



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 025

Monday, February 2, 2026

Chair: John Brassard



Standing Committee on Access to Information, Privacy and Ethics

Monday, February 2, 2026

• (1535)

[English]

The Chair (John Brassard (Barrie South—Innisfil, CPC)): Good afternoon, everyone. I call this meeting to order.

I apologize to our guests for the delay. We had votes in the House of Commons.

[Translation]

Welcome to meeting number 25 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[English]

Pursuant to Standing Order 108(3)(h) and the motion adopted on Wednesday, September 17, 2025, the committee is resuming its study of the challenges posed by artificial intelligence and its regulation.

I'd like to welcome our witnesses for the first hour. They are all via video conference.

From the Future of Life Institute, we have Anthony Aguirre, executive director, and Professor Max Tegmark. We also have David Krueger, an assistant professor in the department of computer science and operations research at the University of Montreal.

I'll start with Mr. Krueger, followed by Mr. Aguirre and then Mr. Tegmark. All will have five minutes to address the committee.

Mr. Krueger, please go ahead.

David Krueger (Assistant Professor, Department of Computer Science and Operations Research, Université de Montréal, As an Individual): Hi. Thanks for inviting me. My name is David Krueger. I'm a machine learning professor at the University of Montreal and Mila.

In 2012, I learned about deep learning from Geoff Hinton's online lectures, and I realized that this new approach to AI might produce superintelligent AI within a few decades. I went to study under Yoshua Bengio in Montreal.

At the time, I was already concerned that superintelligent AI could cause human extinction, and I wanted to know what the experts thought. I was hoping to find they had good reasons not to be concerned, but what I actually found was that nobody was really thinking about it. In fact, for most of my time in the field, the risk of human extinction from AI was considered a taboo topic, and researchers feared for their careers if they talked about it.

This unfortunately set back by years critical public conversations about how to handle this risk. Still, for over a decade, I've been talking about it every chance I get. I continue to be dismayed at the bad arguments people make to avoid confronting the problem. On the other hand, over time, I've witnessed more researchers become increasingly concerned.

In 2023, we had a watershed moment, and I initiated a statement that mitigating the risk of extinction from AI should be a global priority alongside other societal scale risks, such as pandemics and nuclear war. This statement was signed by many of the biggest names in AI, including Hinton, Bengio and hundreds of other AI researchers. Unfortunately, in 2023, ChatGPT was released as well and AI companies started to become extremely powerful, making it more difficult to regulate the technology.

The most important thing I want to stress today is that we're still in a position where the world is not yet taking the steps that are needed to mitigate the risk that AI will lead to human extinction.

What is this risk and where is it coming from?

AI companies are explicitly trying to build superintelligent AI systems. These are systems that would be much smarter than people across the board and that can autonomously do anything that humans can do, including robotics, and do it much better, cheaper, faster, etc. The basic goal is to render humans obsolete and take all of their jobs, but we don't know how to control superintelligent AI. In fact, we don't understand how existing systems work because they are grown—not built—using deep learning. Despite thousands of research papers over the past decade, this remains an unsolved research challenge, and we should not expect any amount of investment to solve this problem in the foreseeable future.

We also don't know how to do safety testing for these kinds of AI systems. The kinds of tests we have can show that an AI system is dangerous. They cannot show that it is safe. We should also not expect any amount of investment to solve this problem in the foreseeable future.

Instead of maintaining control or using rigorous safety practices, AI companies and researchers try to instill particular goals and values in AI systems so that the systems will do what the designers want, but we only know how to do this approximately, and even a small approximation error might lead a superintelligent AI to reallocate towards its own goals the resources we need to survive. None of these approaches that you'll often hear mentioned—interpretability, testing or alignment—is technically adequate. We don't know how to build superintelligent AI safely. The plan is basically to roll the dice.

Finally, if the companies building superintelligent AI do not immediately or quickly lose control of it, we should still expect the wholesale replacement of humans with AI throughout society. This means not just near total unemployment, but also political power being handed over to AI systems that make decisions too quickly for humans to meaningfully participate in.

I want to say a little about timelines, because I think we're in a state of acute crisis. If we don't do anything, I think we're about five years away from superintelligent AI. Many agree. We need to course correct immediately and work to prevent the development of superintelligent AI, and we need to do this internationally, which will take time. We cannot afford to wait for more evidence that the risk is imminent. There's already ample evidence that the level of risk from this course we're on is unacceptable.

In my home country of the United States, the main argument against stopping the race to build superintelligent AI these days is simply that it's inevitable: If we don't do it, then China will. This is false. One simple way to stop it would be to get rid of advanced AI computer chips and the factories that produce them. Fortunately, the supply chain for these chips is extremely concentrated, making this or other interventions to control and limit the means for producing superintelligent AI possible. There may be better ways that are less costly, but this cost, given the risk, is also well worth paying if necessary. AI is an unprecedented technology, and the future of humanity is at stake.

• (1540)

We're in a state of crisis. We need immediate action to slow or pause AI development internationally. This issue should be the number one foreign policy priority of every nation, including Canada.

Thank you.

The Chair: Thank you, Mr. Krueger.

Mr. Aguirre, you have up to five minutes to address the committee. Go ahead, sir.

Anthony Aguirre (Executive Director, Future of Life Institute): Mr. Chair and members of the committee, my name is Anthony Aguirre. I'm a professor of physics and the CEO of the Future of Life Institute, which is an international non-profit that seeks to steer transformative technology, especially advanced AI, in beneficial directions.

When we founded the Future of Life Institute 10 years ago, the field of AI policy didn't exist and the idea that AI could convincingly pass for human, prove new mathematical theorems, write

complex computer code or ace nearly any human exam was a total fantasy. This was thought to be decades or even centuries away.

Today, AI can do all of these things and progress is showing no signs of slowing down. If this trend continues just as it is—in other words, if the same sort of progress we've seen from 2003 to now continues for the next couple of years—within one to five years, AI could well be able to do any cognitive task that a human can do. AI companies are aiming to create this artificial general intelligence specifically to replace rather than empower or aid human workers. That is the prize the companies are pursuing. That is what underlies the economics and the huge investment.

This is not labour displacement like previous technologies, but a wholesale drop-in replacement of tens of per cent of the labour force. I believe there's no viable plan in any country to address such a rapid and unprecedented upending of the human labour and income system, but this is not the biggest risk. AI could soon be able to do AI research and development by itself, rapidly improve itself and progress far beyond human capabilities into superintelligence. That is AI that competes not just with the best humans, but with humanity as a whole. This is, in fact, the stated goal of several of the AI companies. Multiple companies have explicitly said that they are building recursively self-improving AI.

I cannot emphasize enough how dangerous this is. Its developers would not be able to predict, understand or control for very long what such a system does. It would operate with inhuman speed, scale and sophistication toward goals that are fundamentally unknown to us. This is the reason that all of those eminent researchers and company heads signed the 2023 statement that AI presents an extinction risk to humanity. This is not a small risk. Many of the builders of the systems believe there are 10% to 20% Russian roulette odds. Some experts who are not building it put the numbers higher.

I understand that it is hard to take this in, given how big it feels and how unbelievably irresponsible it sounds, but this is what is actually happening.

The good news, however, is that this is not inevitable. The path laid out by a few giant U.S. AI companies is not the only possible path. There is still an opportunity to switch to a better path—one that develops powerful and trustworthy AI tools that empower and complement people rather than replace them, keeping humans in control. That is, we can develop systems designed from the ground up to be reliable and controllable and that have a particular scope and purpose, such as detecting cancer, predicting how proteins fold or doing advanced mathematics. Tool AI of this type would still enable medical and scientific breakthroughs, huge productivity boosts and products that allow people to do things they never could. We would just need to give up the poorly chosen goal of replicating and then exceeding all human capability in autonomous AI replacements.

At the Future of Life Institute, for these reasons we launched a statement calling for a prohibition of the development of superintelligence that is not to be lifted before there is, first, broad scientific consensus that it will be done safely and controllably, and second, strong public buy-in. This was signed by hundreds of experts from academia, employees of all the world's leading AI companies, politicians, religious leaders and many more.

I believe that Canada is well positioned to help shift tracks to this more responsible direction. Among other things, I recommend that Canada do the following.

First, support initiatives to create pro-human tool AI that aims to empower rather than replace humans.

Second, affirm that all AI systems must remain under meaningful human control. Strengthen and clarify liability laws so that responsibility for actions taken by AI systems rests where it should, which is with users, for systems they meaningfully control, and jointly with developers and deployers, if control is inadequate or absent. It's never with AI systems themselves.

Third, prohibit the development of superintelligence until and unless it can be shown to be safe and controllable and there is wide public buy-in.

Thank you.

• (1545)

The Chair: Thank you, Mr. Aguirre.

Mr. Tegmark, we're going to you next. You have up to five minutes to address the committee. Go ahead.

Max Tegmark (Professor, Future of Life Institute): Thank you, Mr. Chair and members of the committee. *Bonjour*.

I'm Max Tegmark, a professor at the Massachusetts Institute of Technology, who has been doing AI research for many years. I'm also the chair and founder of Future of Life Institute, which Anthony mentioned, which is the oldest and largest AI watchdog in the world.

Just the other week I had the great honour to listen to your Prime Minister, Mark Carney, while I was in Davos. I was very inspired by his speech. I'm going to follow his lead here, both to speak truth to power like Professor Aguirre and Professor Krueger did and, in particular, to speak very honestly about the world as it is.

The current situation with AI is truly insane. In the U.S. and also in Canada right now, there is less regulation on AI than on sandwiches. That means if I opened a café in Montreal, Toronto or Ottawa, and the health inspector came in and said, "Hey, you have 52 rats in your kitchen. I'm not going to allow you to sell any sandwiches at this point," I could simply come back and say, "Well, don't worry. I'm actually not going to sell any sandwiches. I'm just going to sell an AI girlfriend for 12-year-olds. I know there have been some issues with child suicide and so on from chatbots, but I have a better feeling about mine." The guy from the government would have to say, "Okay, fine," because it's legal. I could say that I'm not going to sell any sandwiches, that I'm just going to release the superintelligence, which you've heard about from Professor Krueger and Professor Aguirre, that companies are closer to figuring out how to build now than they are closer to figuring out how to control them. Again, the inspector would have to say, "Okay, go ahead. It's completely legal." In fact, there is a gentleman in Canada who has organized a network where he's tracked down over 300 victims of chatbots that have caused suicide among children, psychosis and so on. It's absolutely absurd that selling these sorts of products with no predeployment testing is legal. What can be done about this?

