## EVIDENCE

OTTAWA, Wednesday, April 15, 2026

The Standing Senate Committee on Transport and Communications met with videoconference this day at 6:48 p.m. [ET] to examine and report on the opportunities and challenges of artificial intelligence (AI) in the information and communication technology sector.

**Senator Larry W. Smith** (*Chair*) in the chair.

[*Translation*]

**The Chair:** Honourable senators, I welcome you to this meeting of the Standing Senate Committee on Transport and Communications. Thank you for your cooperation.

[*English*]

My name is Larry Smith. I am a senator from Quebec and chair of the committee. Now I would like to ask my colleagues to introduce themselves.

**Senator Simons:** Senator Paula Simons, Alberta. I come from Treaty 6 territory.

**Senator Wilson:** Duncan Wilson, British Columbia.

**Senator Mohamed:** Farah Mohamed, Ontario.

**Senator Arnold:** Dawn Arnold, New Brunswick.

[*Translation*]

**Senator Petitclerc:** Chantal Petitclerc from Quebec.

[*English*]

**Senator Lewis:** Todd Lewis from Saskatchewan.

[*Translation*]

**Senator Aucoin:** Réjean Aucoin from Nova Scotia.

[*English*]

**Senator Dasko:** Donna Dasko, Ontario.

**The Chair:** Thank you, colleagues. I would like to welcome everyone with us today as well as those listening to us online on the Senate's website, sencanada.ca. We are meeting today to continue our study on the opportunities and challenges of artificial intelligence, or AI, in the information and communication technology sector. With that, I would like to introduce our first panel.

## TÉMOIGNAGES

OTTAWA, le mercredi 15 avril 2026

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 18 h 48 (HE), avec vidéoconférence, pour examiner, afin d'en faire rapport, les possibilités et les défis de l'intelligence artificielle (IA) dans le secteur des technologies de l'information et des communications.

**Le sénateur Larry W. Smith** (*président*) occupe le fauteuil.

[*Français*]

**Le président :** Chers collègues, je vous souhaite la bienvenue à la séance du Comité sénatorial permanent des transports et des communications. Merci pour votre coopération.

[*Traduction*]

Je m'appelle Larry Smith, sénateur du Québec et président du comité. J'aimerais maintenant demander à mes collègues de se présenter.

**La sénatrice Simons :** Sénatrice Paula Simon, de l'Alberta. Je viens du territoire du Traité nº 6.

**Le sénateur Wilson :** Duncan Wilson, de la Colombie-Britannique.

**La sénatrice Mohamed :** Farah Mohamed, de l'Ontario.

**La sénatrice Arnold :** Dawn Arnold, du Nouveau-Brunswick.

[*Français*]

**La sénatrice Petitclerc :** Chantal Petitclerc, du Québec.

[*Traduction*]

**Le sénateur Lewis :** Todd Lewis, de la Saskatchewan.

[*Français*]

**Le sénateur Aucoin :** Réjean Aucoin, de la Nouvelle-Écosse.

[*Traduction*]

**La sénatrice Dasko :** Donna Dasko, de l'Ontario.

**Le président :** Merci, chers collègues. Je tiens à souhaiter la bienvenue aux gens avec nous aujourd'hui, ainsi qu'à celles et ceux qui nous écoutent à partir sur le site web du Sénat sencanada.ca. Nous nous réunissons aujourd'hui pour continuer notre étude sur les possibilités et les défis de l'intelligence artificielle, l'IA, dans le secteur des technologies de l'information et des communications. Sur ce, j'aimerais vous présenter notre premier groupe de témoins.

We have with us today Emily Laidlaw, Canadian Research Chair in Cybersecurity Law, Associate Professor, University of Calgary; and Connor Leahy, United States Director, ControlAI, who is with us virtually. Welcome. Thank you for joining us today.

Witnesses will provide opening remarks, which will be followed by a question-and-answer session with senators. I will now invite Ms. Laidlaw to give her opening remarks.

**Emily Laidlaw, Canadian Research Chair in Cybersecurity Law, Associate Professor, University of Calgary, as an individual:** Thank you, chair and honourable senators, for inviting me to speak today. I will focus my remarks today on two key points: that Canada needs to update its laws to address AI, which is probably not surprising, and that "deepfakes" create unique threats that require particular attention.

First, about AI laws, I want to echo a key message that Brent Arnold will make later today, and that is that Canada cannot continue to rely on outdated, piecemeal laws to handle the tsunami that is AI. We need coherent and comprehensive laws grounded in a whole-of-government strategy.

If I could wave a magic wand, what would a healthy, resilient AI environment look like for Canada? It would mean that innovators and investors have regulatory certainty about their compliance obligations in Canada; that our laws provide rigorous accountability but are sensible and do not create needless complexity for businesses; that Canada has embedded digital sovereignty through investment in Canadian talent and training, minimized dependency on U.S. players and developed strategic international partnerships; that individuals harmed by AI have avenues of legal redress; that all levels of government — federal, provincial and across departments and agencies — work in coordination; and that Canadians are educated about AI, cybersecurity and information manipulation.

So how do we get there? And, importantly, where do we start today?

First, the federal government should prioritize passing comprehensive digital laws and, in the meantime, work with industry to create codes of practice. Several bills have been introduced in recent years on privacy, AI, online harms, critical infrastructure and age verification — I've spoken with all of you a few times on that. All of these deal with different dimensions

Nous accueillons aujourd'hui Mme Emily Laidlaw, titulaire de la chaire de recherche du Canada en droit de la cybersécurité, professeure agrégée, de l'Université de Calgary; et M. Connor Leahy, directeur, États-Unis, de ControlAI, qui est avec nous par vidéoconférence. Bienvenue. Merci à vous d'être avec nous aujourd'hui.

Les témoins feront une déclaration préliminaire, qui sera suivie d'une séance de questions et réponses avec les sénateurs. Je vais maintenant inviter Mme Laidlaw à faire sa déclaration préliminaire.

**Emily Laidlaw, titulaire de la chaire de recherche du Canada en droit de la cybersécurité, professeure agrégée, Université de Calgary, à titre personnel :** Merci, monsieur le président et honorables sénateurs et sénatrices de m'avoir invitée aujourd'hui. Ma déclaration liminaire d'aujourd'hui concerne deux points clés précis : d'abord, le Canada doit mettre ses lois à jour pour qu'elles traitent de l'IA, ce qui n'est sans doute pas surprenant, et ensuite, les « hypertrucages » créent des menaces uniques qui requièrent une attention particulière.

Tout d'abord, parlons des lois sur l'IA. J'aimerais me faire l'écho d'un message clé que M. Brent Arnold transmettra plus tard aujourd'hui, soit que le Canada ne peut pas continuer de s'en remettre à des lois fragmentaires désuètes pour traiter le tsunami qu'est l'IA. Nous avons besoin de lois cohérentes et complètes fondées sur une stratégie pangouvernementale.

Si j'avais une baguette magique, à quoi ressemblerait un environnement sain et résilient en matière d'IA au Canada? Cela voudrait dire que les innovateurs et les investisseurs ont une réglementation claire, qui indique clairement leurs obligations en matière de conformité au Canada; que nos lois exigent une reddition de comptes rigoureuse, tout en ayant du sens et en ne compliquant pas inutilement la vie des entreprises; que le Canada a assuré sa souveraineté numérique en investissant dans des talents canadiens et dans la formation, qu'il a diminué sa dépendance à l'égard des joueurs américains et qu'il a tissé des partenariats stratégiques internationaux; que les gens qui ont subi des préjudices en raison de l'IA ont des recours juridiques; que tous les ordres de gouvernement — fédéral, provinciaux, ministères et organismes — travaillent en coordination; et que les Canadiens sont renseignés au sujet de l'IA, de la cybersécurité et de la manipulation de l'information.

Comment pouvons-nous arriver à cela? Mais surtout, par où commençons-nous aujourd'hui?

Premièrement, le gouvernement fédéral devrait en priorité adopter des lois complètes sur les services numériques et, entre temps, travailler avec l'industrie pour établir des codes de pratique. Ces dernières années, on a présenté plusieurs projets de loi sur la vie privée, l'IA, les préjudices en ligne, l'infrastructure essentielle et la vérification de l'âge; je vous en ai tous parlé à

of the AI conundrum. The foundation is privacy law, as AI runs on data.

The next layer is cybersecurity. AI poses an existential threat to cybersecurity while also being part of the solution, as we saw, of course, with news last week of Anthropic's latest Mythos model. That is one story among many.

The next layer would be what I would call risk management laws. Both the proposed AI act and online harms legislation were based on the idea that companies have obligations to mitigate the risks associated with the products and services they are putting out into the world.

Second, interoperability with other legal regimes is the name of the game. What do I mean by that? Technology is global, and a secure and resilient Canada relies on cooperation with others. That does not mean our laws are the same but that they have certain features in common. For example, risk management duties are the interoperable features of AI and online harms legislation in numerous jurisdictions. That is why that foundation is so important for any law passed in Canada.

Lastly, I want to talk about the unique threat posed by "deepfakes." AI, as we know, has made creation of hyper-realistic images, video and audio easy and voluminous. This is a threat at all levels, from weaponizing foreign actors to undermine democracy, to fraud, creation of child sexual abuse images and intimate images of adults or other distortions that can ruin reputations, and so on.

In my research, I talk about it as a slow violence. It's gradual, hidden in plain sight and rooted in structural inequalities. There is only so much law can do to address this.

