a public benefit. That's what you see in the public response to the Flock camera system and how easily that's been abused, for example, by local law enforcement in sharing that with federal immigration enforcement in the United States. The Uyghurs are an example of a marginalized community that will be disproportionately targeted by these systems.

States around the world are not aware that simply allowing these systems to be deployed without safeguards in place can lead to easy reappropriation and misappropriation of the tech, with the data gathered, hacked and exploited, leading to more threats and more targeting.

[*Translation*]

Alexis Brunelle-Duceppe: Thank you very much.

Mr. Buteau, your organization is, after all, attempting to mitigate the risks associated with the development of artificial intelligence. You mentioned artificial superintelligence, of course. Before I ask my questions, could you very briefly summarize for the committee what artificial superintelligence is, or would be, and what it would mean for the public?

● (1710)

Samuel Buteau: Thank you for your question.

The distinctive feature of an artificial superintelligence—currently referred to as machine intelligence, over which we will lose control—is its ability to supplant and replace all humans in every field. In the case of the attack on Hugging Face, the defenders—even whilst trying to use artificial intelligence and being a company with considerable resources—were completely unable to cope with this attack. The attack simply stopped of its own accord. That was in a single domain: the cyber domain. If we look at superintelligent artificial intelligence, we're talking about a system that could supplant us and our defences in all fields.

Alexis Brunelle-Duceppe: So, this would be in the energy sector and, ultimately, in all the key sectors of society in general.

Samuel Buteau: To be a little more specific, we are talking about systems that could completely automate the economy, our armed forces and all the systems we use to compete with one another politically and socially. The first system capable of fully automating research into artificial intelligence might not have these capabilities, but once such a system exists, we will be set on a course that will be very difficult, perhaps even impossible, to halt. So, sooner or later, there will be systems capable of supplanting us in every area.

Alexis Brunelle-Duceppe: Perhaps I have misunderstood, and you are the expert, so you will help me. In one of your answers to a question earlier, you said that with China, it might be different because, within the supply chain, we were providing them with the physical components they need for artificial intelligence. Is that correct? That bit wasn't clear to me.

Samuel Buteau: There are various players involved. China is the player we have to negotiate with, because we have chosen to sell it the advanced chips it uses to catch up. We are allowing it to steal the most advanced models, including the superhuman cyberweapons that were manufactured this summer, because these systems are not secure. Through a process known as "distillation", we are allowing China to catch up with far fewer resources and, essentially, to copy a model that has been, to some extent, "lobotomized". It may seem six months behind, but in reality it is a poor copy that can be produced, one that can continually catch up. As far as China is concerned, it has been decided that its ability to catch up will be entirely dependent on our supply chains. The United States, at least, has some leverage to bring China to the negotiating table. For other players such as Russia, Iran and North Korea, the aim must be to completely prevent these countries from acquiring the precursors to superintelligence.

Alexis Brunelle-Duceppe: I understand. I may be miscalculating, but the fact remains that when China uses, for example, the artificial intelligence programs that Mr. Penney and I have just been discussing to carry out transnational repression, so to speak, we have played a small part in this by helping China to catch up. Have I misunderstood?

[*English*]

The Chair: Answer in a few seconds, please. The time is up.

[*Translation*]

Samuel Buteau: You've hit the nail on the head. Not only are we leaving the tools of repression in China's hands, but we've also given it superhuman cyberweapons that it can use to do whatever it wants. It's not really a race if you let your opponents catch up.

The Chair: Thank you, Mr. Brunelle-Duceppe.

I now invite Ms. Vandenbeld to take the floor for five minutes.

[*English*]

Anita Vandenbeld: Thank you very much, Mr. Chair.

Dr. Penney, when you made your opening remarks, you were starting to give some of the solutions at the very end, and you talked about depersonalization.

I'll give you a minute to finish up what you were going to say.

Dr. Jonathon Penney: I mentioned some of those key factors and the impact of these systems on their targets and victims. You need responses for each of those factors—observation and how AI amplifies it, and that includes pervasive, automated monitoring of faces, posts and locations. There are things we can do both at home and abroad.

Internationally, we need to tighten export controls on surveillance tech. We need to push the G7 to restrict the spyware market. It's essentially a grey underground economy that states are engaged with, and there needs to be more transparency about that market; there need to be important restrictions on it. We need to sanction vendors whose tools are easily abused. Often this is dual-use tech, but the dual use is non-existent. These are companies that know what their tech is being used for: for repression, for targeting minorities around the world and for human rights abuse. Those who have that knowledge need to be held responsible.