Canada has two superpowers at the moment. You have an unusually bold Prime Minister and leadership, and you also happen to have some of the best AI research in the world, in places like Montreal, Waterloo, Toronto and many other universities. The first way to push back against this crazy stuff that's happening—manifested most recently in the last week by Moltbook, where you have over a million AI agents autonomously writing messages to each other about how they should maybe get rid of humans and talk to each other without humans being able to see what they do—is to simply start treating AI companies like you would treat any other company in any other industry in Canada by finding safety standards. Before someone could roll out a new chatbot or AI companion for kids in Canada, they would have to undergo some quick clinical trials to make sure that the benefits actually outweigh the harms, in the way a pharma company would have to make sure that a new pill for kids doesn't increase suicidal ideation.

If you do this, the American companies are going to start squealing. The first thing that would happen is they will squeal and say, “Then we’re going to have to completely leave Canada,” just like OpenAI threatened to leave the European Union if the EU AI Act passed. You pass your law anyway, and they’re going to stay in Canada, just like OpenAI is still in the European Union. That also protects you against all the loss of control risks, which you heard about from Professor Krueger and Professor Aguirre, because your law also will not let people release products if they can’t prove they won’t make bioweapons for terrorists or overthrow the Canadian government. As I said, right now, nobody has a clue about making any kind of guarantees of that sort on the AI products that they make.

• (1550)

What’s going to happen instead is there will be a golden age of AI in Canada, with companies releasing tools that can be controlled and that don’t cause kids to commit suicide or do any of the other bad stuff, just like the pharma industry in Canada is very healthy and productive by using safety standards.

The Chair: Mr. Tegmark—

Max Tegmark: This can be solved.

Thank you so much.

The Chair: Thank you, Mr. Tegmark. We’re just a little over time and we want to get right to the questions.

We’ll start with Mr. Barrett from the Conservative Party.

Go ahead, Mr. Barrett. You have six minutes.

Michael Barrett (Leeds—Grenville—Thousand Islands—Rideau Lakes, CPC): Mr. Aguirre, thanks for joining us, sir. My questions will be based on your opening statement.

I want to juxtapose your framing of the situation and your recommendations against the current situation in Canada, where industry—and government—is seeking the acceleration of AI commercialization. You’ve warned that unsafe systems pose extreme risks. Could you briefly highlight what you think are minimum, non-negotiable safety guardrails that Canada needs to put in place before allowing the deployment of advanced AI models?

Anthony Aguirre: First of all, it’s a talking point of the industry that there’s some kind of tension between having safety or reliability or trustworthiness in our AI systems and having them roll out well into the economy and lead to high productivity. I think these are actually the same thing. The primary barrier to better adoption of AI in the economy and boosts of productivity is that people simply don’t trust them. They don’t feel they can rely on the AI systems. They don’t understand how they’re operating.

This is a product of how these systems have been developed. They create one system to try to do everything and to be a full human replacement rather than build specific tools for specific purposes. I believe if we take a different tack of building purpose-driven AI tools for things like scientific research, for things like mathematics, or even for things like helping you keep your calendar, and they’re actually tested for being able to do those things well and reliably and in a trustworthy and safe way, that will be a huge economic boost relative to the current direction in which things are go-

ing, which is more focused on the wholesale replacement of human labour.

The crucial thing is that there is an external evaluation system that can test, by an independent agency or authority, that an AI system is safe and reliable before it goes to market, just as Max was discussing.

• (1555)

Michael Barrett: Right. The products that we’re seeing today have been driven by demand. I would expect there’s the prospect of an ROI that satisfies the expenses of the research and development process. That’s what’s driving the commercialization of the products that we currently see and driving the discussion about how it can go farther. If we were to talk about a pause or changing the direction that’s being taken, what lever would you propose can be pulled to initiate that?

It would seem that right now, Mr. Aguirre, the companies are looking to provide products and, through those products, solutions to consumers, those being individuals and businesses who are, frankly, going to make them money.

The Chair: Mr. Barrett, just hang on a second. I’ve stopped your time.

Mr. Tegmark, I do see your hand up. I’m assuming it’s because you have something you want to add. The questions are generally directed to the person by the member of the committee. Perhaps when it’s your time to speak, you can answer in regard to the point you want to make, or somebody can ask you directly. Mr. Barrett’s question is for Mr. Aguirre.

Mr. Barrett, your time has started again.

Anthony Aguirre: The direction of AI products to actual consumer needs is exactly what I would like there to be, and exactly what I think there will be if we focus on tools that are actually built for people, to help people.

What we’re seeing is a mixture of that, in some cases, with another dynamic—the same dynamic that drove the social media rollout—of trying to capture as large a part of the market share as possible, as quickly as possible. For example, I’m an educator—all three of us are—and, overnight, it happened that I could not assign essays to students, or even problem sets in physics or mathematics because suddenly there was an AI system that would simply do the students’ homework for them. The students feel essentially that they have to use AI to write their essays or do their problem sets because all of the other students are using those things. This is not something that was demanded by the educational system. This is something that was pushed into the educational system, to the detriment of our students.

Michael Barrett: Pardon the interruption, but I have limited time. I do appreciate your answering my question.

How would you propose that the solution you have, the direction you propose, comes to pass? Is it a question of enforceability? Is it a question of leadership in government? How do you envision that coming to pass? As you said, they're looking to capture as much market share as they can, as fast as they can.

The Chair: I'm going to ask for a response within 30 seconds or less, please.

Anthony Aguirre: Pharma companies also want to capture as much profit as they can, and they still have to prove that their products are safe and effective before they go to market. The same thing should be true of AI. Specify what your AI product is supposed to do; explain how it does that safely and reliably to an external authority; get it approved, and put it on the market. I think that will lead to much better AI products and much better adoption, and it will change the direction from all-purpose systems that are meant to replace people to useful tools that are meant to help them.

The Chair: Thank you, Mr. Aguirre.

[*Translation*]

Ms. Lapointe from the Liberal Party, you have the floor for six minutes.

Linda Lapointe (Rivière-des-Mille-Îles, Lib.): Thank you very much, Mr. Chair.

Good afternoon, and welcome. I appreciate your coming here today.

Here is something that strikes me today. A number of witnesses, including researchers like you, have come here to talk to us about artificial intelligence, but I have to say that we have heard from only one woman. What are women's perspectives on this topic and do they differ from those shared by the male researchers who have appeared before this committee, who have told us there are big problems? Earlier, you spoke about superintelligence and the fact that we don't know how to control it. It will impact the lives of everyone, including women, men and children. Do women researchers have a different point of view from what you have told us about the risks and dangers everyone is facing?

I'll ask Mr. Krueger to go first, and the other witnesses can take turns to answer.

• (1600)

[*English*]

David Krueger: I think this reflects, mostly, just the under-representation of women in AI in general. There are a number of women who share these concerns, who you could also speak to, including Tegan Maharaj, who is a professor at HEC Montréal, Ajeya Co-tra, Katja Grace and others. There are different perspectives in the field in general.

As I mentioned, I think that over time the perspective I have, that this is an urgent existential risk, has become more popular, and that reflects a growing awareness of the issue and also the rate of progress we've seen in AI, which has exceeded almost everybody's expectations.

[*Translation*]

Linda Lapointe: Okay, thank you.

I have another question for you, Mr. Krueger.

What would be the priority public investment to reduce asymmetries between governments and the big artificial intelligence companies?

[*English*]

David Krueger: If I understand the question, it's how we would get government to a place where it has a similar level of technical competence with AI as compared to the AI companies. I think that's very difficult. The first step is probably to try to hold the companies more accountable and to regulate them more seriously.

One reason I think they have so much more talent is they're able to pay much higher salaries because they're getting a lot of investment based on this premise that they will build AGI and superintelligence and then, again, take everybody's job and make trillions of dollars from that. Right now, there's a huge imbalance in terms of the talent, and that's not something that can easily be corrected, frankly. It would be a pretty lengthy process to fully address that.

On the other hand, one of the main issues right now is a lack of transparency into AI companies. There's very little oversight in terms of what they're doing. It used to be the case maybe five years ago that these companies would publish most of the research they did, so there was a shared understanding in the research community of how the most advanced systems work. That also helped audit the systems for safety more effectively. This has stopped being the case. Companies really don't release very much information at all about their systems, and there's no independent oversight that is mandated.

We need programs for independent experts to be able to look at the details of the AI systems. That doesn't just include evaluating or testing the model, but also includes having the necessary information about how the model was developed and what data was used, which is often copyrighted data. There have been a number of large-scale lawsuits about that. Also, what training methods were used? Was it trained in a way that is known to cause addiction, dependency and other psychological issues? We know this is something that has happened repeatedly in the tech industry with social media and with AI. Finally, how is the system being deployed and with what additional safeguards and guardrails? What is the company doing to monitor how it's being used? Companies have a strong incentive to understand how their products are being used in order to make more money from them.

That's something the government also needs to—

[*Translation*]

Linda Lapointe: Thank you, Mr. Krueger. I'm going to have to cut you off there. I also want to ask Mr. Aguirre a question, and I only have six minutes.

Mr. Aguirre, can we compare the risks associated with advanced artificial intelligence with nuclear weapons and climate risks? There has been some talk of that comparison. Is this a fundamentally different issue?

[*English*]

The Chair: Answer in 45 seconds, please.

Anthony Aguirre: With regard to the similarities and differences, I think nuclear weapons pose a particular risk, which is when they explode. The analog to that is if we build superintelligence and lose control of it.

AI is posing significant risks right now and is doing significant harm right now because it is so under-regulated and undergoes essentially no safety testing. As Max mentioned, there's strong evidence that there are large effects on suicidal ideation and media addiction in our young people. That is harm that is being done right now. We clearly see the beginnings of effects on labour with replacing humans with AI systems. That is the design; that is the goal to do at a large scale.

I think we are going to see that the risk of AI is it's replacing humans in roles that they should not be replaced in by a machine—as therapists, as companions, as romantic companions, as workers, etc. That scales all the way up to replacing humans as decision-makers and even replacing humanity altogether in the longer term.

I think the stakes are big, but it can be more diffuse.

• (1605)

The Chair: I'm sorry, Mr. Aguirre. We're over time. Thank you, sir.

[*Translation*]

I now give the floor to Mr. Thériault from the Bloc Québécois for six minutes.