Laws can be updated to hold individuals legally culpable when they can be identified. Bill C-16 is a good example of this. Currently, it is not a crime to create and share an intimate "deepfake," but Bill C-16 proposes to amend the Criminal Code to criminalize that.

The other area is platform regulation. This would be the online harms legislation that was introduced in Bill C-63, duties to address the systemic risks of harm. It might be labelling synthetic media or having special rules during crises or election periods. It might be policies for impersonation.

quelques reprises. Tout cela concerne différentes dimensions du mystère de l'IA. La fondation, c'est la loi sur la protection de la vie privée, puisque l'IA fonctionne avec des données.

La prochaine couche, c'est la cybersécurité. L'IA est à la fois une menace existentielle pour la cybersécurité et une partie de la solution, comme nous l'avons vu, bien entendu, dans les nouvelles, la semaine dernière, au sujet du dernier modèle Mythos d'Anthropic. C'est une histoire parmi tant d'autres.

La prochaine couche est ce que j'appellerais les lois sur la gestion du risque. Tant la loi sur l'IA proposée que la Loi sur les préjudices en ligne sont fondées sur l'idée que les entreprises doivent atténuer les risques associés aux produits et services qu'elles offrent au monde entier.

Deuxièmement, le nerf de la guerre, c'est l'interopérabilité avec d'autres régimes juridiques. Qu'est-ce que je veux dire par là? La technologie, c'est mondial, et pour avoir un Canada sécuritaire et résilient, il faut coopérer avec les autres. Cela ne veut pas dire qu'il faut adopter des lois identiques, mais elles doivent avoir des traits communs. Par exemple, l'obligation de gérer le risque est une caractéristique interopérable des lois sur l'IA et des lois sur les préjudices en ligne de nombreuses administrations. C'est pour cette raison que la fondation est si importante pour n'importe quelle loi adoptée au Canada.

Troisièmement, j'aimerais parler de la menace unique que représentent les « hypertrucages ». L'IA, comme nous le savons, crée d'énormes quantités d'images, de vidéos et de contenus audio très réalistes, et elle le fait facilement. C'est une menace à plusieurs niveaux; des acteurs étrangers pourraient s'en servir pour attaquer la démocratie, d'autres pour commettre des fraudes, pour créer de la pornographie juvénile ou pour générer des images à caractère sexuel d'adultes ou des représentations modifiées pour nuire à la réputation de quelqu'un et ainsi de suite.

Dans mes recherches, j'appelle cela de la violence lente. C'est graduel, caché, mais à la vue de tous, et enraciné dans les iniquités structurelles. Dans ce domaine, les lois ont leur limite.

Les lois peuvent être mises à jour pour que les auteurs de tels actes, quand ils peuvent être identifiés, soient reconnus coupables en vertu de la loi. Le projet de loi C-16 est un bon exemple. À l'heure actuelle, ce n'est pas un crime de créer et de partager un « hypertrucage » à caractère sexuel, mais le projet de loi propose d'amender le Code criminel pour criminaliser cela.

L'autre aspect, c'est la réglementation des plateformes. C'est la Loi sur les préjudices en ligne qui a été présentée dans le projet de loi C-63, concernant le devoir de protection contre les risques de préjudice systémiques. Il pourrait s'agir d'identifier les médias synthétiques ou d'adopter des règles spéciales durant les crises ou les périodes électorales. Il pourrait s'agir de politiques sur l'usurpation d'identité.

These are systemic laws because they are not concerned with actioning individual pieces of content. Rather, they are more about the deeper organizational and technical practices that, together, improve the health of the information ecosystem. While some AI-generated content is illegal and should be removed, some of the most insidious forms of "deepfakes" that impact democracy are perfectly legal, so systemic approaches are the only and best solution.

I see that I am almost out of time, so I will leave the comments there, and perhaps we can discuss a human-centric approach to cybersecurity in the question period. Thank you.

**The Chair:** Thank you, Ms. Laidlaw.

**Connor Leahy, United States Director, ControlAI:** Thank you, Mr. Chair and members of the committee, for inviting me to testify today.

I am the U.S. Director of ControlAI, a non-profit organization focused on mitigating the security risks posed by advanced AI. Previously, I was the CEO of the AI safety start-up Conjecture and the head of the open source research collective EleutherAI.

There are many varied, complex and important challenges we face with AI, but today, I want to highlight the catastrophic risks up to and including human extinction that are posed by what is called superintelligence or "smarter-than-human" AI.

The existence of systems that could outperform humans across all relevant domains — including science, business and politics — and that is not controllable by trustworthy, democratically elected institutions poses a massive national and international security risk.

While such systems do not yet exist, the creation of the first such superintelligent system is widely expected by experts, both in industry and academia, to happen within the next two to five years. It is rare these days to find an expert in the field who believes it is more than 10 years away.

A major part of the problem is that AI researchers and companies fundamentally do not understand how the AI systems they are creating actually work and cannot develop them in a safe manner. AIs are not built from code that is written line by line, like we do with traditional software. Instead, AI is essentially grown. AI models are created by taking vast amounts of data and using enormous computing power, through a process called "training," to produce what is called a "neural network." One can imagine this neural network as billions and billions of

Ce sont des lois systémiques parce qu'elles ne mettent pas en œuvre des mesures législatives individuelles. Elles concernent davantage les pratiques organisationnelles et techniques plus approfondies qui, ensemble, améliorent la santé de l'écosystème de l'information. Même si certains contenus générés par l'IA sont illégaux et qu'ils devraient être retirés, certaines des formes les plus insidieuses « d'hypertrucage » qui ont une incidence sur la démocratie sont tout à fait légales, et c'est pourquoi la meilleure, voire la seule solution, ce sont les approches systémiques.

Je vois que mon temps est presque écoulé, donc je vais m'arrêter là, et, nous pourrons peut-être durant la période de questions parler d'une approche axée sur l'humain en matière de cybersécurité. Merci.

**Le président :** Merci, madame Laidlaw.

**Connor Leahy, directeur, États-Unis, ControlAI :** Merci, monsieur le président et membres du comité, de m'avoir invité à comparaître aujourd'hui.

Je suis directeur aux États-Unis pour ControlAI, un organisme à but non lucratif qui cherche à atténuer les risques de sécurité que représente l'IA avancée. Avant, j'étais PDG de Conjecture, une entreprise en démarrage œuvrant dans le domaine de la sécurité de l'IA et j'ai été à la tête du collectif de recherche en code source ouvert EleutherAI.

Nous faisons face à beaucoup d'enjeux différents et complexes dans le domaine de l'IA, mais aujourd'hui, j'aimerais vous faire part des risques de catastrophe, pouvant aller jusqu'à l'extinction de l'humanité, que pose la soi-disant superintelligence ou l'IA « plus intelligente que l'humain ».

L'existence de systèmes qui pourraient faire mieux que les humains dans tous les domaines pertinents — y compris les sciences, les affaires et la politique — et que les institutions dignes de confiance, élues démocratiquement, ne parviennent pas à contrôler, fait peser un énorme risque sur la sécurité nationale et internationale.

Même si ces systèmes n'existent pas encore, la plupart des experts de l'industrie et du milieu universitaire s'attendent à ce que le premier système superintelligent soit créé d'ici deux à cinq ans. De nos jours, il est rare qu'un expert du domaine nous dise que cela prendra plus de 10 ans.

Le problème, c'est principalement que les chercheurs en IA et les entreprises qui œuvrent dans ce domaine ne comprennent pas vraiment dans les faits comment fonctionnent concrètement les systèmes d'IA qu'ils créent et qu'ils ne peuvent donc pas les développer de façon sécuritaire. L'IA n'est pas construite à partir de codes rédigés ligne par ligne, comme c'est le cas pour les logiciels traditionnels. On fait plutôt croître l'IA. On crée des modèles d'IA en recueillant d'énormes quantités de données, puis on les traite à l'aide d'une puissance informatique colossale;

numbers. And if one multiplies and adds all these numbers in the right order, you get ChatGPT. However, we don't really know why or what is going on inside these numbers. This is an unsolved scientific problem.

Dario Amodei, the CEO of Anthropic, one of the largest AI companies, recently said that we now perhaps "understand 3% of how they work." This is, in my opinion, somewhat of an overestimation.

If a superintelligence is built, humanity will lose control over its future. If there is a non-human force that outcompetes us in scientific and military development; in persuasion; in politics and propaganda; and in business and economic activities, this force will, all things equal, be the force deciding the future. It is likely such systems, for example, wishing to take our resources, would simply outcompete and drive humanity to extinction. It is hard to imagine a world with millions or even billions of uncontrolled superintelligent systems running around and competing with humanity that turns out well.

Unfortunately, the current AI development paradigm and lack of insight into how AI systems function do not allow the safety-by-design approaches we use for other advanced, highly risky technologies. We would not, for example, build nuclear power plants if we did not know how to control nuclear reactions.

Where does this leave us today? Right now, multiple companies are pouring hundreds of billions of dollars into developing superintelligent AI as quickly as possible, despite experts' warnings that this stage of the technology poses unprecedented risks up to and including the extinction of humanity.

This haste is, in my opinion, directly tied to an attempt to outrun legislation and to complete their project before the wider public and government wake up to these completely unconscionable risks that the non-consenting public is being exposed to by private, oversightless and reckless actors.

To conclude, I'd like to offer the committee three recommendations for how Canada can act now to respond to the threat posed by superintelligence.