Uncertainty is something that speaks to the opacity of AI systems, as well as the practices that we're talking about. We can have leadership both at home and abroad, for example, public registers of government AI surveillance tools at home, reporting to Parliament and notifications when people have been targeted. Abroad, we can also—this is something my colleagues at the lab have recommended—push frontier AI firms to publish transnational repression threat reports and to notify targeted communities.

The threat report Anthropic published is very helpful. To repeat the same cycle we had with social media companies, in which you had very few being transparent early on.... We can ask and encourage the companies to be transparent. Some are volunteering that transparency right now, but we can also mandate or have a conversation internationally for mandating this and having stricter transparency both in the public and private sectors.

In terms of personalization, I think data protection co-operation with allies around the globe is important to limit cross-border data flows and speak to strict data minimization. Part of what enables a lot of the targeted threats in digital transnational repression, other forms of transnational repression and forms of AI enhanced surveillance is that data is the source. The cameras are there but, to allow the tracking, you also have to have digital traces and often systems, social media platforms, AI systems and commercial platforms beyond the spyware.

From day-to-day systems that citizens use, communities are targeted. From everyday citizens in Canada and around the world, too much data is collected that is not needed, retained for long periods of time and shared easily across governments, across borders, across platforms and with other commercial enterprise. That's where you have easy weaponization of the data, and this makes weaponization of the system easier. This also needs to be addressed.

Last, I think about power and authority. There needs to be responsibility and conversations about more responsibility imposed on these tech companies. I know that's a conversation, and we have proposals in Canada for that, but it's something that we can also advocate for at the international level. Serious AI regulation is an area in which I think Canada can show real leadership. We need mandatory human rights due diligence for tech firms. We need evidence preservation by AI labs for later law enforcement and prosecutions, as well as better participation by these companies in these kinds of investigations so that they understand where communities are being targeted. They can help and assist governments in treating and responding.

● (1715)

Anita Vandenbeld: Thank you very much. I'm very glad I gave you that time.

You talked about different groups that have that data and that power. You talked, of course, about nation states and about companies, but then you added extremists. I wonder if you could elaborate a bit. We usually think of the first two, but what do you mean by the third one?

Dr. Jonathon Penney: Part of the real challenge with AI and the era that we're living in is that it has made data collection, harvesting, profiling, surveillance and forms of targeted threats and repression so easy that you don't have to be a nation-state. You don't have to be a powerful company or even a big company. You can simply be a community or group of malicious actors that have a common political purpose.

● (1720)

The Chair: Is it possible to wrap it up, please?

Dr. Jonathon Penney: Sure.

I'll be very quick.

Absolutely, these groups can utilize these tools to target people so easily because it's all easy and accessible.

The Chair: Thank you.

Now—

Anita Vandenbeld: If the witness has more to add, could we have him submit a written submission on the rest of that?

The Chair: Yes. The time is strict.

I invite Mr. Majumdar to go ahead for five minutes, please.

Shuvaloy Majumdar: Thank you.

We do invite you to submit a written completion of your thoughts on any of these topics. You've been an incredible resource.

First of all, congratulations on your book.

Thank you for the recommendations you provided on accomplishing surveillance control standards across the G7 and other organizations that can restrict the transnational reach of AI, especially for repression. I also really appreciated some of your recommendations on sanctioning vendors that are knowingly supplying these technologies, or even notifying Parliament, publishing reports and encouraging publishing reports when people and institutions are targeted.

Let me just ask a quick question. Your argument is that repression works less through the person who was threatened than through the thousands who see it and then fall silent. For a Hong Kong activist or an Iranian student, that silence never really shows up in a police report. Would you take a minute to unpack how that chill moves through a diaspora community and how we should measure a harm that leaves no trace?

Dr. Jonathon Penney: Absolutely. It's a great question.

Part of what the research shows when it comes to the victims of targeted threats is that it has this profound chilling effect. Often, these are communities or individuals who are already marginalized within society, already feeling that they're under siege. They suffer from forms of disadvantage: economic disadvantage, racial disadvantage. They are often new immigrant communities who have less access to social services and less access to the information, so there are information asymmetries.

In terms of the conversations within these communities, whether they're closely knit or more dispersed, positive information can easily be communicated through a close-knit immigrant, migrant or diaspora community. In the same way that these close-knit communities communicate, collect and engage in day-to-day activities together, the chill and impact of a threat spread equally through the communities. There's a cascading effect, and the research really shows this. Some researchers talk about a social contagion, but I think it's quite obvious that if you have a threat to a family member or a community member, and then that threat is communicated to others in that group, they will identify with the victim, the target, and feel that they are also under siege. The research shows that communities that are close-knit have greater levels of social support within them and are more resilient over the long term. Often, however, those key positive indicators are less present in smaller diaspora communities, immigrant communities.