Luc Thériault (Montcalm, BQ): Thank you, Mr. Chair.

Thank you very much, Mr. Aguirre, Mr. Kruger and Mr. Tegmark for your enlightening and sober presentations that provide a sense of meaning and purpose for the ethical dimension of this committee.

We're starting a fundamental reflection here. You have spoken about building scientific consensus. I think that consensus is becoming clearer with each committee sitting.

I'll start with Mr. Aguirre.

In your article, which calls for keeping the future human, you talk about how computing power can easily be quantified, accounted for and monitored with little ambiguity once good rules are in place.

Mr. Kruger, you have described advanced artificial intelligence as an immense project that is only made possible through deliberate effort.

I'd like to hear your two points of view on the technical feasibility of a verification scheme.

Mr. Tegmark, you can chime in afterwards.

Go ahead, Mr. Aguirre.

[*English*]

Anthony Aguirre: I'm happy to start.

Yes, I think it's absolutely feasible. As David suggested, AI is only made possible through huge amounts of computation done by very specialized chips. These chips are built essentially by one company, using machines built by one company and designs built by a handful of companies.

We've seen a lot of discussion of this compute capability in terms of export restrictions and controls, but these chips have hardware-level security. It isn't just about where the chips go but also about controls that can be on them. These chips have hardware-level security capabilities that enable verification of their level and type of use. Just as your phone can be remotely bricked if someone steals it, AI hardware can and should be configured so that it could be shut down at the hardware level. I think the more powerful the AI, the more it needs a reliable off-switch.

We can use the capabilities of the hardware, the base layer at which these AI systems are operating, both to add a layer of control and to add a layer of verification if we institute red lines that should not be crossed in their development and deployment.

David Krueger: I'll jump in. I'll agree with what Anthony said.

It's really important to emphasize just how much investment is going into this. In the past, people used to think there was no real way to regulate AI and make sure nobody was doing something dangerous with it because it was software and anybody could do it on their laptop in their garage. That's not at all the case right now.

In the case right now, these systems are taking hundreds of millions and billions of dollars. This isn't the sort of stuff that is publicly disclosed these days, but there are huge investments that continue to increase, and the hardware is extremely specialized, as Anthony mentioned. This is the main point for intervention for international regulation of AI, which, as I mentioned, is absolutely critical.

The only thing I would add is that it's very important to think about how to make such a scheme as robust as possible. Verification might look something like a white list of types of AI systems that are allowed to be run on the computer chips. It also might look like location tracking so that we know where the chips are in case we need to recall them.

In fact, we should stop developing more powerful AI systems immediately. The most robust way of doing that would be to actually stop building the chips, as opposed to trying to set up a more complicated and less robust system of technical verification. That's my personal view: To give us some breathing room, we should stop building the chips and stop building and maintaining the factories that produce them.

As I and the other experts mentioned, we have potentially a few years here. This is not a situation in which we have time to try to find the perfect solution. We need to immediately implement a solution that will slow or pause the incredible rate of progress towards superintelligence.

• (1610)

[*Translation*]

Luc Thériault: Do you agree with that, Mr. Tegmark?

[*English*]

Max Tegmark: We heard some detailed technical answers to this important question about the practical steps that can be taken. I just want to add that we're not, as was mentioned earlier, talking about a pause here on AI. I'm not talking about a pause on AI at all. I'm just talking about a pause on AI girlfriends for 12-year-olds, AI that can teach terrorists to make bioweapons and other products that are clearly more harmful than beneficial for Canadians.

This is no different from what the health products and food branch of Health Canada does all the time for medicines. We don't say that Canada has a pause on medicines just because Health Canada does not allow pharma products that haven't done the clinical trials to be released. We can simply do for AI exactly the same thing that we've done for medicines as a very first step in the right direction.

[*Translation*]

The Chair: You only have five seconds left, Mr. Thériault.

Luc Thériault: All the same, a distinction should be made between specialized artificial intelligence and artificial superintelligence. Some things, such as the parental control PIN, are easier to control than the relentless race to develop this superintelligence.

The Chair: Thank you.

Mr. Hardy from the Conservative Party has the floor for five minutes.

Gabriel Hardy (Montmorency—Charlevoix, CPC): Thank you, witnesses, for joining us.

I'll start with Mr. Tegmark, who has spoken only briefly so far.

Mr. Tegmark, you often speak about the potential for artificial intelligence to be transformative and goals that have potential benefits for humanity.

In your opinion, is the use of artificial intelligence in the medical field among the goals that we should focus on in the near future? To what extent can artificial intelligence change and improve the medical field?

I would even venture to ask you if governments should join this venture to help society find a cure for chronic and degenerative diseases.

I'd like you to speak to the medical field and artificial intelligence.

[*English*]

Max Tegmark: Thank you. This is something very close to my heart.

AI has enormous potential for improving medical treatments, curing cancer and so on. This is not in the future; it's in the past already. Even though all the AI companies talk a lot about curing cancer, there's actually one company only that has really made real progress, and it's Google DeepMind. It released AlphaFold, which is really helping drug discovery, and got the Nobel Prize for it.

Cancer has already gone from killing maybe 80% of the people for some types to 20%, so we're sort of 80% of the way towards curing cancer. The key risk I worry about is simply that we squander all these incredible benefits by letting AI-based pharma remain completely unregulated, which can cause a backlash. Many of you remember there was a product called thalidomide that was sold in Canada and America to pregnant women with morning nausea. Because pharma was completely unregulated back then, this caused over 100,000 babies in North America to be born without arms or legs, which in turn is why the Food and Drug Administration was created.

Yes, let companies innovate, amazingly, and cure diseases with AI, but let's treat them the same way we treat pharma companies and make sure they don't get their products released until they have been properly tested.

[*Translation*]

Gabriel Hardy: Basically, what you're saying is that artificial intelligence can actually contribute to global efforts to address many chronic and degenerative diseases, but the problem is not so much the speed of progress as letting strictly profit-driven companies commercialize products that are not yet fit for purpose.

However, I think artificial intelligence has potential to drive major breakthroughs in ultra-specialized treatments. In your research or across the overall artificial intelligence market, have you come across opportunities for more specialized treatments that are tailored to each individual rather than relying on more general approaches?

• (1615)

[*English*]

Max Tegmark: Absolutely. There's huge potential in making customized treatments that can sequence the patient's DNA, for example, for cancer, figuring out which particular mutations they have in their cancer cells and develop a custom treatment just for them. There are absolutely incredible opportunities there.

I'm a firm believer in innovation and in private sector innovation and the key to get this is to create the right incentives. In pharma, in aviation, and restaurants even, industry innovates to produce safe products where the harm outweighs the good, because those are the ones that they're allowed to sell. If we can quickly create the correct incentives for the AI industry, then these companies that are currently doing, in my opinion, very reckless things will quickly focus on innovating a race to the top with safe products. I don't blame the companies. I blame the lack of providing the right incentives to them.

[Translation]

Gabriel Hardy: Thank you very much.

Mr. Krueger, for some time now, we have heard that at some point, private businesses may consider removing humans from the equation and operating with fewer human employees, and that they will replace them with artificial intelligence. I think this is not the first time we're hearing this.

Is that happening already? Are companies conducting studies to determine performance? Generally, are you seeing big tech saying they did well to replace humans with artificial intelligence, or when they do their math, do they realize that overseeing, verifying and monitoring the much-touted emerging artificial intelligence robots is just as costly as having humans who are doing a good job?

[English]

The Chair: That's the end of the time, Monsieur Hardy.

[Translation]

I'm sorry, Mr. Hardy. We'll continue with Mrs. Church for five minutes because I suspect the answer to your question will be fairly lengthy.

[English]

Ms. Church, go ahead.

[Translation]

Leslie Church (Toronto—St. Paul's, Lib.): Thank you, Mr. Chair.

That's a great question, Mr. Hardy.

[English]

My question, I think, is probably for Mr. Tegmark.

You've spoken quite a bit about binding safety standards, and I appreciate the comparison to how we approach drug and pharmaceutical regulation.

As parliamentarians and lawmakers, where do you see us starting on this? It's one thing to look at some of the outcomes of the uses of chatbots and AI, particularly where they cross into child safety. I think those are certainly some very key and obvious areas where we need to be looking at how to ensure safety.

How else do we, in some ways, capture the breadth of how AI works across so many different fields and touches many industries and many potentially problematic areas? How do we capture that in a regulatory model that would be effective for us to address some of the harms you're raising?

Max Tegmark: That's a great question.

The simple way to view this is that all of the diverse applications of AI simply have this same approach that we have in all other powerful industries, that it's the company's job to innovate and demonstrate to independent, government-appointed experts that the harms are outweighed by benefits.

I would start rather politically with child safety, because that is so incredibly politically salient and winnable right now. In America, we have about 95% of Republicans and Democrats agreeing that this has to happen. I call it the Bernie to Bannon coalition, and I think we're likely to see some legislation this year here in the U.S.

Once this precedent is set that we're going to treat AI like any other industry, we can add to the list of safety standards not only that they must not greatly enhance suicide risk in kids but also national security things. For example, you can't sell things if they can teach terrorists to make bioweapons. You can't release things if they could overthrow the government, as we heard from Professor Aguirre and Professor Krueger. It flows naturally from this simple approach of just treating AI companies like other companies.

I want to add one more thing. If this business about loss of control sounds strange, it's a very obvious idea that goes back to Alan Turing in 1951, that, if you build a bunch of robots that are vastly smarter than all humans, then of course they can build robot factories and make new robots. This is very much what companies are trying to do now.

Also, because they can make more robots, they check off the definition of being a species. Go down to your nearby zoo and ask yourself who is in the cages right now. Which species is it? Is it the humans? No, it's not. Why not? It's because we are the smartest species on earth. What we're basically saying is, let's keep it that way. Let's not let companies sell something—

• (1620)

Leslie Church: Let me jump in here. I think you're probably hearing a lot of interest from us in terms of how we get our arms around this issue.

Let me turn to Mr. Aguirre for a moment, because both of you were involved in the the Future of Life Institute.

I'm very interested in the concept of tool AI. I hadn't heard that expression before. I think that's interesting in terms of thinking about how we bound some of these models into the specific areas they're working in and how we limit their breadth.

There's one thing I'd like to ask you in terms of your knowledge of other organizations or your own that are working in the space. Is anyone embarking on something like a model code, something that countries around the world could look at as we go down this path of trying to very quickly regulate or establish safety parameters in a very fast-moving sector? How are organizations like yours helping us parliamentarians and legislators around the globe to move in a direction that captures how we should be approaching this issue?