First, the Canadian government should publicly recognize superintelligence as a national and global security threat that poses an extinction risk to humanity.

on appelle ce processus la « formation », et on finit par produire ce que l'on appelle un « réseau neuronal ». Vous pouvez voir ce réseau neuronal comme une accumulation de milliards et de milliards de chiffres. Si vous multipliez ou additionnez tous ces chiffres dans le bon ordre, vous obtenez ChatGPT. Toutefois, nous ne savons pas vraiment pourquoi, ni ce qui se passe avec ces chiffres à l'intérieur. C'est un problème scientifique qui reste sans réponse.

Dario Amodei, le PDG d'Anthropic, l'une des plus grandes entreprises d'IA, a récemment dit que, à l'heure actuelle, nous « comprenons peut-être 3 % de son fonctionnement ». Selon moi, c'est une surestimation.

Si on construit une superintelligence, l'humanité perdra le contrôle de son avenir. Si une force qui n'est pas humaine nous supplante dans les domaines du développement scientifique et militaire, de l'influence, de la politique, de la propagande, des affaires et de l'économie, cette force, toutes choses étant par ailleurs égales, décidera de l'avenir. Il est probable que de tels systèmes, s'ils souhaitent prendre nos ressources, par exemple, n'auront qu'à nous supplanter et ils entraîneront l'extinction de la race humaine. Il est difficile d'imaginer que tout finira bien dans un monde où des millions, voire des milliards de systèmes superintelligents incontrôlables rivalisent avec l'humanité.

Malheureusement, le paradigme actuel du développement de l'IA et l'absence de connaissances sur le fonctionnement de ces systèmes ne nous permettent pas d'appliquer les approches de conception sécuritaire dont nous nous servons pour d'autres technologies avancées très risquées. Nous ne construirions pas, par exemple, des centrales nucléaires si nous ne savions pas comment contrôler les réactions nucléaires.

Alors, où en sommes-nous aujourd'hui? À l'heure actuelle, de multiples entreprises investissent des centaines de milliards de dollars pour développer une IA superintelligente le plus vite possible, malgré la mise en garde des experts qui disent que cette étape de la technologie pose des risques sans précédent qui pourraient même mener à l'extinction de l'humanité.

Selon moi, cette hâte est directement liée à une tentative de prendre la loi de vitesse et de terminer les projets avant que le grand public et le gouvernement réalisent les risques inadmissibles auxquels des acteurs privés imprudents qui ne sont pas surveillés exposent le grand public non consentant.

Pour terminer, j'aimerais présenter au comité trois recommandations sur ce que le Canada pourrait faire maintenant pour réagir à la menace que pose la superintelligence.

Premièrement, le gouvernement canadien devrait reconnaître publiquement que la superintelligence est une menace pour la sécurité nationale et mondiale et qu'elle pourrait entraîner l'extinction de la race humaine.

Second, Canada should begin negotiating an international agreement to prohibit the development of superintelligence, given that there is no scientific consensus it can be developed in a way that does not threaten humanity with extinction.

Third and finally, alongside other major national security issues, the Canadian government should begin closely monitoring the threat of superintelligence being developed and develop detailed scenario planning and doctrines.

I would be happy to take any questions you may have. Thank you.

**The Chair:** Thank you very much, Mr. Leahy. That was quite a sobering introduction, I must say.

I would like to advise senators they will have five minutes each for the first round of questions, and the same for the second round if time permits.

I'm a little nervous, actually, sitting here after reading that. There will be quite a bit of feedback for Mr. Leahy.

**Senator Dasko:** It's very sobering. I guess I have to jump right in and take this on. Thank you both for being here.

So the superintelligent AI systems are going to take control. What is the goal of one of these systems? They don't have the human goals of power, wealth, prestige or happiness — the goals that we have. How do they operate? What is the motivation of a system that is seeking control?

**Mr. Leahy:** The true answer is we don't know. We don't know how the systems work internally. We don't know why they make many of the decisions they do.

What we are seeing in tests of systems already is they are, in certain circumstances, showing unwanted behaviour, such as attempting to escape containment, reproduce themselves onto other servers or even threaten or blackmail users or developers when threatened with deletion.

This is not behaviour that was programmed into these systems on purpose; it developed purely spontaneously.

In my opinion, what I expect will happen is it won't be one specific AI system on one specific computer; it will be millions and billions of AIs competing with each other that leads to this threat.

Deuxièmement, le Canada devrait commencer à négocier un accord international visant à interdire le développement de la superintelligence, étant donné que le milieu scientifique n'est pas arrivé à un consensus sur la question de savoir si elle peut être développée sans devenir une menace pour la race humaine.

Troisièmement, le gouvernement canadien devrait commencer à surveiller étroitement la menace de la superintelligence qui est en train d'être développée, ainsi que les autres enjeux importants qui touchent la sécurité nationale, planifier des scénarios et élaborer des doctrines détaillées.

Je répondrai avec plaisir à vos questions. Merci.

**Le président :** Merci beaucoup, monsieur Leahy. Je dois dire que c'est une introduction qui donne à réfléchir.

J'aimerais souligner aux sénateurs qu'ils disposent d'environ cinq minutes pour la première ronde, tout comme la deuxième ronde, si le temps nous le permet.

Je suis en fait un peu nerveux d'être ici, après avoir lu cela. Beaucoup de commentaires seront adressés à M. Leahy.

**La sénatrice Dasko :** C'est très inquiétant. Je vais me jeter à l'eau et poser la première question. Merci d'être ici.

Donc, vous dites que les systèmes d'IA superintelligents prendront le contrôle. Quel est l'objectif de ces systèmes? Ils ne recherchent pas le pouvoir, la richesse, le prestige ou le bonheur comme les humains, nos objectifs à nous. Comment fonctionnent-ils? Pourquoi un système chercherait-il à prendre le contrôle?

**M. Leahy :** En vérité, nous ne le savons pas. Nous ne savons pas comment fonctionnent les systèmes, à l'intérieur. Nous ne savons toujours pas pourquoi ils prennent les décisions qu'ils prennent.

Ce que nous voyons déjà quand nous faisons des tests, c'est que, dans certaines circonstances, les systèmes ont un comportement indésirable. Ils tentent parfois, par exemple, de s'échapper d'un confinement, de se reproduire dans d'autres serveurs ou même de menacer ou de faire chanter des utilisateurs ou des développeurs quand ils sont menacés d'élimination.

Ce n'est pas un comportement qui a été programmé délibérément dans ces systèmes; il s'est développé spontanément.

Selon moi, la menace ne viendra pas d'un seul système d'IA installé sur un seul ordinateur; elle viendra des millions et des milliards d'IA qui rivalisent les unes avec les autres.

The various AI systems will be set out into the world with many different tasks and configurations, and they will compete with each other. They will compete for power, resources, political and military control and so on.

Out of this chaos, quite frankly, I expect there will emerge forces that may have simple goals or may have goals that are very hard for us to understand.

**Senator Dasko:** How do they gain political control in a democracy?

**Mr. Leahy:** Mass persuasion is a very powerful tool, as we have already seen through psychological operations run by foreign nation-states within the West and elsewhere. AI systems can bring this to a whole new level.

Imagine every person with their own personalized KGB agent assigned to them who can convince them of anything, show them fake media, make promises to them, threaten them, bribe them and blackmail them. A lot of this isn't feasible at the moment because intelligence agents are expensive to train, but if you have one AI system that is capable enough as a top intelligence system, you can copy it a million times and run operations that are hard to imagine compared to today.

**Senator Dasko:** I don't know where to begin. Maybe I should switch for a moment. I will have to contemplate this.

Professor Laidlaw, you mentioned the types of laws we need to have. We have no laws right now, correct? Are we actually nowhere?

**Ms. Laidlaw:** We are somewhere. Isn't that a terrible answer? We have outdated laws that address aspects of it.

**Senator Dasko:** Like privacy and —

**Ms. Laidlaw:** We have a privacy law. Is it outdated? Absolutely, so we need to update that.

We don't have any specific law that regulates AI, but even if you pass an AI law tomorrow that just generally regulates AI, you still need subject-matter-specific laws that deal with dimensions of AI. That is why I mentioned things like online harms legislation, even age verification laws and competition law.

Divers systèmes d'IA configurés de différentes façons seront déployés dans le monde et ils auront des tâches différentes à effectuer. Ils rivaliseront les uns avec les autres. Ils se livreront concurrence pour le pouvoir, les ressources, le contrôle politique et militaire, et ainsi de suite.

Franchement, je m'attends à ce que de ce chaos émergent des forces qui pourraient avoir des objectifs simples ou des objectifs que l'on a de la difficulté à comprendre.

**La sénatrice Dasko :** Comment parviennent-ils à prendre le contrôle dans une démocratie?

**M. Leahy :** La persuasion de masse est un outil très puissant, comme nous l'avons déjà vu dans le cadre d'opérations psychologiques menées par des États-nations étrangers dans des pays occidentaux et ailleurs. Les systèmes d'intelligence artificielle peuvent faire passer cela à un tout autre niveau.

Imaginez un peu que chaque personne se voit attribuer son propre agent du KGB, qui peut la convaincre de n'importe quoi, lui montrer de fausses nouvelles, lui faire des promesses, la menacer, la soudoyer et la faire chanter. C'est en grande partie impossible à faire à l'heure actuelle parce que la formation des agents de renseignements coûte très cher, mais si vous avez un système d'intelligence artificielle suffisamment performant, un système d'intelligence de pointe, vous pouvez le copier un million de fois et mener des activités qui sont difficiles à imaginer aujourd'hui.