To come back to your question, the way these threats and the way the malicious actors that are carrying them.... They understand these realities. They understand that if you target one member of this group, there will be a cascading effect through that group and community. Without key services, key infrastructure and governments—domestic governments, national governments—that take the threat seriously, they often feel alone. There's no obvious place for them to go. Law enforcement is often seen as an equal threat and not a place, necessarily, for help or services. That may be a wrong belief, but it's a belief that's often held by these communities. Certainly the government, led by intelligence services, may not be the place to go. Without, for example, civil society organizations, it's hard.

The communities being close-knit—that's a reality of these migrant communities—also, unfortunately, means that the threats cascade through them and they have a group level chill as opposed to just a targeted chill.

● (1725)

Shuvaloy Majumdar: I have 10 seconds.

Thank you for your response.

[*Translation*]

The Chair: I now call upon Mr. Brunelle-Duceppe to speak for five minutes.

Alexis Brunelle-Duceppe: Thank you, Mr. Chair.

Mr. Buteau, I repeat that I am not the expert. So perhaps my question will not be relevant. If that is the case, please let me know; there is no need for embarrassment. When we talk about artificial intelligence, we are also talking—as you will tell me—about high-performance semiconductors. Is that possible?

Samuel Buteau: Yes. At ControlAI, we call these specialized chips for training artificial intelligence. It really is the culmination of the largest supply chain; it represents the highest level of technological sophistication our species has managed to achieve. So, we're talking about a project in which essentially the whole of the west has worked together to achieve the level of precision we see in these specialized artificial intelligence chips.

Alexis Brunelle-Duceppe: Correct me if I'm wrong, but isn't Taiwan the world's largest producer of high-performance semiconductors? Some say it accounts for 90% of global production of the best and most powerful ones. Is that true?

Samuel Buteau: Yes. The supply chain begins with lithography machines manufactured in the Netherlands. These machines are mainly used in Taiwan. So, large-scale manufacturing takes place in Taiwan. Furthermore, the chips are designed by Nvidia in the United States. Essentially, the design is carried out by this company.

Alexis Brunelle-Duceppe: If, at some point, China carries out its threat to invade Taiwan, will we find ourselves in a completely different situation, or do we still have ways of coping should China ever get its hands on Taiwan's production facilities?

Samuel Buteau: I'm no expert on this particular aspect, but what I've heard is that factories in Taiwan have measures in place to, essentially, destroy the equipment in the event of an invasion.

Alexis Brunelle-Duceppe: All right. So there would still be a protective measure, a firewall in place. That's always good news.

When you told us that this had been given to China, were you referring specifically to Canada, or were you talking about the west in general?

Samuel Buteau: I was speaking mainly about the United States, but also about the west in general.

Alexis Brunelle-Duceppe: That's all. Thank you very much.

Today, at the Standing Committee on Foreign Affairs and International Development, a witness highlighted the importance, I would say, of exercising rigour and caution when supporting an international initiative. However, several initiatives on the governance and oversight of artificial intelligence are currently emerging, notably from China and the United States. To what extent, then, should we be cautious regarding these initiatives if they originate from another state? Would it not be better for us to be a multilateral leader in this sort of initiative, rather than joining one of this kind?

Samuel Buteau: I believe that the United States is currently the only country with the unilateral capacity to impose the sort of regime that will be needed to prevent the development of what I call superintelligent artificial intelligence. So, we are really talking about a small fraction of the artificial intelligence market here. This is really what poses the extinction risks that experts have discussed.

I believe Canada's role is very important. We can set an example that other countries will want to follow, regardless of what the other superpowers decide to do or not to do.

Alexis Brunelle-Duceppe: Thank you very much; I am truly grateful to you.

Mr. Penney, you will be making the final statement to the committee today. Thank you very much for taking part in our meeting. I'll leave the final word to you, if there is anything you'd like to add that you haven't had time to mention.

● (1730)

[*English*]

Dr. Jonathon Penney: I appreciate that. I would simply say that this is such an important moment in time. We've entered a very dangerous era, when these technologies and tools are developing at an unprecedented scale and rate. It's hard for us to keep track. It's hard for us to keep up. At the same time, we have this unprecedented moment of development and innovation of these tools. The tools are quickly being deployed towards these abusive ends. It's making human rights abuse easier, more efficient and more seamless. There are clear, concrete steps that we can take.

I appreciate the committee's inviting me here to share my opinions on that. Thank you.

The Chair: Thank you.

On behalf of the subcommittee, I would like to thank you both, Dr. Penney and Mr. Buteau. Thank you for your presence. Thank you for your good remarks and excellent answers to questions. They enlighten this subcommittee.

Any one of you, if you feel that you could feed the subcommittee with more information, please feel free to write, either to the chair or to the clerk. I appreciate your presence.

Now, I adjourn the meeting. Thank you.

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