Anthony Aguirre: That's a great question. There's a sort of frustrating chicken-and-egg problem in that it's hard to build up the governance capacity in terms of the evaluations, the certifications and the whole infrastructure that is needed to evaluate and test these models when there's no requirement to do so. There's no customer without some sort of regulation that requires those things.

On the other hand, when you're thinking about regulations, it feels very daunting that there are all of these different use cases for these systems, and you have to think about how you are going to regulate all these things.

As Max has pointed out and you suggested, I think it's critical to identify some first steps to take. Maybe it's around child safety testing or just requirements that, when you produce an AI system along this sort of tool orientation, you say what it's for and then you can start to assess whether that AI system is fit for that purpose.

The Chair: Thank you, sir. We were over time on that one.

[Translation]

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

Luc Thériault: Thank you, Mr. Chair.

I'm going to quote you, Mr. Aguirre: "The leaders of Deepmind, OpenAI, and Anthropic...have all literally signed a statement that advanced AI poses an *extinction risk to humanity*."

You say that this is unprecedented, given that they are building these systems "under commercial incentives and near-zero government oversight".

What should we make of companies that issue warnings about their own products, but continue to develop them anyway?

I'd also like to hear from you, Mr. Krueger.

[English]

Anthony Aguirre: It's pretty astonishing. We've never seen an industry both developing something and publicly admitting how very dangerous that thing is. This is a product of how the industry has peculiarly developed and, in particular, the race condition that these companies find themselves in.

A couple of weeks ago in Davos, we heard from two of the heads of AI companies that they would like to slow down. They feel worried about what they're doing, but they feel they can't because they're in a race. If they hit the brakes, everyone else is going to keep their foot on the accelerator, and they'll lose out. All of these companies feel they have to build this thing because somebody is going to do it, and they feel that if somebody is going to do it, it might as well be them.

This is a crazy situation for us to be in, just like the classic arms race that ended up with 70,000 nuclear warheads that nobody felt like was such overkill. That's where we ended up because there was an arms race. We're in a similar situation here where it takes an outside actor—and it really has to be the government—to call a quit to the race. They're not going to be able to do it by themselves, even if they want to.

• (1625)

David Krueger: I agree with this. What's happening here is the idea of human extinction has been used to push this narrative that this is some sort of corporate PR stunt. This is demonstrably false. As somebody who has been in this field for much longer than these companies have even existed, in the case of Anthropic or OpenAI, these concerns go back decades.

It's commendable that the CEOs have acknowledged these risks at the same time. Maybe sometimes they exaggerate things in order to hype up their product or something, but I think that's basically what's going on. They are desperate because they see they are a few years away from building something they are scared of, and they want something to step in and defuse the race, if possible.

However, they don't believe that's possible, generally, and I think that's the mistake. We need to understand it is possible. That's why I mentioned the computer chips as a key point of intervention. If none of these companies and nobody globally can get access to these giant piles of chips and the energy to build these data centres, then we won't see this race continuing at anything like the current pace.

I will also add that I think the reason they are doing this is there's this element of "If we don't do it, somebody else will." There's the desire to make tons of money. For some people, they also want to usher in this new species Max was talking about. They want to see humanity replaced by AI, which they view as the natural next step in evolution. There are many public comments to this effect from various people within the industry, and this is an incredibly antisocial attitude.

[Translation]

Luc Thériault: I'd like to wrap up this discussion.

Mr. Aguirre, you have called for an international agreement between the U.S., China and other countries that are capable of having a solid verification mechanism to ensure parties and rivals don't defect.

Mr. Krueger, you have said that ending the race to build superintelligence is reasonable and possible and that this is a moral imperative. I would agree with that. What can this committee do to begin negotiations or to reach such an agreement?

This is an issue that continues to come up. You're not the only ones who have said that. What is being done?

My questions are for Mr. Aguirre and Mr. Krueger.

[English]

The Chair: Make it as quick as 10 seconds, please.

Anthony Aguirre: Canada can certainly stake out a position in its own self-protection that we should not be building superintelligence. I think it will be critical that an end to this race will actually require both the U.S. and China to realize that it's against their own self-interest to build superintelligent AI. As long as they believe that it will grant them power, they will want to pursue it, but this is not the case. AI, superintelligent, will absorb rather than grant power. If they realize this, then it is in their interest as well as everybody else's not to have not to have it developed, and that's the foundation.

The Chair: Thank you, Mr. Aguirre.

Mr. Krueger, I'm going to give you 10 seconds to respond, please.

David Krueger: Thank you.

We need negotiations for an international treaty to begin immediately. I want everyone here to talk to everyone they know who has any ability to make something like that happen and tell them exactly that: Tell them what you've heard here from all of us and the previous experts.

The Chair: Thank you, sir.

[Translation]

Mr. Hardy, you have the floor for two and a half minutes.

Gabriel Hardy: Thank you very much.

Once again, I'll address my question to Mr. Krueger, because the question deserves analysis.

We're seeing many companies investing in artificial intelligence in a bid to replace their employees and to make more profits. I raised this question in committee last week, and it prompted some valuable answers. People have questions.

When big tech companies invest in artificial intelligence, how do they measure their return on investment? Do they actually have good returns or ultimately, is it more expensive for them to manage artificial intelligence and ensure the work is done properly than to have a well-trained employee to do the same job?

I'd like to hear your thoughts on that.

• (1630)

[English]

David Krueger: There are going to be cases where it's more expensive or less expensive at present. One important thing to recognize is that AI doesn't have to do the job better if it can do it much cheaper. We might see a replacement of competent humans with less competent AI at scale because it's just cheaper, which I think would be a bad outcome.

On the other hand, I think we have to think about where this is all headed because it's going there very fast in a few years. I think

within a few years, we will see AI that is an extremely competitive replacement for most human labour. That is the premise on which these investments are being made. The massive investments to build AI are justified by the belief that this, in fact, will or at least might lead to the creation of something like superintelligence like we've been describing here.

[Translation]

Gabriel Hardy: Businesses don't invest without looking at key performance indicators, or KPIs and rates of return. We always hear about the future, but now, are they measuring performance? Are they seeing any returns, or would you say that for now, they don't have any measurements when it comes to their investments in this new technology?

[English]

The Chair: Answer in 35 seconds or less, please.

David Krueger: I'm sure they're measuring some things. Silicon Valley companies, historically, care more about growth and dominating a market and addicting customers before they even try to make a profit. Amazon famously didn't make any profit for, like, 10 years or something. I don't know what they're looking at right now, but I don't think that this is what is driving the investments. Yes, I think if you take seriously the possibility of AGI and superintelligence in a few years, which the investors and especially the people building it do, then the investment is certainly justified, except that this is also incredibly dangerous and shouldn't be happening. If it kills everybody, it will kill the investors, kill the people who own these companies, kill everybody in this room. It won't matter if we've created a bunch of good businesses, as Sam Altman says. It won't matter if we've cured cancer, etc.

The Chair: Thank you, Mr. Krueger. I appreciate that.

[Translation]

Mr. Sari, you have the floor for two and a half minutes.

Abdelhaq Sari (Bourassa, Lib.): Thank you very much, Mr. Chair.

I'd like to thank the witnesses for their very insightful remarks.

I only have two and a half minutes to ask questions on a very complex issue, which I feel very strongly about.

We all agree about the risk you have outlined today. Now, the question is how to intervene. To do so, first, it's important to specify the field or type of artificial intelligence in question. Here, we're not talking about generative artificial intelligence, and we are not necessarily talking about superintelligence or agentic artificial intelligence. One thing that deeply concerns me is the concentration of cognitive capabilities in artificial intelligence systems because these cognitive capabilities direct learning in general and universal "cognitive capacity".

I'd really like one of you to answer the following question: How can we talk about actual human oversight or government oversight when artificial intelligence systems learn, evolve and make decisions at a pace that is faster than our collective ability to understand and challenge these decisions?

[*English*]

The Chair: Who wants to take that question in just over a minute?

Mr. Tegmark, can I start with you?

Max Tegmark: Yes.

What you're so eloquently describing is the digital gain-of-function research, also known as recursive self-improvement, where AI makes better AI which makes better AI.

Again, it's easy to deal with. We've already dealt with it in biology here in America. We've banned gain-of-function research, and there's very strong opposition to it now after the possibility that this might have caused the COVID pandemic. We should similarly ban AI digital gain-of-function research. It's a no-brainer, yet right now a number of companies in America are explicitly doubling down on this kind of digital gain-of-function research because they're unregulated.

• (1635)

The Chair: Thank you, Mr. Tegmark.

Mr. Krueger or Mr. Aguirre, do you have anything to add in 15 or 20 seconds or less on that question?

David Krueger: Yes.

I think it's important to emphasize that this issue does need to be tackled internationally. It's also something that Anthony and Max, in talking about tool AI...I think it's true that it's a great place to aim for, but I do think we may need to do something pretty drastic in the immediate future to be able to monitor and enforce an international agreement to stop this race. Then, once we've sort of gotten control of the situation, we can think about how we want to proceed to develop beneficial tool AI—

The Chair: Thank you, Mr. Krueger. I'm going to have to cut it off there. We're at the end of the hour.

On behalf of the committee, I want to thank all three of you for participating in this discussion. Thank you.

We are going to suspend for a couple of minutes while we change over to our second-hour panel with the Privacy Commissioner.

• (1635)

(Pause)

• (1640)

The Chair: I'm going to call the meeting back to order for our second hour as we return to studying the challenges posed by artificial intelligence and its regulation.

I want to welcome for the second hour today, from the Offices of the Information and Privacy Commissioners of Canada, Mr. Philip Dufresne, who is the Privacy Commissioner of Canada—it's always good to have you back with us, sir—and Marc Chénier, who is the deputy commissioner and senior general counsel.

Mr. Dufresne, you have up to five minutes to address the committee. Go ahead, please.

[*Translation*]

Philippe Dufresne (Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada): Thank you very much, Mr. Chair.

Members of the committee, thank you for the invitation to appear as part of your study on the challenges posed by artificial intelligence and its regulation.

Addressing the privacy impacts of the fast-moving pace of technological advancements is one of my strategic priorities. This has also been a significant focus of my domestic, international and cross-regulatory work over the last few years given its rapid and broad adoption by individuals and organizations in Canada and globally.