**La sénatrice Dasko :** Je ne sais pas par où commencer. Je devrais peut-être changer de sujet pour un instant. Il faut que j'y réfléchisse.

Madame Laidlaw, vous avez parlé du type de lois dont nous avons besoin. Présentement, il n'y a aucune loi, n'est-ce pas? N'y a-t-il vraiment rien?

**Mme Laidlaw :** Il y a quelque chose. N'est-ce pas une réponse terrible? Nous avons des lois caduques qui traitent de certains aspects de la question.

**La sénatrice Dasko :** Comme la vie privée et...

**Mme Laidlaw :** Nous avons une loi sur la protection de la vie privée? Est-elle caduque? Absolument, donc nous devons la mettre à jour.

Nous n'avons aucune loi régissant spécifiquement l'intelligence artificielle, mais, même si vous adoptiez demain une loi qui réglemente l'intelligence artificielle de manière générale, vous aurez tout de même besoin de lois spécifiques traitant des différentes dimensions de l'intelligence artificielle. C'est pourquoi j'ai mentionné des choses comme la loi sur les préjudices en ligne ou même des lois sur la vérification de l'âge et sur la concurrence.

For Canada to be truly resilient, we need to prioritize all-digital laws that have to work together to address the different dimensions where AI is causing an impact.

**Senator Dasko:** Right. So when it comes to comprehensive laws, what should be in those laws? What are the elements?

**Ms. Laidlaw:** I think the core should be risk management. I think some of it should be no-go zones. To reference my colleague Mr. Leahy, the threats he mentions are sobering, right? So we should be thinking in terms of there being no-go zones for AI.

Not everything can be risk-managed because risk management assumes we're okay with a certain error rate and certain things going wrong.

The challenge we're facing right now is this: Let's say we create this risk management law based on the idea of certain no-go zones. We follow some of what Europe has done, and it takes a while to legislate. We need a short-term solution now, which is basically a certain amount of cooperation until it's a practice, but also then to prioritize moving ahead with certain forms of thoughtful legislation.

**Senator Dasko:** I think my time is probably up.

**Senator Lewis:** Thank you both for being here tonight.

Ms. Laidlaw, the minister came and addressed the Senate this week. He talked about some of the recent consultations they've gone through and so on. Have you seen gaps in some of that consultation process as the government tries to move forward to get a handle on some of the things that you're talking about? Have there been gaps in some of that consultation? Is there more the government can do?

**Ms. Laidlaw:** Yes. I think that is the challenge we're facing right now: the need for speed but also thoughtfulness with the laws.

The consultation that happened in the fall was widely criticized — and I think for good reason — because it was so hurried, even though there were really good people at the table who were part of it.

What we need, though, is wider consultation about a more diverse group that reflects the way AI can impact all kinds of sectors, groups and regions of Canada. We need to see that representation across Canada. That hasn't happened so far.

Pour que le Canada soit réellement résilient, nous devons prioriser un ensemble de lois sur le numérique qui fonctionnerait de concert pour encadrer les différentes sphères où l'intelligence artificielle a un impact.

**La sénatrice Dasko :** D'accord. Donc, des lois exhaustives, et qu'est-ce que ces lois devraient contenir? Quels sont ces éléments?

**Mme Laidlaw :** Je pense que la gestion des risques devrait être au cœur de tout cela. Je crois que certaines zones devraient être interdites d'accès. Pour reprendre les mots de mon collègue, M. Leahy, les menaces dont il a parlé font réfléchir, n'est-ce pas? Nous devons donc déterminer des zones dans lesquelles l'intelligence artificielle ne peut pas exister.

Il est impossible de tout gérer en fonction du risque, car la gestion du risque suppose que nous acceptons un certain taux d'erreur et la possibilité que certaines choses vont mal tourner.

Le défi auquel nous faisons face présentement est le suivant : disons que nous élaborons une loi sur la gestion des risques, qui tient compte du concept des zones interdites. Nous suivons en partie ce que l'Europe a fait, et l'adoption d'une loi prend du temps. Nous avons besoin aujourd'hui d'une solution à court terme, qui suppose essentiellement un certain niveau de coopération, jusqu'à ce que cela devienne pratique courante, mais il s'agit aussi de prioriser l'adoption de certaines mesures législatives bien réfléchies.

**La sénatrice Dasko :** Je crois que mon temps est écoulé.

**Le sénateur Lewis :** Merci à vous deux d'être ici ce soir.

Madame Laidlaw, le ministre s'est adressé au Sénat, cette semaine. Il a parlé des récentes consultations qu'ils ont menées et ainsi de suite. Avez-vous relevé des lacunes dans ces processus de consultation, alors que le gouvernement essaie d'aller de l'avant pour prendre en main certains des éléments dont vous avez parlé? Y a-t-il eu des lacunes dans certaines de ces consultations? Le gouvernement peut-il en faire plus?

**Mme Laidlaw :** Oui. Je crois que c'est le défi auquel nous faisons face à l'heure actuelle : le besoin d'aller vite, mais aussi de bien réfléchir aux lois.

La consultation qui a eu lieu l'automne dernier a été critiquée de toute part — et, je crois, avec raison — parce que tout s'est fait très hâtivement, même si des gens vraiment formidables y ont participé.

Nous avons besoin d'une consultation plus large auprès d'un groupe plus diversifié, qui reflète les répercussions que l'intelligence artificielle peut avoir sur toutes sortes de secteurs, de groupes et de régions au Canada. Nous devons voir cette représentation à l'échelle du Canada. Cela n'a pas encore été fait.

I think what we need to do going forward is basically have that core framework in mind of what risk management looks like but start that hard process of a more thorough consultation.

I feel uneasy saying that, given that we need to move on this quite quickly.

**Senator Lewis:** Mr. Leahy, some of the things you brought up — are there AI systems currently being trained to try to balance against some of the things you're talking about?

Are AI policing and trained systems going to be able to police some of the bad actors or some of the things that we're headed toward? Of course, as we learn more and more, there are a lot of gaps in understanding around how AI works.

I really liked your nuclear comparison. There's no way we would allow that kind of activity without controls on it. Is some of that being worked on — AI systems that will police other AI systems?

**Mr. Leahy:** There are definitely many press releases claiming so. In my technical opinion, no adequate efforts currently exist or are adequately funded, or are even in scope with a problem as large as superintelligence.

I think there's a lot of very good work on more narrowly scoped problems, for limited domains, non-general purpose intelligence and so on. But when it comes to something that might be smarter than humans, this is just such a large thing that goes far beyond our current scientific understanding of what it would even mean to control something smarter than us.

There are no adequate measures whatsoever, which is why my general recommendation is not to do so until — if generations of our greatest scientists work on this problem, I'm sure they could make a lot of progress.

Currently, in the nuclear industry, for example, we have a culture of perspective security where we don't allow people to build nuclear reactors and then check if they melt down. Instead, we have people who design extremely detailed security cases for why a reactor design is safe. They submit it to the nuclear regulator. The regulator checks it extremely thoroughly and only then issues a licence to build what is extremely dangerous technology.

À mon avis, à partir d'aujourd'hui, nous devons essentiellement, en gardant à l'esprit ce cadre de référence sur la gestion du risque, commencer le processus exigeant une consultation plus approfondie.

Je suis mal à l'aise de le dire, d'autant plus que nous devons agir assez rapidement.

**Le sénateur Lewis :** Monsieur Leahy, parmi les choses dont vous avez parlé, entraîne-t-on présentement des systèmes d'intelligence artificielle pour tenter de contrebalancer certaines des choses dont vous avez parlé?

Les systèmes de maintien de l'ordre basés sur l'intelligence artificielle et les systèmes entraînés seront-ils capables de contrôler certains acteurs malveillants ou de faire face aux situations qui s'annoncent? Bien sûr, à mesure que nous en apprenons davantage, il y a énormément de lacunes dans la compréhension du fonctionnement de l'intelligence artificielle.

J'ai bien aimé votre comparaison avec le nucléaire. Il est impossible que nous autorisions ce genre d'activité sans contrôle. Est-ce qu'on y travaille, à des systèmes d'intelligence artificielle qui surveilleront d'autres systèmes d'intelligence artificielle?

**M. Leahy :** Il y a certainement de nombreux communiqués de presse qui le prétendent. À mon avis, d'un point de vue technique, il n'existe présentement aucune initiative adéquate, ou bénéficiant d'un financement suffisant, ou qui est même à la hauteur face à un problème aussi vaste que la superintelligence.

Je crois qu'il se fait d'excellents travaux en ce qui concerne des problèmes plus ciblés, pour des domaines limités, les renseignements à des fins autres que générales, et ainsi de suite. Mais, lorsqu'il est question d'une chose qui pourrait être plus intelligente que les humains, c'est un concept tellement vaste, qui dépasse de loin notre compréhension scientifique actuelle de ce que supposerait même le fait de contrôler quelque chose de plus intelligent que nous.

Il n'y a aucune mesure adéquate, et c'est pourquoi je recommande globalement de ne pas nous y aventurer tant que... Si des générations de nos plus grands scientifiques travaillaient sur ce problème, je suis sûr qu'ils pourraient réaliser d'énormes progrès.