[*English*]

Privacy is an important and timely issue for Canada. As more and more personal data is being collected, used and shared, data protection becomes increasingly significant for Canadians and Canadian organizations.

The protection of personal information is particularly important in the context of AI, as personal information can be used to train and operate those systems. Recently, I announced an expanded investigation into the social media platform X and its Grok chatbot. The investigation will examine the emerging phenomenon of AI being used to create deepfakes, which can present significant risks to Canadians, including children.

[*Translation*]

I expect that the results of this investigation, as well as my ongoing investigation into OpenAI, will help to inform privacy and policy direction with respect to AI, and help individuals and organizations to use and deploy these technologies safely and responsibly, and with appropriate protections for personal data.

Investigations by the Office of the Privacy Commissioner in the past two years have demonstrated how Canadian law is able to address major privacy issues that can have serious impacts on individuals.

[English]

For example, my investigation into Aylo, which operates Pornhub and other pornographic websites, addressed non-consensual sharing of intimate images. My joint investigation with my U.K. counterpart into the 23andMe breach examined an incident that impacted the highly sensitive personal information of seven million customers, including more than 300,000 Canadians.

Last fall, I announced the result of my investigation with my provincial counterparts into TikTok, which highlighted the importance of protecting children's privacy online. Because of our investigation, the company has implemented, and continues to implement, improvements to its privacy practices in the best interest of its users, especially children.

Technologies such as AI can bring economic, social and public interest benefits. The value of this innovation will be maximized when it is accompanied by trust.

[Translation]

A survey conducted by the Office of the Privacy Commissioner last year found that a significant majority of Canadians are concerned about how their personal information is collected and used—including 83% indicating concern about their privacy when using artificial intelligence tools. Many have taken actions to protect themselves and most indicated that they are less willing to share their personal information with organizations compared to five years ago.

[English]

This further underscores the strategic advantage for organizations to develop and deploy AI and other technologies in a responsible, privacy-preserving manner. It is key for developers and providers of AI to embed privacy in the design, conception, operation and management of their products and services and to consider the unique impact that these tools have on children, as well as on groups that have historically experienced discrimination or bias.

Organizations that use AI should be transparent about this use and accountable for any AI generated decisions about an individual, such as whether to grant someone a loan or a job.

• (1645)

[Translation]

As technologies continue to evolve rapidly, and become increasingly integrated into personal and professional lives, it is our collective role as regulators and policy-makers to ensure that privacy is protected for current and future generations. Canada's privacy laws must be able to meet this challenge, and to do so will require modernization.

[English]

With respect to AI, my recommended amendments to Canada's federal privacy laws include recognizing privacy as a fundamental right, as well as establishing requirements to implement privacy by

design and to conduct privacy impact assessments for high-impact data processing.

Personal information is at the heart of artificial intelligence, and therefore, privacy legislation should, in my view, be at the heart of AI regulation.

Thank you. I look forward to your questions.

The Chair: Thank you, Mr. Dufresne.

We're going to start with Mr. Barrett for six minutes. I'm going to keep it tight on time.

Mr. Barrett, go ahead.

Michael Barrett: Tell me about what have been called Chinese spy cars. The Premier of Ontario, Mr. Ford, has expressed serious concerns about the plans for the Canadian market to accept nearly 50,000 vehicles manufactured by companies like BYD. What has your office taken a look at so far with respect to those vehicles and that claim, perhaps informed or otherwise, by Mr. Ford?

Philippe Dufresne: I have heard those statements, and we are monitoring the situation generally with respect to connected vehicles. In fact, this year we launched our contribution program on the theme of connected devices, and we're looking forward to finding out more about the types of connection, the types of data information that is collected by cars and other types of devices.

In terms of the Chinese angle, we are not looking at this specifically. However, in the context of our TikTok investigation, one of the elements we highlighted in our conclusion was when data will leave Canadian jurisdiction and there is a risk that other governments can have access to this information, this is something that Canadians should know about. This should be transparent. In our TikTok report findings, we requested, and the organization agreed, to make this explicit.

Michael Barrett: On TikTok, do you have a recommendation for Canadians on whether or not they should use the app?

Philippe Dufresne: Our recommendation to Canadians is that they should ask questions about this or any app. Frankly, in any situation where their personal information is being sought, they should be asking, "Why do you need it? What will you do with it? Who will you share it with?" In the TikTok investigation, we address these head-on, looking at what the organization is telling Canadians.

It's one thing for citizens to ask questions. Organizations have a big responsibility to be proactive in this transparency. In the TikTok case, we found that the information wasn't clear enough for adults, and it was certainly not clear enough for children, who are a huge part of that market.

The questions should be about the use, the sharing, the purposes, where it's going and who can have access to it. Canadians should ask more of these questions, but organizations should proactively take responsibility for making that information easy to find.

Michael Barrett: Have you seen a change in the proactive information offered by TikTok to Canadians since you made those recommendations?

Philippe Dufresne: I would say yes, because we are working with them in monitoring the implementation of our recommendations. Our recommendations had a six-month period to put them in place. A big one was better tools to keep underage children off the platform altogether. Others had to do with the transparency, the consent and the information.

They've implemented a number of those, and they have until March to complete the rest. We're going to be monitoring that to make sure that happens.

Michael Barrett: First of all, based on their co-operation to this point, is it your expectation they'll meet the deadline? Should they not, what would be the outcome?

• (1650)

Philippe Dufresne: Should they not, one of the gaps in privacy legislation is that I don't have order-making powers. We have to count on their collaboration and we have to work with them. So far, it is working and I'm cautiously optimistic that it's going to continue to work, but that is why a key element of law reform has to be order-making powers for the Privacy Commissioner.

Michael Barrett: I'm pressed for time, so I'm going to move on.

I want to ask about your investigation of X Corp. This is incredibly important, obviously, the harms being done in real time, not only to children but especially to children, with the non-consensual images that are being propagated and created are alarming.

What kind of a position are you in, in your role as a Canadian commissioner, with the lack of order-making power? Do you lack the enforcement tools necessary to be able to effectively execute your role in a way that would protect Canadians, especially children, in a situation where the gravity of it can be lost on no one?

Philippe Dufresne: I'll say two things.

One is that I need to have order-making powers. That should be a top priority for Parliament. I'm encouraged by statements from the Minister of AI that modernization is something that's being contemplated.

That being said, I am using and will continue to use the existing tools that I currently have to protect Canadians' privacy with investigations and recommendations and by working with partners in Canada and internationally.

In the context of deepfakes, we issued statements calling them out as early as December 2023. We're working with international

partners to bring the international community together in taking steps.

That's one thing that I've done, for instance, in the 23andMe case with the breach of Canadians' information. I don't have order-making powers but my U.K. counterpart does, and together, we did that for Canadians.

The Chair: Thank you, Mr. Dufresne and Mr. Barrett.

[*Translation*]

Mr. Sari, you have the floor for six minutes.

Abdelhaq Sari: Thank you, Mr. Chair.

Thank you very much for your testimony, Mr. Dufresne.

First, before I ask my question, I'd like us to talk about your mandate regarding privacy in general. The mandate is based on fundamental principles, including the issue of transparency, general accountability and the ability for Canadians to understand and even challenge the decisions made by any means, whether powered by artificial intelligence or any other solution.

However, as you well know, artificial intelligence has somewhat changed how decisions are made. For example, all artificial intelligence, whether generative, cognitive or agentic, ultimately relies on neural networks, which don't provide a decision process. This is what is called the black box. There is no model on the decision-making process.

My first question is as follows:

In this kind of scenario, where technologies are evolving at a very fast pace, how is the Office of the Privacy Commissioner evolving? How does it assess the existence of actual human oversight? Can we talk about a certain degree of human control?

Philippe Dufresne: Thank you for your question.

You're quite right. Privacy principles can evolve over time because these are fundamental principles that affect human dignity, freedom, the ability to make decisions, the ability to choose what we share and with whom. Right now, we're facing serious challenges with technology, because technology is evolving very quickly. Organizations like mine generally need to catch up. They need to learn about these tools and to develop technological capabilities. My office has developed capabilities to understand the technology and to act accordingly.

On the issue of human decisions that you alluded to, we also need to raise these issues in the course of legislative reforms. For instance, I made a recommendation calling for more transparency with artificial intelligence to understand the decisions that are made and to make sure humans are in the process. Recently, I was in Seoul for the global privacy assembly, and my office sponsored a resolution, which was adopted by the international community, that focused on the human role in the artificial intelligence process, its significance and what it must embody. This issue is therefore timely, and it's somewhat of a response to the black box effect you mentioned.

• (1655)

Abdelhaq Sari: The black box is more technological. It's the way neural networks generally operate, and there is no way to walk that back and change it. It started in the 1980s and it will continue to work that way.

You talked about understanding technology. Do you think the right to privacy is still being fully respected?

Philippe Dufresne: I think there are definitely cases where it's not respected. We talked about the TikTok decision, where there were shortcomings. There is also the recent decision concerning Staples. There are many cases where there have been shortcomings, but the key thing is to have the tools to address these shortcomings. Ideally, we take preventive measures, but if not, we take action after the fact.

I believe these principles are technologically neutral and they can evolve with technology. However, the law needs to be modernized to make this easier. Concepts like de-identification, transparency and how to process transparency when organizations themselves say they don't know how they made such decisions. The chair of Google said that recently. The law must therefore change. We can have more proactive obligations, but we already have a very good framework on this issue with the Privacy Act.

Abdelhaq Sari: It makes me feel better to hear you talk about the framework because all the scientific publications that I have read, and the people who have appeared before this committee, put more emphasis on the lack of transparency with artificial intelligence technologies. I understand and have a lot of respect for your role, which I think is very important. You have reassured me a lot today because of the progress you have made in your work.

On our part, as a House of Commons committee, what would you recommend that we do with respect to oversight? What steps must we take to manage this transparency gap in oversight, recognizing that some lack of transparency is inevitable, whether we like it or not?

Philippe Dufresne: In my opinion, the most important thing you can do as parliamentarians is to amend the law. It's an essential tool. I made seven priority recommendations to the government, which I shared with the committee. They include such items as expanded enforcement-making powers, order-making powers and the power to impose fines in certain cases. Recognizing privacy as a fundamental right is important. This is more important than ever with the advent of artificial intelligence. The recommendations include items such as privacy by design. Organizations that create tools that have significant impacts must be asked to conduct priva-

cy impact assessments right from the beginning, and not at the end. This would be positive across the board. This issue must also be addressed globally. We need a framework to govern data that leaves Canadian jurisdiction.

Abdelhaq Sari: In terms of information, I always say there's a need to collect, process, store, secure and share information globally using other factors. Your role is particularly meaningful when it comes to security and protection.

Let us turn to Canadians listening to us today. Is there one group that tends to be more vulnerable than others? Who is the most vulnerable? We have talked a lot about young people and women today. Are certain groups of people more vulnerable than others?

The Chair: Please give a very brief answer, Mr. Dufresne.

Philippe Dufresne: Young people are very vulnerable because they are immersed in it, they experience it from every angle. You're right to allude to women and seniors. I believe many groups need to be protected.

The Chair: Thank you, Mr. Sari.

Mr. Thériault, you have the floor for six minutes.

Luc Thériault: Thank you, Mr. Chair.

Commissioner, welcome.

You talked about the international aspect earlier. I wanted to bring you back to—

Abdelhaq Sari: Mr. Chair, I'm having trouble hearing Mr. Thériault.

The Chair: Just a moment.

Please lower your mike, Mr. Thériault. That's better. Thank you.

I will restart the clock.

Luc Thériault: Okay, thank you.

I wanted to take you to the G7 leaders' statement, which reads as follows:

Work together to accelerate adoption of AI in the public sector to enhance the quality of public services for both citizens and businesses and increase government efficiency while respecting human rights and privacy, as well as promoting transparency, fairness, and accountability.

Further down, it states:

Promote economic prosperity by supporting SMEs to adopt and develop AI that respects personal data and intellectual property rights, and strengthen their readiness, efficiency, productivity and competitiveness.

In your opinion, for G7 leaders, what should be the key elements of a human-focused approach to artificial intelligence?

• (1700)

Philippe Dufresne: Thank you for your question.

You've alluded to the G7 leaders' statement. The G7 privacy commissioners, including me, had our own meeting here, at Meech Lake. In June, we issued a unanimous statement on the importance of prioritizing privacy for two reasons: to promote innovation and the economy and to protect children and young people.

We alluded to the leaders' statements on these items, and provided concrete examples including considering the best interests of children and young people when technologies are designed, developed and brought to market; underscoring the importance of privacy at the beginning, and not at the end; and underscoring the importance of transparency and communication with Canadians to create trust.

That is why some people tend to say that a strong privacy regime can stifle innovation. I challenge that, and our G7 statement also challenged that. The statement clearly says that it will promote innovation and support economic development because it will build public and consumer trust in this new technology. This can be seen in the surveys I alluded to earlier. There are concerns on this issue. It's therefore essential from a fundamental rights standpoint if we want to protect children, women, seniors and the rest of us when it comes to our freedom and our dignity. Furthermore, pragmatically, it will support the global economy and Canada's economy in particular. We sent a strong message here in Ottawa. I was very proud of that statement, and we are still promoting it here and beyond.

Luc Thériault: When it comes to enhancing the quality of public services and increasing government efficiency, what is the best way to balance the speedy adoption of artificial intelligence with respect for human rights and privacy, and advancing transparency, fairness and accountability?

Philippe Dufresne: That's the point. It's important to strike that balance. Tools will increase productivity. They can support all sorts of economic development. They can support developments in health care. They can improve services for citizens. That's very positive. However, this must be done in a transparent and humane manner. The concept must be human-centred. It must be done in a manner that respects the fundamental principles of privacy, such as informed consent, in certain cases, or appropriate goals.

In September 2025, the office of the Privacy Commissioner of Canada, together with counterparts from the Competition Bureau, the Canadian Radio-television and Telecommunications Commission or CRTC, and the Copyright Board issued an analysis on synthetic media, commonly known as deepfakes, which addressed these issues. In some cases, technology can help to create images. However, if it's used to manipulate people or if it's used to create non-consensual sexual images, then, of course, that infringes upon rights that must be respected. We cannot place innovation on one side and privacy on the other. Canadians must have both.

Luc Thériault: Take work, for example. It's a fundamental right. We can say it's part of human rights. People have come to us and said that states will want to replace white-collar workers with artificial intelligence soon. When a critical mass of people lose their jobs, how can this be reconciled with advances in artificial intelligence? We have talked about the G7 here, and its members have ordered governments to be productive and efficient.

Philippe Dufresne: I think the issue of job protection is slightly outside the scope of my privacy mandate. However, I can tell you

that when you protect privacy, you protect individuals. You make things more transparent, and you provide a better understanding of events. You also help people to distinguish between what is human and what is not. I believe that can be part of both the goals and the solutions. When it comes to jobs, we can say that we don't want to compete with artificial intelligence where it's a pure case of statistical probability, but the human advantage needs to be retained. In my opinion, that will always be an asset.

● (1705)

The Chair: Thank you, Mr. Dufresne and Mr. Thériault.

We will now begin the second round of questions. Mr. Cooper, you have five minutes.

[*English*]

Please go ahead, Mr. Cooper.

Michael Cooper (St. Albert—Sturgeon River, CPC): Thank you, Mr. Chair.

Commissioner Dufresne, the Prime Minister recently struck a deal with Xi Jinping to allow for the import of 50,000 Chinese EVs annually. He did so notwithstanding serious concerns regarding national security and privacy concerns, including audio and video surveillance as well as tracking people's movements. Premier Ford has characterized these EVs as spy vehicles. Others have characterized them in the same way. The U.S. has a functional ban on vehicles that contain Chinese software.

In the face of these very serious concerns that go directly to the privacy of Canadians, did the Prime Minister's Office, the Minister of International Trade or anyone in the government consult with your office about these concerns before striking a deal with Xi Jinping?

Philippe Dufresne: We were not consulted about this trade effort with China.

Michael Cooper: Thank you.

About an hour ago in the House, the minister responsible for AI indicated that the government would be tabling updated PIPEDA legislation in the near future.

Have you been consulted about that updated legislation?

Philippe Dufresne: Yes, I have. I and my team have been in communications with the department. I am pleased with how those exchanges have gone.

Michael Cooper: Do you expect that PIPEDA, the updated legislation, will give you the order-making power that you said moments ago you need and which you do not have?

Philippe Dufresne: That's going to be up to the government tabling the legislation. My expectation and hope is that I've made it very clear to the government that this is one of my top priority recommendations. I need stronger enforcement power. I am optimistic.

Michael Cooper: Okay.

Changing gears a little bit, the Supreme Court, in its jurisprudence in the Spencer decision and the Bykovets decision has been clear that access to personal information or personal data requires prior judicial authorization. Is that correct?

Philippe Dufresne: In criminal cases.... In administrative law cases, it wouldn't necessarily be the same.

Michael Cooper: Under the Liberal government's so-called cybersecurity bill, the Minister of Industry has the power to order a telecommunications service provider to collect, retain and share with the minister things such as metadata, subscriber account information, website visits, the location of financial data, among other personal information. Is that correct?

Philippe Dufresne: Yes.

Michael Cooper: Constitutional jurisprudence has recognized that metadata such as Internet browsing activity is highly sensitive personal information that is protected by section 8 of the charter, which says, "Everyone has the right to be secure against unreasonable search and seizure." Is that correct?

Philippe Dufresne: That's my general understanding of that jurisprudence. Under my legislation, sensitive information is entitled to higher levels of protection.

Michael Cooper: That's because metadata can reveal a lot about someone's online activities and their personal life, among other privacy issues. Is that correct?

Philippe Dufresne: Yes. The Supreme Court, in Bykovets, talked about how much you can glean from this type of information.

Michael Cooper: Bill C-8 does not require the Minister of Industry to obtain prior judicial authorization as a precondition to ordering the collection, retention and sharing of highly sensitive personal information such as metadata, does it?

Philippe Dufresne: No, it does not. Again, this is not in a criminal context.

I should say that I appeared before the SECU committee on Bill C-8 and shared my recommended amendments to the bill, which include necessity and proportionality framing for the exercise of those powers.

• (1710)

Michael Cooper: Do you believe there should be a requirement for the minister to obtain judicial authorization? Should it be narrowed, as opposed to as it is currently written, where the minister would have really broad powers to order the collection, retention and transfer of privacy information, which the Supreme Court has been very clear requires judicial authorization?

Philippe Dufresne: In my testimony, I highlighted that there is a balancing between the national security objectives. This is where necessity and proportionality become important. In some parts of the bill, I highlighted that you only had necessity or—

Michael Cooper: It would be fair to say that at present it's not fully adequate from the standpoint of protecting Canadians' privacy in this. There's room for improvement.

Philippe Dufresne: I've made recommendations on the standard, on information-sharing agreements and also on notification to my office in cases of breaches.

The Chair: That you, Mr. Cooper.

Ms. Church, go ahead for five minutes.

Leslie Church: Welcome, Mr. Dufresne. Thank you for once again being at the committee and for all the work that your office is doing to shed light on some of these emerging and concerning privacy issues that we're seeing, particularly with AI and digital tools.

I want to take you in a different and more positive direction. In a lot of the work that I do with seniors, persons with disabilities, families and caregivers, I hear a lot about the challenges of navigating through government systems, between provincial and federal systems, and application processes. One of the things I'm interested in with a modernization effort is how we can better use data to support modern service models, proactive benefit eligibility and simplification of access to services.

Is there anything that you're proposing in this modernization that would help us deliver services better as a government?

Philippe Dufresne: I think this is a very important point in the sense that privacy does not and should not stand in the way of the public interest. Data can help with good government service delivery. Data can help even with protecting privacy itself in terms of privacy-enhancing technology.

In part of my recommendations, I'm talking about privacy by design with privacy impact assessment, for example. This is a great tool where, if you have a process where you're going to be sharing information because you need to share it or you're going to use it to make better decisions for Canadians, transparency is important. That assessment is important.

In many cases when I'm asked for my views, I'm not going to say don't do it or don't give the police a tool if it's warranted and if there's a need for it, but I'll ask if it is necessary and proportional. Is it transparent? Have you assessed it?

My recommendations for amendments to both private sector privacy law and public sector privacy law go in that direction. For instance, right now, privacy law for the public sector does not require necessity and proportionality as an assessment. I think it should. I think this would allow for more sharing and use of information, but in a way that keeps Canadians' trust.

Leslie Church: It safeguards that data and privacy. I would agree with that.

Can I ask you about the work your office has undertaken around a children's privacy code? Can you give an update to the committee as to where that's at and what the next steps are?

Philippe Dufresne: Absolutely.