Présentement, dans l'industrie nucléaire, par exemple, nous avons une culture de la sécurité préventive, c'est-à-dire que nous ne permettrons pas aux gens de construire un réacteur nucléaire, puis de vérifier s'il se produit une fusion. Nous avons plutôt des gens qui conçoivent des scénarios de sécurité extrêmement détaillés pour expliquer pourquoi la conception du réacteur est sécuritaire. Ces scénarios sont soumis à l'organisme de réglementation nucléaire. Ce dernier les examine attentivement puis c'est seulement à ce moment-là qu'on leur délivre une

This is not at all how AI systems are currently regulated. In fact, there's more regulation on selling a sandwich to the general public than there is on attempting to build superintelligence. Also, this is currently technically impossible; we don't even know how we would build such a safety case.

I believe that if government regulations were put in place, this would incentivize our academics, industry, et cetera, to actually develop these methods. Currently, there's no incentive to build or develop these methods, and government action here could be very valuable.

**The Chair:** Before we move on, I'd like to have Senator Miville-Dechêne introduce herself.

[*Translation*]

**Senator Miville-Dechêne:** Julie Miville-Dechêne from Quebec. I apologize for being late; I had another commitment that went long.

[*English*]

**Senator Wilson:** The scope of my question, I think, is for Mr. Leahy. The scope of our study here is actually quite limiting, but I can't help but ask about the issues you raised.

It seems to me that, to a certain extent, the genie is out of the bottle. Even if we were able to convince our partners that we should try and stop superintelligence, with the companies in those countries that invested in those things, it would be like squeezing Jell-O: It would go somewhere else, to other countries that are prepared to just throw caution to the wind and accept them.

What could Canada do in terms of a regulatory push — but also almost more physically, to block or create a defence for ourselves against this?

**Mr. Leahy:** My work in the U.S. focuses primarily on advocating for the creation of a trust-but-verify regime globally. This is, of course, the kind of regime where it is very important to have the collaboration of U.S. allies, such as Canada, the EU, et cetera. They would, of course, hopefully be part of such regimes. Then, hopefully, we would also be able to establish such regimes with potentially hostile nations.

This doesn't fully exclude, for example, rogue actors or non-compliance, and in this regard, I would say that we should reserve the right to self-defence. The creation of a superintelligence is a direct threat to the lives of our citizens,

licence pour la construction d'une technologie extrêmement dangereuse.

Ce n'est pas du tout ainsi que les systèmes d'intelligence artificielle sont présentement réglementés. En fait, il y a plus de règlements sur la vente d'un sandwich que sur la conception d'une superintelligence. De plus, cela est présentement impossible du point de vue technique; nous ne savons même pas comment nous pourrions élaborer un tel scénario de sécurité.

Je crois que, si le gouvernement adopte une réglementation, cela encouragerait nos universités, nos industries, et cetera, à développer ces méthodes. Présentement, rien ne les incite à mettre au point ou à développer ces méthodes, et une intervention du gouvernement dans ce domaine serait précieuse.

**Le président :** Avant de passer à autre chose, j'aimerais que la sénatrice Miville-Dechêne se présente.

[*Français*]

**La sénatrice Miville-Dechêne :** Julie Miville-Dechêne, du Québec. Je m'excuse de mon retard; j'avais un autre engagement qui s'est prolongé.

[*Traduction*]

**Le sénateur Wilson :** Je crois que, étant donné sa portée, ma question s'adresse à M. Leahy. La portée de notre étude est, en réalité, assez limitée, mais je ne peux m'empêcher de vous poser des questions sur les points que vous avez soulevés.

Il me semble que, dans une certaine mesure, le génie est sorti de la bouteille. Même si nous pouvions convaincre nos partenaires d'essayer d'arrêter la superintelligence, puisque les entreprises de ces pays ont investi dans ce genre de choses, ce serait un coup d'épée dans l'eau : les projets se développeront dans d'autres pays qui sont prêts à faire fi de toute prudence et à les accepter.

Que peut faire le Canada sur le plan réglementaire, mais aussi plus concrètement, pour bloquer cette menace ou trouver un moyen de se défendre contre elle?

**M. Leahy :** Mon travail aux États-Unis vise principalement à promouvoir la mise en place à l'échelle mondiale d'un système fondé sur le principe « faites confiance, mais vérifiez ». C'est bien sûr, le genre de régime où il est essentiel de pouvoir compter sur la collaboration des alliés des États-Unis, comme le Canada, l'Union européenne, et cetera. Ces pays feraient bien sûr, je l'espère, partie de ce genre de régimes. Puis, avec un peu de chance, nous pourrions aussi mettre en place de tels régimes avec des pays potentiellement hostiles.

Cela n'exclut pas entièrement, par exemple, les acteurs malveillants ou les cas de non-conformité, et, à cet égard, je dirais que nous devrions nous réserver le droit de nous défendre. La création d'une superintelligence est une menace directe à la

both in Canada, the U.S. and everywhere else. If necessary, we must be willing to take the necessary defensive measures, the same way we would for, for example, threats regarding weapons of mass destruction, or WMDs.

**Senator Wilson:** I'm going to leave it there. I might have a question in the second round.

**Senator Simons:** Since I don't believe in the Butlerian Jihad, my questions will be for Professor Laidlaw.

At the Liberal Party convention this weekend — which I did not attend, not being a Liberal — there was a motion on the floor to suggest that children aged 16 and under should be banned from using ChatGPT and other large language models, or LLMs. I understand this, not just from a children's mental health perspective but from the point of view of teachers in the classroom, who are increasingly frustrated at the amount of cheating that is going on using AI. At the same time, Canada seems to have an economic strategy that wants everybody to use AI.

The last time you and I spoke, it was about Bill C-63 before it died. Can you tell me, from an online harms perspective, what kind of regulatory regime could work? Should we be worried about the constitutional and Charter impacts of banning kids below a certain age from having access to these tools that I loathe?

I know you've thought a lot about online harms, and I wonder if you could speak to that kind of legislative regime.

**Ms. Laidlaw:** Yes, and I invite you to interrupt me if I'm talking for too long.

I am part of the reconvened expert group that is advising on a reformulated version of the online harms legislation, and we will be looking at social media bans.

The challenge right now is that the political will is strongly for social media bans. There's been an enormous amount of pushback, though, on a few fronts, and one of them regards their effectiveness. We're seeing in Australia how easy it is to route around the bans. The question you have to ask is this: Will it actually help achieve the outcome of providing safer spaces for children?

**Senator Simons:** This isn't just for social media. That was one resolution, but the other resolution was specifically about LLMs.

**Ms. Laidlaw:** When it comes to LLMs — and this makes sense after Tumbler Ridge — to my mind, you lump them together. If you want to create safe spaces for kids, are you

vie de nos citoyens, au Canada, aux États-Unis et partout dans le monde. Si nécessaire, nous devons être prêts à prendre des mesures défensives, comme nous le ferions, par exemple, pour des menaces liées aux armes de destruction massive.

**Le sénateur Wilson :** Je vais en rester là. J'aurais peut-être une question à poser pendant la deuxième ronde de questions.

**La sénatrice Simons :** Puisque je ne crois pas à la guerre des machines, ma question s'adresse à Mme Laidlaw.

Au congrès du Parti libéral, cette fin de semaine — auquel je n'ai pas assisté, n'étant pas membre de ce parti —, on a débattu d'une motion visant à interdire l'utilisation de ChatGPT et d'autres grands modèles de langage, les GML, aux enfants de 16 ans et moins. Je comprends cela, non seulement du point de vue de la santé mentale des enfants, mais aussi du point de vue des professeurs dans les salles de classe, de plus en plus irrités par l'utilisation de l'intelligence artificielle pour tricher. Au même moment, la stratégie économique du Canada semble vouloir que tout le monde utilise l'intelligence artificielle.

La dernière fois que nous nous sommes parlé, c'était au sujet du projet de loi C-63, avant qu'il meure. Pourriez-vous me dire, en ce qui concerne les préjudices en ligne, quel type de cadre réglementaire serait efficace? Devrions-nous nous soucier des répercussions au regard de la Constitution et de la Charte, du fait d'interdire aux enfants de moins d'un certain âge d'accéder à ces outils que je déteste?

Je sais que vous avez beaucoup réfléchi aux préjudices en ligne, et je me demandais si vous pouviez nous parler de ce genre de régime législatif.

**Mme Laidlaw :** Oui, et je vous invite à m'interrompre si je parle trop longtemps.

Je fais partie du nouveau groupe d'experts qui donne des avis sur une version reformulée de la loi sur les préjudices en ligne, et nous allons examiner la question de l'interdiction des réseaux sociaux.

Le défi, à l'heure actuelle, c'est que la volonté politique tend fortement vers l'interdiction des médias sociaux. Toutefois, il y a beaucoup de réticence sur quelques fronts, y compris en ce qui concerne l'efficacité. Nous voyons à quel point il est facile de contourner ces interdictions, en Australie. La question que vous devez vous poser est la suivante : est-ce que cela nous aidera réellement à offrir des espaces plus sécuritaires aux enfants?

**La sénatrice Simons :** Ce n'est pas seulement pour les médias sociaux. C'était une résolution, mais l'autre résolution portait précisément sur les GML.

**Mme Laidlaw :** En ce qui concerne les GML — et cela est logique après Tumbler Ridge — à mon avis, vous devez les regrouper. Si vous voulez créer des espaces sécuritaires pour les

creating a kind of ban when it comes to kids' access to social media or chatbots?