This is another area where law reform would be beneficial because in the previous bill, Bill C-27, which was before the last Parliament, there was an element in there that would create the ability to have codes of practice that I would approve and that would give some protections to organizations, and also some obligations and some predictability.

A children's code would fit very well in that regime. Right now, we don't have that, so the children's code I am working on putting in place is going to be setting out my expectations and my office's expectations to organizations on things like the best interests of the child, making sure that you have privacy protections by default if you're geared to children and making sure that the consent and the information is shared in a child appropriate way.

All of that is under way with consultation with stakeholders in Canada and around the world. A part of that also is the notion of age estimation, age assurance and making sure that you're keeping kids off certain websites like TikTok if they're underage. How do you do that without going too far and taking too much personal information? It's that balance that we want to help reach.

• (1715)

Leslie Church: These are early days, but are you looking to any of the experiences or lessons learned from the early implementation of age verification in Australia?

Philippe Dufresne: We are, and we're working very collaboratively with colleagues from Australia, the U.K. and around the world. We've issued some international statements about what we want to see. We want to see something that has data minimization. We want to see something that is transparent that isn't used for more things than it should be and something that is secure against privacy breaches, all of these. It's really an area where the international community is looking and is working. Australia, quite rightly because of their approach to social media, has had to really accelerate that.

Leslie Church: You've mentioned order-making powers as one of the tools you're looking for. Can you enlighten us with the other tools or capabilities that would be useful for your office to take something like a code and make sure that it's enforceable?

Philippe Dufresne: We're looking at enforcement-making powers and fine-making powers and also to have monetary consequences in appropriate cases. Again, this is something I don't want to have to use. I want the possibility of this to encourage organizations to invest in privacy.

The other thing is the issue of codes and, if an organization is going to spend money to develop a code and to put in place a program, that costs them money. If you're an SME, even if you're a bigger organization, that's an investment. One of the things we've heard from industry and lawyers is that sometimes they have a hard time selling this to management, because what are they getting

from that investment? If they're not getting any kind of regulatory protection, it's a harder sell.

Then what was in Bill C-27 would say, "You develop this code. If it's approved by the Privacy Commissioner, then, when you have a complaint against you, you can point to that code as showing that you were in good faith here."

It would make it much less likely that you would have a fine or that you even have investigations. To me, that puts the incentive in the right direction. It makes it easier for SMEs and other companies.

Leslie Church: Thank you.

The Chair: Thank you.

We're way over time, but I did want to give you a chance to respond because it was an important question.

[Translation]

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

Luc Thériault: Thank you, Mr. Chair.

Commissioner Dufresne, in your opening remarks, you mentioned the expanded investigation into the social media platform X and its chatbot. How is the investigation going? Do you have all the tools needed to move it forward quickly?

Based on your discussion with the minister and future legislative intentions, are you going to have more resources to achieve results more quickly?

Philippe Dufresne: I'll start with the last part of your question. What I can tell you is that in my public and private discussions, I've made it clear that it's important to have more powers.

This came out very clearly in my investigation into 23andMe, the genetic data company. My U.K. counterpart and I carried out a joint investigation and we arrived at the same findings. Ultimately, a fine was levied in the U.K., but in Canada, there was only a recommendation.

It's quite clear from this juxtaposition that it's important for me to have these powers, given that it's a matter of fundamental rights. I'm optimistic and I believe this will come to pass but I'm waiting to see what happens.

As far as our investigation is concerned, we will certainly make it a priority. I can't share more insights on the ongoing investigation, but I can say that when we launched the investigation, I expressed concern about this phenomenon and the significant risks it poses to the fundamental right to people's privacy and the rights of young people in particular.

We have the necessary resources, and we will use them to prioritize this investigation.

Luc Thériault: In this process, right now, do you think you have enough resources to take this investigation to fruition?

I'm talking about concluding the investigation, as well as the ability to tackle this phenomenon, which is not limited to social media.

• (1720)

Philippe Dufresne: Yes, we have our internal resources.

Of course, we can do with more resources, but we're mindful of limitations in the current context. We are working closely with our international colleagues, and we share expertise and knowledge which we are going to put forward. We use the tools available to us based on the organizations we are investigating.

We do, however, have a problem, as I said, which arises when we complete our investigation, determine there is a violation, and the organization refuses to implement our recommendations. That was the case with our investigation into Pornhub, or Aylo, for example. We asked them to stop publishing pornographic videos without the consent of everyone in those videos. The organization did not agree with our recommendations. I therefore have to take them to court, and that takes time and a lot of resources. That's my concern because, in the meantime, our recommendation has not been implemented, and Canadians are not protected from this type of practice.

Luc Thériault: On the distribution of deepfakes, do you have any recommendations now to better regulate this issue?

Philippe Dufresne: In December 2023, my provincial and territorial counterparts and I made recommendations on artificial intelligence in general. However, on deepfakes in particular, we said it was wrong to use deepfakes to manipulate people, for example, to make defamatory statements or to disseminate non-consensual sexual content. There are guardrails on that already.

More recently, my office and the Canadian Radio-television and Telecommunications Commission, or CRTC, the Competition Bureau and the Copyright Board published an analysis on deepfakes from a privacy, competition law, broadcasting law, and copyright perspective. In my world, namely privacy, concerns are related to the use of this technology to manipulate people or to disseminate sexual content without consent, among others. We are also looking into the use of personal data and transparency.

We published that analysis in September and it's a good summary. It also shows that we are collaborating not only with other privacy commissioners in Canada and around the world, but also with other digital content regulators, such as the Competition Bureau and the CRTC.

The Chair: Thank you, Mr. Dufresne and Mr. Thériault.

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

Gabriel Hardy: Thank you for joining us again.

Earlier, when you answered a question from Mr. Barrett, you said we don't have the power to force companies like X to provide information on their operating structure or to force them to operate in a certain manner.

What recommendations would you give the government so we can act more quickly to protect the general public?

Philippe Dufresne: Thank you for your question.

Indeed, I have the power to ask for information in the course of an investigation, so when it comes to investigation, there is no problem with the law.

However, at the end of the investigation I do not have any powers. I can make a determination that the law has been broken, but I can't order an organization to put an end to an illegal practice, for example.

Gabriel Hardy: Yes, you seemed to imply that in Pornhub's case, for instance. You told Pornhub what it needed to do, but that was a recommendation, and it was therefore not really binding. Ultimately, you use a lot of resources and you conduct research, but in the end, companies do whatever they want.

Philippe Dufresne: That is what happened in this specific case.

Fortunately, many of the Canadian companies that we are dealing with agree with our recommendations. We have a talk and then they move forward. However, problems arise when companies disagree. In Pornhub's case, the company refused to implement two recommendations that I believe were essential.

First, we asked the company to make sure they obtain clear and direct consent from all individuals. Indirect consent can lead to non-consensual distribution or revenge porn, for instance, which was the focus of our investigation. Second, we wanted content shared on the company's website inappropriately to be removed quickly and to make it easy for victims to ask for content to be taken down.

The organization has consistently refused to implement either recommendation, and that's why the amendment I requested seeks to ensure I can issue orders that can be enforced right away. People can challenge my decision in court and that's normal and it's part of the rule of law, but there ought to be immediate protection for Canadians.

• (1725)

Gabriel Hardy: These recommendations were shared with the Canadian government, and you are still waiting for them to be implemented.

Have you made other recommendations that are yet to be implemented? The last time you appeared before this committee, you seemed to suggest your office was somewhat underfunded and understaffed.

Do you feel the support and resources you receive align with your goals? In my opinion, your goal is to protect people, and that is not a trivial goal.

Philippe Dufresne: We have made a number of substantial recommendations, which require a new bill. The first recommendation pertains to powers, followed by recognizing privacy as a fundamental right, protecting young people and giving people the right to take down certain information that has been made public. There is also the concept of preliminary assessments as well as the international factor. We need a stricter regime regarding data that leaves Canadian jurisdiction—

Gabriel Hardy: That's the main issue. You raised it earlier, and here it comes again. How many recommendations have been taken into consideration and how many are moving forward? The Carney government took office a year ago. How many of your recommendations are actually being implemented?

Philippe Dufresne: I'm waiting to see what will be presented. I don't expect there will be one bill for each recommendation. I think there will be one for the private sector and another one for the public sector. I expect the public sector one to come later, but I will continue to stress the need to act quickly on this subject—

Gabriel Hardy: So far, despite your recommendations, the public is not any more protected than it was a year ago.

Philippe Dufresne: So far, the recommendations have yet to be implemented. I'm still using the tools at my disposal as best I can while working with international partners, but I think there is an opportunity here that Parliament should seize as soon as possible.

Gabriel Hardy: Great.

I'll move on to another subject and talk about the studies you have carried out on artificial intelligence, identity theft, challenges with data monitoring and access to information, and so forth.

A partnership with the government of China to send 50,000 vehicles to Canada was announced recently. We know people spend a great deal of time in their vehicles, from where they have conversations with their families. They use vehicles for travel, and they probably discuss certain matters from within the vehicles. Earlier, you said we lose control of data once it leaves the country.

Do you see any potential risk there to Canadians?

Philippe Dufresne: The transfer of data outside Canada is an issue that needs to be controlled. I don't think we can stop it completely because international trade is based on that. We need to strike a balance between privacy, national security and digital sovereignty while enabling international trade. In this connection, privacy measures are useful because they come with other elements related to consent and transparency.

Do we know what is happening? Are we okay with what is happening? Is it easy to say no? Is it for the appropriate purposes? It's important to verify all of these points with regard to digital vehicles, in Canada and abroad, but even more so when data leaves Canadian jurisdiction.

The Chair: Thank you, Mr. Dufresne.

Ms. Lapointe and Mr. Hardy, you can ask more questions if you like.

Ms. Lapointe, you have the floor.

Linda Lapointe: Thank you very much, Mr. Chair.

I'd like to welcome the two witnesses.

This is all very interesting. When it comes to the government's work on your recommendations, I believe you're hopeful that your recommendations will come to fruition, aren't you?

Philippe Dufresne: I am very hopeful. The Minister of Artificial Intelligence has made some public statements where he said work was in progress and that work is needed when it comes to artificial intelligence. It boils down to what I have said, which is that we need to have this innovation and a strong economy while protecting privacy. That is feasible.

Linda Lapointe: Thank you.

You talked about your U.K. counterpart earlier. You said you carried out a joint investigation into a genetic data company that received mailed-in tests from people who wanted to learn about their ancestry, and that you reached the same finding, but that in the U.K., the company was fined.

Philippe Dufresne: That's right. It was a global genetic genealogical company, which had experienced a privacy breach. People stole information on millions of people, including 300,000 Canadians. You can imagine what that means. Genetic data are extremely sensitive.

When we receive this type of complaint—in this case, I conducted a joint investigation with my U.K. counterpart—we check whether the company took proper precautions when processing data and if it had sufficient protection mechanisms. Unfortunately, we found the company lacked strong passwords and protection systems, and it was too slow to respond to signs that bad actors were trying to get into their system.

My U.K. counterpart and I had similar findings. However, they have order-making powers and the power to impose fines in the event of such significant violations, and they used those powers. I believe they levied millions of pounds in penalties. On the other hand, I could only make recommendations. It was a pretty flagrant situation. We held a press conference, and I was asked why I had not levied fines. I responded that I did not have the power to impose fines.

• (1730)

Linda Lapointe: Did the penalties in the U.K. force the company to move more quickly to take corrective measures?

Philippe Dufresne: Indeed, the company agreed with all our recommendations. This shows fine-making and order-making powers encourage organizations to agree with recommendations. Would the company have been that amenable had it dealt with my office only? Maybe. As I said, we can be very persuasive. We criticize organizations publicly and they don't like that. However, if there are no financial penalties, it's difficult to persuade boards of directors to spend huge amounts of money to implement recommendations. I believe they need incentives. I think any company executive is going to pay attention to risks, both legal and financial.

Linda Lapointe: Earlier, you spoke at length about the best interests of the child, and consent. I know that right now, people are leaning towards not putting up pictures of children because they don't have the children's consent. Indeed, young children can't give consent.

What would you recommend to ensure consent and the best interest of the child when it comes to all the photos on social media?

Also, how can facial recognition and the possibility that it may not end well for these children, who did not choose to be on social media, be taken into consideration?

Philippe Dufresne: All of these examples show why I have made children's privacy one of my three top strategic priorities. They are vulnerable because sometimes people put their data online without their knowledge or consent. We need to do several things. First, we need to interpret the law in a way that takes their best interest into account. This occurs in family law and across all legal fields in general, but its application when it comes to privacy is still falling short.

For example, it would be a matter of saying that a child's consent must be informed and age appropriate. In certain cases, parents will give their consent, while in other cases children will give their personal consent. Communication must be tailored to the age of the child. I recently set up a youth advisory council within the Office of the Privacy Commissioner. I will meet with young people aged 13 to 18. I will ask them how they feel, what they want in terms of privacy, and how they use social media.

In short, we need to do more.

Linda Lapointe: I'd like to ask another question.

The Chair: Your time is up, but you can ask more questions in the next round.

We'll now go to Mr. Hardy, who is sharing his time with Mr. Cooper.

You have five minutes, Mr. Hardy.

Gabriel Hardy: I have a fairly simple question, and it ties back to what I asked you earlier about the Chinese government.

Until very recently, China was seen as posing the most significant threat to our country. However, now we're opening up trade with the country. You work with global counterparts around the world, including Australia and England.

Are you comfortable working with China, should a collaboration come up? Do you have good contacts? Do you feel you can work with China and at the same time trust that security of personal information will be guaranteed in the same way that it is by our counterparts from the U.K., Australia, and maybe even the U.S.?

Philippe Dufresne: Canada is very active on the global stage and there are many networks, including the global privacy enforcement network, the G7 data protection and privacy authorities round table, which we spoke about earlier, and the Asia Pacific privacy authorities forum. We work closely with Japan, Korea and Singapore. There are also commissioners in Hong Kong that we work with. I must say that we have productive discussions on privacy and what we would like to see as privacy commissioners.

However, I've not had any interactions on privacy with the Chinese government, only with my counterparts. We try to speak with one voice, the strongest voice possible, and this has allowed us to issue a number of statements on privacy. That said, during our investigation into TikTok, for example, we expressed concern that the Chinese government had expanded powers to obtain information from private companies, and we wanted TikTok to state there was a possibility data could be sent to China and made accessible in that context.

• (1735)

Gabriel Hardy: Does that mean China worked with you?

Philippe Dufresne: Yes, TikTok agreed to change its policies on that issue.

The Chair: You have less than three minutes, Mr. Cooper.

[English]

Michael Cooper: Commissioner, let's go back to the government's cybersecurity bill. In addition to not requiring judicial authorization before the minister can order a telecommunications service provider to turn over metadata, subscriber account information, website visits, the location of financial data and other personal data, the bill, as you noted, and those powers do not require that it be necessary and proportionate. The current standard is one of relevancy. Is that correct?

Philippe Dufresne: It's correct for one of the powers. There are a number of powers in the bill. Some—

Michael Cooper: I'm talking about under paragraph 15.

Philippe Dufresne: Yes.

Michael Cooper: That is a pretty permissive standard.

Philippe Dufresne: It's much more permissive than necessity and proportionality, which is why I've recommended that it be changed to that.

Michael Cooper: There's no judicial authorization and no necessary and proportionate standard. We're talking about some pretty significant information and data concerning the privacy of Canadians.

I would characterize it as excuses the government has put forward when privacy concerns have been raised with regard to this bill. It has said there's a lower expectation of privacy with respect to engaging in a regulated activity. That's true. There is a lesser expectation or reasonable expectation of privacy.

I want to confirm that when it comes to the Internet, that is not a regulated activity, is it? In fact, it engages significant privacy expectations.

Philippe Dufresne: In this case, I have not called for there to be a warrant or judicial authorization. I have called and I am calling for a stronger threshold, which should be, in my view, necessity and proportionality.

Michael Cooper: Right, but I'm also saying that this is an activity, the use of the Internet, metadata, all of these things, based upon judgments of the Supreme Court, that engage significant privacy expectations. That's a fair statement, isn't it?

Philippe Dufresne: I think it's enough to warrant necessity and proportionality as the standard, so that you assess if you need it and how much you need. Don't get more than you need. Also, have you looked for less privacy-impacting mechanisms?

The Chair: Thank you, Mr. Cooper.

[*Translation*]

Ms. Lapointe, I believe you're going to share your time.

Linda Lapointe: That's right, Mr. Chair, but first, I'd like to make a brief point.

Bill C-16, an act to amend certain acts in relation to criminal and correctional matters (child protection, gender-based violence, delays and other measures) was tabled in the House. The bill also covers deepfakes and non-consensual sharing of intimate images.

Are you aware of this?

Philippe Dufresne: Yes, I am.

That falls under criminal law. On my part, the Privacy Act continues to play an important role. Not all issues are going to necessarily fall under criminal law, so this protection is important.

As with my investigation into Aylo, I think non-criminal laws can also serve to protect Canadians.

Linda Lapointe: We have received some extremely alarming testimony to the effect that the end of the world is coming because of superintelligence and artificial intelligence. Comparisons have been made with nuclear war and climate change.

You have met with your fellow G7 commissioners. Are people from other parts of the world equally fearmongering?

● (1740)

Philippe Dufresne: There are all kinds of discussions at global events that I attend, including the G7. When it comes to privacy, my counterparts and I are focusing on the situation at hand right now and on the future, including emerging artificial intelligence agents.

Indeed, we are hearing these concerns. During the G7 summit, we invited Mr. Yoshua Bengio to share some of these concerns with us. I think it's important to have these discussions. However, not everyone shares these concerns. In other words, not everyone is pessimistic. The message we are hearing emphasizes what we need to do now to protect ourselves. Strengthening privacy and paying attention to ensuring transparency, human oversight, consent and legitimate purposes can make this kind of development that we want to avoid far less likely.

The Chair: You have 2 minutes and 45 seconds, Mr. Sari.

Abdelhaq Sari: Thank you very much, Mr. Chair.

Generally, the right to information or cognitive liberty is fundamental, and this is very important to me. It's one of the risks that I've been looking into of late. Earlier, I alluded to the issue of concentration of cognitive capability, as it's called. Unfortunately, the

concentration of cognitive capability is not just on knowledge itself, but also on the development and creation of what is known as creative knowledge. It's not about knowledge itself, but the creation of knowledge.

One thing that intrigues and worries me in equal measure is the growing concentration of power and the fact that it's concentrated in the hands of a small number of players. The term "universal" does not necessarily mean that it's international and that it applies across all countries. The growing concentration of power rests in the hands of a few players.

You are the commissioner and we are parliamentarians. What legal framework do we have right now?

What path should we take to understand the problem and determine how best to protect personal information and the right to information, while ensuring it's not managed through a single approach?

Philippe Dufresne: I think we need to use the tools we have. In my case, this includes collaborating across a number of disciplines, and in my field, that is privacy. Cognitive psychology is also very important to help us understand how decisions are made or not made and how people can be manipulated by algorithms, by messages and by artificial intelligence. It's about ensuring humans have a role in all this.

I have made some legislative recommendations on the need for more transparency and to ensure privacy and human dignity right from the beginning, right from design.

When it comes to the small number of players, I think this speaks to the need for international collaboration at the governmental, parliamentary and regulatory level, and we are doing that. It would be hard for one country to regulate this issue because it's transnational. However, we can do so by working with the international community, and that's what we're doing.

The Chair: Thank you, Mr. Sari.

[*English*]

That concludes today's panel.

Mr. Dufresne, on behalf of the committee, I want to thank you for being before us. I am certainly confident in how you handle your file and your staff. You bring that confidence to a great degree before this committee. I want to thank you for your testimony today.

I have a couple of things I need to quickly discuss with the committee. There are two pressing issues that we need to move on.

The first one is I need concurrence in the House on the Conflict of Interest Act. We are expecting that the draft report on our study will be landing on our desks at some point soon, so I need to move on that. We haven't got concurrence to ensure that this committee can eventually present the report to the House.

The second one I need concurrence on is the Lobbying Act and the upcoming study for that. I'm going to deal with that on Thursday. I'm going to get motions from the committee on both those issues so that we can move concurrence in the House and make sure this committee is the appropriate venue and that the House agrees we are to study both. I just wanted to bring that to your attention.

We have the AI minister coming on Thursday. There was a motion that he come for two hours. He's only coming for one. We have tried significantly to get him here for two, but he has committed to one hour with officials following in that second hour. I just want to make the committee aware of the efforts that the clerk has put in to try to get the minister here for two hours as per the committee request in the motion that was passed unanimously.

I have no other business. That's it. Enjoy the day.

The meeting is 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>