In some ways, it can be effective for certain kids under a certain age, when their brains are not developed. It provides them the opportunity to develop naturally without their minds being manipulated before they are ready.

The challenge is that there are also positives for some of these tools. They're used for education. They're used for research. We are using AIs in all kinds of different ways. You want to train them up on how to use them, and you also want them to learn how to use them in a healthy way before they leave the nest.

I have a 17-year-old who is about to fly the coop. I would be horrified if she just got on these at 16, where she hadn't had that opportunity under my roof to learn how to safely use these tools.

The other thing is that if you just ban it without accompanying safety by design, none of us will be better off. There's no point in doing this unless we actually put in place all the safety features that we think should be there — not only to protect kids but also adults — so they have to go together.

I'm not entirely against bans, especially for kids who are under 13 years old, but they don't actually solve that problem, and we also have to think through who might be negatively impacted by this.

**Senator Simons:** I'm thinking about large language models and writing and kids falsifying their essays, but I'm sure there are also kids who are just playing and making talking Chihuahuas — I don't want to say "cat videos" because it's such a cliché — but there are all kinds of games and very childlike things you can do with AI that adults seem to enjoy, and kids do too.

**Ms. Laidlaw:** They are also helping with math tutoring and different forms of education. There are benefits to it.

Should it be heavily controlled for children? Absolutely, but the idea that there should be no access whatsoever can be more challenging.

There's some justification for it maybe being used only in classrooms or only with parents when you're talking about children under 13. It is much more problematic once you get above that age.

**Senator Simons:** Thank you very much.

enfants, est-ce que vous allez leur interdire d'accéder aux médias sociaux ou aux robots conversationnels?

D'une certaine façon, cela peut être efficace pour les enfants de moins d'un certain âge, lorsque leurs cerveaux ne sont pas encore développés. Cela leur permet de se développer naturellement, sans que leur cerveau soit manipulé avant qu'ils ne soient prêts.

Le problème, c'est qu'il y a aussi des avantages, pour certains de ces outils. Ils sont utilisés pour l'enseignement. Ils sont utilisés pour la recherche. Nous utilisons l'intelligence artificielle d'une foule de façons. Vous voulez leur montrer comment les utiliser, comment les utiliser de manière saine, avant qu'ils quittent le nid.

Ma fille de 17 ans s'apprête à partir de la maison. Je serais consternée de savoir qu'elle commence à utiliser ces outils à l'âge de 16 ans seulement, sans avoir eu la chance d'apprendre à les utiliser de manière sécuritaire à la maison.

L'autre chose, c'est que, si nous nous contentons de les interdire, sans y incorporer des mesures de sécurité, cela n'améliore en rien notre situation. Il est inutile de faire cela, si nous ne mettons pas en place les mesures de sécurité que nous croyons être nécessaires — pour protéger non seulement les enfants, mais aussi les adultes —, donc ils doivent aller de pair.

Je ne suis pas totalement opposée aux interdictions, surtout pour les enfants de moins de 13 ans, mais elles ne règlent pas vraiment le problème, et il faut aussi penser aux personnes qui pourraient en subir les conséquences négatives.

**La sénatrice Simons :** Je pense aux grands modèles de langage, à l'écriture et aux enfants qui copient leurs dissertations, mais je suis certaine qu'il y a aussi des enfants qui s'amusent simplement à créer des chihuahuas qui parlent — je ne veux pas dire « vidéos de chat » parce que c'est un véritable cliché —, mais il y a toutes sortes de jeux et d'activités très enfantines que l'on peut faire avec l'intelligence artificielle et qui semblent plaire aux adultes, tout comme aux enfants.

**Mme Laidlaw :** L'intelligence artificielle apporte également de l'aide pour les cours particuliers de mathématiques et dans d'autres formes d'enseignement. Cela présente des avantages.

Faut-il exercer un contrôle strict sur son utilisation par les enfants? Absolument, mais l'idée d'en interdire carrément l'accès peut s'avérer plus difficile à mettre en œuvre.

On peut justifier que son utilisation soit réservée aux salles de classe ou aux parents quand il s'agit d'enfants de moins de 13 ans. Cela devient beaucoup plus problématique dès que l'on dépasse cet âge.

**La sénatrice Simons :** Merci beaucoup.

[*Translation*]

**Senator Aucoin:** Are you able to understand?

**Ms. Laidlaw:** Yes, but I will listen to you in English.

**Senator Aucoin:** Take your time. My first question is for you. I will have a question for Mr. Leahy afterwards. It's like the end of the world is coming; it could be tomorrow. My problem is waiting until we have identified all the problems that AI might pose before creating the act or regulations. On top of that, technology and research are moving so fast that we will never be ahead of the curve. Wouldn't it be better to have a framework already in place to provide some protection, rather than waiting and trying to identify everything? If my suggestion makes sense, could you outline some urgent issues that you think should be prioritized?

**Ms. Laidlaw:** Thank you very much for the question.

[*English*]

I agree that technology will always be ahead of anything that can be done in law. We shouldn't wait to pass legislation or form that framework. We have a gold standard, and that is that idea of risk management.

We have the framework we need to be working with, which is if you are a company and designing AI, you have an obligation to think about safety by design up front and to have a process in place where you assess, monitor, act on problems and have to report back to some sort of oversight body. That standard is there, and I think that the legislation can be written in a way that can evolve as the technology evolves. That's the art form of how it needs to be written, but we have somewhere to start.

[*Translation*]

**Senator Aucoin:** Mr. Leahy, did you want to add anything?

[*English*]

**Mr. Leahy:** I want to fully agree with what my colleague is saying — that action soon is very important. Tech companies are specifically optimizing to be as fast as possible in order to outrun legislation. They are trying to slow down the legislative process so they can get far ahead of without any formalization, which is why it's so important for us to move quickly.

[*Français*]

**Le sénateur Aucoin :** Est-ce que vous êtes en mesure de comprendre?

**Mme Laidlaw :** Oui, mais je vais vous écouter en anglais.

**Le sénateur Aucoin :** Prenez votre temps. Ma première question s'adresse à vous. J'aurai une question pour M. Leahy par la suite. C'est comme la fin du monde qui arrive incessamment; ce pourrait être demain. Mon problème, c'est d'attendre d'avoir identifié tous les problèmes que l'IA peut poser avant de créer la loi ou les règlements; de plus, la technologie et les recherches vont tellement vite qu'on ne sera jamais en avance. Ne serait-il pas préférable d'avoir un régime déjà en place pour protéger jusqu'à un certain point, plutôt que d'attendre et d'essayer de tout identifier? Si ma suggestion est bonne, pourriez-vous répéter certaines choses urgentes qu'il faudrait prioriser, à votre avis?

**Mme Laidlaw :** Merci beaucoup pour la question.

[*Traduction*]

Je suis d'accord pour dire que la technologie aura toujours une longueur d'avance sur tout ce que les lois peuvent faire. Nous ne devrions pas attendre une loi ou un cadre réglementaire. Nous avons une règle d'or, à savoir le concept de gestion du risque.

Nous avons le cadre dont nous avons besoin pour travailler; si vous êtes une entreprise et que vous concevez un système d'intelligence artificielle, vous avez l'obligation de penser à la sécurité dès la conception, de mettre en place un processus pour évaluer, surveiller et traiter les problèmes et de rendre compte à une sorte d'organisme de surveillance. Cette norme existe, et je pense que la loi peut être rédigée de manière à évoluer à mesure que la technologie évolue. C'est tout un art, de la rédiger, mais nous avons un point de départ.

[*Français*]

**Le sénateur Aucoin :** Monsieur Leahy, vous vouliez ajouter quelque chose?

[*Traduction*]

**M. Leahy :** Je partage entièrement l'avis de ma collègue : il est essentiel d'agir sans attendre. Les entreprises technologiques s'efforcent précisément d'accélérer leurs activités au maximum afin de devancer la loi. Elles tentent de ralentir le processus législatif afin d'avoir une longueur d'avance avant même que la réglementation ne soit officialisée; c'est pourquoi il est si important que nous agissions rapidement.

[*Translation*]

**Senator Aucoin:** I'm going to ask you another question. My understanding is that talks are already under way with a consortium that is looking at the possibility of bringing together groups, industries, governments and countries to try to do just that. What worries me is that time is now crucial, because even if we could do that, if we could have these….

There will always be people who will hijack those regulations or policies to do what you said. Can you tell us how we could prevent this from happening? Mr. Leahy, you talked about computers or AI itself, which will make decisions against individuals, governments and society, but there may also be rogue nations or entities that want to go straight to action and control AI so that it controls certain things. What can we do about that?

[*English*]

**Mr. Leahy:** The most important thing is that we must arrest and pause the development of extremely powerful general purpose superintelligence systems. The only levers we have with the necessary force and jurisdiction to speak are law enforcement and the military. This is a national security and international security problem. It's important that there are many economic issues relevant to AI, its applications and safety management. But when it comes to systems that have such military and security implications, this is truly a matter of the national security and international security apparatuses. It should be illegal to attempt to build superintelligence. This should be enforced. There are many ways for one to think about how to enforce this. On the international front, Canada and other countries should make it a priority to create a trust-but-verify regime, where countries commit to not building such technology within their borders, enforce it within their borders and, if necessary, use appropriate sanctions or other means on non-compliant actors.

**The Chair:** Ms. Laidlaw, do you have a comment on that point?

**Ms. Laidlaw:** The only thing I wish to add is that we face an enormous challenge because there needs to be cooperation among countries internationally to play that role. It could only be governments that step in, and they need to coordinate. I don't see that happening across the board. The closest we can come is essentially finding friends, partnerships and relationships with like-minded jurisdictions. Part of the reason I push the risk management approach is the fact that this is what is being

[*Français*]

**Le sénateur Aucoin :** Je vais vous poser une autre question. J'ai cru comprendre qu'il y avait déjà des pourparlers d'un consortium qui examine la possibilité de réunir des groupes, des industries, des gouvernements et des pays pour justement essayer de faire cela. Ce qui m'inquiète, c'est que le temps est maintenant crucial, parce que, même si on pouvait faire cela, si on pouvait avoir ces...

Il y aura toujours des gens qui vont détourner ces règlements ou ces politiques pour faire ce que vous avez dit. Pouvez-vous nous dire comment on pourrait faire en sorte que cela n'arrive pas? Vous avez parlé, monsieur Leahy, des ordinateurs ou de l'IA elle-même, qui va prendre des décisions contre des individus, des gouvernements et la société, mais il se peut aussi qu'il y ait des nations ou des entités voyous voudront passer directement à l'action et contrôler l'IA pour que cette dernière contrôle certaines choses. Qu'est-ce qu'on peut faire par rapport à cela?

[*Traduction*]

**M. Leahy :** Le plus important, c'est que nous devons mettre à l'arrêt et suspendre le développement des systèmes superintelligents à usage général extrêmement puissants. Les seuls leviers que nous avons et qui ont la force et la compétence nécessaires pour agir, ce sont les forces de l'ordre et l'armée. C'est un problème de sécurité nationale et de sécurité internationale. Il est important de noter les nombreux enjeux économiques liés à l'intelligence artificielle, à ses applications et à la gestion de la sécurité. Mais, quand il s'agit de systèmes ayant de telles implications militaires et sécuritaires, c'est véritablement une question relevant des appareils de sécurité nationaux et internationaux. Il devrait être illégal de tenter de construire une superintelligence. Cette interdiction devrait être appliquée. Il y a de nombreuses façons de concevoir des manières de faire respecter cette interdiction. Sur la scène internationale, le Canada et d'autres pays devraient se donner pour priorité de créer un régime « faites confiance, mais vérifiez », selon lequel les pays s'engagent à ne pas développer une telle technologie sur leur territoire, à faire respecter cette interdiction sur leur territoire et, si nécessaire, à recourir à des sanctions appropriées ou à d'autres moyens contre les acteurs qui ne se conforment pas à ces règles.

**Le président :** Madame Laidlaw, aimeriez-vous ajouter quelque chose?

**Mme Laidlaw :** La seule chose que j'aimerais ajouter, c'est que nous sommes confrontés à un défi colossal, car il faut une coopération internationale, entre les pays, pour jouer ce rôle. Seuls les gouvernements peuvent intervenir, et ils doivent se coordonner. Je ne vois pas cela à tous les niveaux. Le mieux que l'on puisse faire est essentiellement de se trouver des alliés, des partenariats et des relations avec des pays qui partagent les mêmes valeurs. Si je prône l'approche de gestion du risque, c'est

developed by other jurisdictions too, and the only way to deal with this on a global level is almost interoperable laws to be able to hold companies accountable.

**The Chair:** Thank you.

**Senator Arnold:** This is somewhat panic-inducing, I have to say. Is there any buy-in anywhere in the world on this?

**Mr. Leahy:** Yes. These issues are mostly bottlenecked, in my experience, through education. I've talked to many lawmakers here in the U.S., on both sides of the aisle and from across the political spectrum, and I can say that, overwhelmingly, the number-one bottleneck is most people have never heard of these problems. It's not that they disagree over this seeming really bad or whether we should do something about it.

Both Democrats and Republicans in the U.K. and my colleagues over in the U.K. have built a coalition of over 100 members of Parliament who are now calling for binding regulations around that. We've done some work in Canada and in Germany. There's a lot of interest in doing something about this. I think it's pretty intuitive why this is a problem that we should be dealing with. If we look at polling numbers around AI in basically any Western country, the numbers are very stark and very cross-partisan. People feel that AI is not currently being regulated properly; they don't want AI that is smarter than humans or that destroys their way of life.

There is a lot of interest. The bottlenecks at the moment are mostly education, knowledge of these issues and forming large enough coalitions to take action.

**Senator Arnold:** Well, that all sounds really interesting, but we have a government and a world right now where there are a lot of complex issues, and this is being sold to us as sort of the saviour for all of those as well. I recently read an article by Matt Shumer entitled "Something Big Is Happening." I don't know if you're familiar with it, but his whole premise was that it's better to be using it all the time, to be aware of it and to learn about it, rather than disengaging from it. I'm wondering what your opinion is on that.

**Mr. Leahy:** Disengagement is not the right solution. For example, I do not advocate for the slowdown of the development of data centres because I think the primary outcome of such a policy would be for power to diffuse outside the Western sphere of influence. If, for example, Canada, the U.S. and other Western

entre autres parce que c'est ce que d'autres pays sont en train de mettre en place, et la seule manière de traiter cette question à l'échelle mondiale est d'avoir des lois quasi interopérables permettant de tenir les entreprises pour responsables.

**Le président :** Merci.

**La sénatrice Arnold :** Je dois dire que cela fait un peu peur. Y a-t-il un endroit au monde prêt à adopter cela?

**M. Leahy :** Oui. D'après mon expérience, ces enjeux se heurtent principalement à des obstacles liés à l'éducation. J'ai discuté avec de nombreux législateurs ici aux États-Unis, des deux partis et de tout le spectre politique, et je peux affirmer que, dans la grande majorité des cas, le principal obstacle tient au fait que la plupart des gens n'ont jamais entendu parler de ces problèmes. Ce n'est pas qu'ils ne s'accordent pas sur le fait que la situation semble vraiment grave ou sur la nécessité d'agir.

Au Royaume-Uni, tant les démocrates que les républicains, ainsi que mes collègues britanniques, ont formé une coalition de plus de 100 députés qui réclament aujourd'hui une réglementation contraignante en la matière. Nous sommes également passés à l'action au Canada et en Allemagne. Les gens veulent vraiment agir dans ce dossier. Je pense que l'on peut comprendre assez intuitivement pourquoi c'est un problème auquel nous devons nous attaquer. Si l'on examine les résultats des enquêtes sur l'intelligence artificielle dans pratiquement tous les pays occidentaux, les chiffres sont très clairs et transcendent les divisions partisanes. Les gens estiment que l'intelligence artificielle n'est pas réglementée correctement à l'heure actuelle; ils ne veulent pas d'une intelligence artificielle plus intelligente que les humains ou qui détruit leur mode de vie.

L'intérêt est grand. Les obstacles actuels sont principalement l'éducation, la connaissance de ces enjeux et la formation de coalitions suffisamment importantes pour passer à l'action.

**La sénatrice Arnold :** Eh bien, tout cela a l'air vraiment intéressant, mais nous vivons actuellement dans un monde où le gouvernement fait face à de nombreux problèmes complexes, et on nous présente cette technologie comme une sorte de solution miracle à tous ces problèmes. J'ai récemment lu un article de Matt Shumer intitulé « Something Big is Happening », titre que je traduirais par « Quelque chose d'important est en train de se produire ». Je ne sais pas si vous le connaissez, mais son argument principal était qu'il vaut mieux l'utiliser tout le temps, en être conscient et s'y intéresser, plutôt que de s'en dissocier. Je me demande quelle est votre opinion à ce sujet.

**M. Leahy :** Le désengagement n'est pas la bonne solution. Par exemple, je ne préconise pas de ralentir le développement des centres de données, car je pense que le principal effet d'une telle politique serait de disperser le pouvoir en dehors de la sphère d'influence occidentale. Si, par exemple, le Canada, les

countries were to stop using AI entirely, these companies would then defect to China and/or rogue nations and simply continue their goal of building a superintelligence system.

It's important to understand these big tech companies act more like geopolitical entities or rogue nation-states. They are not purely economic actors. Their goals are power and control, not just money. A lot of these companies are, to varying degrees, attempting to supplant or undermine government capabilities for their own power.

All this being said, this doesn't solve the problem that these companies also themselves don't control their AIs and are delusionally optimistic about their ability to continue to maintain control over these systems versus the systems disempowering them. This is a pretty classic market failure, where, if there is no regulation, markets tend to vastly underprovision public security and the most reckless actors will be the ones racing forward the most. This is where regulatory and, if necessary, national security interventions are deeply necessary.

**The Chair:** Ms. Laidlaw, any comments to add on that particular point?

**Ms. Laidlaw:** I think I might leave it at that for now. I think Connor is terrifying me as well, and I work in this area. I'll just sit with that for a minute.

**The Chair:** I have to take a blood pressure pill right now.

**Senator Petitclerc:** I might not help with the terrifying part of the question, but I'm curious to hear you on this, Mr. Leahy. Regarding safety mechanisms, we have Geoffrey Hinton thinking about this idea of fostering or developing maternal instinct in AI. What is your take on that? Is it something that makes sense? To me, it's science fiction.

**Mr. Leahy:** I agree, quite frankly. If there's one thing we understand less than AI, it's human emotions and the brain — and something as complex as maternal instinct or the morals behind it. I deeply respect Professor Hinton. He's one of the smartest men alive and truly someone I admire, but I don't see how this is a feasible proposal, at least for the short-term future.

**Senator Petitclerc:** Thank you. I appreciate that.

États-Unis et d'autres pays occidentaux cessaient complètement d'utiliser l'intelligence artificielle, ces entreprises se tourneraient alors vers la Chine ou des États voyous et poursuivraient tout simplement leur objectif de construction d'un système superintelligent.

Il est important de comprendre que ces grandes entreprises technologiques agissent davantage comme des entités géopolitiques ou des États voyous. Elles ne sont pas de simples acteurs économiques. Leurs objectifs sont le pouvoir et le contrôle, pas seulement l'argent. Bon nombre de ces entreprises tentent, à des degrés variables, de supplanter ou de saper les capacités des gouvernements pour asseoir leur propre pouvoir.

Cela dit, cela ne règle pas le problème, car ces entreprises ne contrôlent pas elles-mêmes leur intelligence artificielle et sont d'un optimisme délirant quant à leur capacité à conserver le contrôle sur ces systèmes et d'empêcher que ces systèmes prennent le pouvoir. Il s'agit là d'une déficience classique du marché, où, en l'absence de réglementation, les marchés ont tendance à sous-financer considérablement la sécurité publique et où les acteurs les plus imprudents iront le plus loin. C'est là que des interventions en matière de réglementation et, au besoin, en matière de sécurité nationale, sont absolument indispensables.

**Le président :** Madame Laidlaw, aimeriez-vous ajouter quelque chose à cela?

**Mme Laidlaw :** Je crois que je vais m'arrêter là pour l'instant. Je crois que M. Leahy me fait peur, à moi aussi, alors que je travaille dans le domaine. Je vais juste laisser cette pensée faire son chemin pendant un moment.

**Le président :** J'ai besoin de prendre un comprimé pour la tension artérielle, maintenant.

**La sénatrice Petitclerc :** Je ne vous aiderai probablement pas, étant donné le côté effrayant de la question, mais je suis curieuse d'avoir votre avis à ce sujet, monsieur Leahy. En ce qui concerne les mécanismes de sécurité, Geoffrey Hinton réfléchit à l'idée de favoriser ou de développer l'instinct maternel de l'intelligence artificielle. Qu'en pensez-vous? Est-ce que cela vous semble plausible? Pour moi, cela relève de la science-fiction.

**M. Leahy :** Je suis tout à fait d'accord, pour être franc. S'il y a bien une chose que nous comprenons encore moins que l'intelligence artificielle, ce sont les émotions humaines et le fonctionnement du cerveau, ou un phénomène aussi complexe que l'instinct maternel et la moralité de ce que cela sous-tend. J'ai un profond respect pour M. Hinton. C'est l'un des hommes les plus brillants de notre époque et quelqu'un que j'admire sincèrement, mais je ne vois pas comment cette proposition pourrait être réalisable, du moins à court terme.

**La sénatrice Petitclerc :** Merci. J'apprécie votre réponse.

Ms. Laidlaw, I'm trying to understand what the right balance is in terms of being successful in the AI race but having proper safeguards. A few days ago, we heard that the EU AI Act has more specific obligations, safeguards and protections, but apparently, they are thinking that maybe they need to back off a bit because it blocks how fast they are evolving as a country.

When it comes to AI and, as you mentioned before, the protection, should we use the precautionary principle or just go forward and then try to fix it after?

I worry that it is going to be like social media, where we let it all out. My angle is maybe more around children, but we realized it is very difficult to fix it.

**Ms. Laidlaw:** We don't want Canada to be hamstrung such that our innovation industry isn't able to develop and compete. They talk about trustworthy AI, and Connor was talking about that: Trust but verify. How do we encourage trustworthy and competitive AI and all the wonderful things that it can bring?

Understanding the rules is important. Some of the feedback we're hearing from innovators — I know conversations I have had with different folks — is that they say, "We just want to know what the rules are so that we can be confident." That's good for investors. That's good for businesses. If they want to open up markets with the EU, having laws that are coordinated — at least at a basic level — with the EU is helpful. But we cannot make overly complicated rules. I think that's where they start impacting innovation. It has to be clear what the risk management rules are.

It has to be done up front, though. It has to be precautionary. We cannot just go forth and break things and just retroactively fit in some security measures. We need to think of it more as being like road safety laws. We wouldn't want planes flying without having an understanding of what the basic rules are, and we would not want that with roads either. So let's set out what the rules of the road should be so that there can be some confidence in the industry. I know that's not getting into too much detail. The devil will be in the details with this, but it is a framework.

**Senator Petitclerc:** What about literacy? How are we doing as Canadians when it comes to AI literacy? We have the safeguards, but how about literacy?

Madame Laidlaw, j'essaie de comprendre quel est le juste équilibre entre bien se classer dans la course à l'intelligence artificielle et se doter de garde-fous adéquats. Il y a quelques jours, nous avons appris que la loi européenne sur l'intelligence artificielle prévoyait davantage d'obligations, de mesures de sécurité et de protections précises, mais il semblerait que les décideurs envisagent de faire marche arrière, car cette loi freine l'évolution du pays.

En ce qui concerne l'intelligence artificielle et, comme vous l'avez mentionné précédemment, la protection, devrions-nous appliquer le principe de précaution ou simplement aller de l'avant et essayer de corriger le tir par la suite?

Je crains que cela ne devienne comme les réseaux sociaux, où on laisse tout passer. Je pense peut-être davantage aux enfants, mais nous avons réalisé qu'il est très difficile de régler le problème.

**Mme Laidlaw :** Nous ne voulons pas que le Canada soit paralysé au point que notre secteur de l'innovation ne puisse se développer et être compétitif. On parle d'une intelligence artificielle digne de confiance, et M. Leahy en a justement parlé : « faites confiance, mais vérifiez. » Comment pouvons-nous encourager une intelligence artificielle digne de confiance et compétitive ainsi que toutes les choses formidables qu'elle peut apporter?

Il est important de comprendre les règles. Nous recevons des commentaires des innovateurs — j'ai discuté avec différentes personnes —, par exemple : « Nous voulons seulement connaître les règles pour pouvoir avoir confiance. » C'est une bonne chose pour les investisseurs. C'est une bonne chose pour les entreprises. Si elles souhaitent ouvrir des marchés dans l'Union européenne, il serait utile d'avoir des lois coordonnées — au moins à un niveau de base — avec celles de l'Union européenne. Mais nous ne voulons pas établir des règles trop compliquées. Je pense que c'est là qu'elles commencent à freiner l'innovation. Les règles de gestion du risque doivent être claires.

Mais cela doit être fait dès le départ. Il faut agir avec prudence. On ne peut pas se lancer tête baissée, faire des dégâts, puis adopter des mesures de sécurité a posteriori. Il faut plutôt voir cela comme les règles de sécurité routière. On ne voudrait pas que les avions volent sans que personne comprenne les règles de base, et on ne voudrait pas non plus que cela se passe ainsi sur les routes. Définissons alors les règles de la route pour qu'il y ait une certaine confiance dans le secteur. Je sais que cela n'entre pas trop dans les détails. Le problème tient à des détails, mais c'est un cadre.

**La sénatrice Petitclerc :** Qu'en est-il de la littératie? Où en sommes-nous, en tant que Canadiens, en matière de connaissance de l'intelligence artificielle? Nous avons des mesures de protection, mais qu'en est-il de la littératie?

**Ms. Laidlaw:** That is a wonderful question, and that is just as critical as regulation.

We need literacy. We need to be training our youth. We need to be going into old folks' homes and training our parents. We are not doing enough there. I think it is being left to teachers. It is being left to smaller non-profits. It needs to be a whole-of-government push.

In some other areas, such as online harms — where I do a lot of work — you can look to the eSafety Commissioner in Australia. She has a huge education role. She has a huge literacy mandate. That needs to be at the forefront of what we do, and some of these regulatory bodies can be the key ones doing that. The Canadian Centre for Cyber Security is built out. In any case, that would be the approach I would suggest.

**Senator Miville-Dechêne:** Hello again, Ms. Laidlaw. You will not be surprised that I will ask you about children, but in the context of AI chatbots. We had Minister Solomon come to the Senate the other day, and he was asked questions about chatbots. This is AI, but this is also a tool that can incite kids to suicide. There was a report in Quebec of a teenager who was sexually assaulting imaginary people — obviously not real people, but they were letting him do all kinds of stuff on this chatbot thing.

You said, "Let's not control it if they are over 13," but what about that? What are your thoughts?

**Ms. Laidlaw:** I'm glad that you asked that question because I think the proper place for this is online harms legislation. We actually talked about chatbots at our meeting on Monday. I will tell you my view.

Some of the forms of harm that have happened to children are horrifying. Also, vulnerable adults have been prompted to psychotic breaks and so on from using some of these chatbots.

Yes, you could explore the idea of banning it for kids that are especially vulnerable and young, but it should be under online harms legislation because there should be safety by design. They should have special duties of responsibility to take certain steps to make sure that they have thought through how they have structured it. Are there certain safety features for children? Do you have certain mechanisms in place to flag problematic content, and what do you do when it lands on your desk?

**Mme Laidlaw :** C'est une question formidable, et c'est tout aussi important que la réglementation.

Nous avons besoin de littératie. Nous devons former nos jeunes. Nous devons nous rendre dans les maisons de retraite et former nos parents. Nous n'en faisons pas assez dans ce domaine. Je pense que cette tâche est laissée aux enseignants. Elle est laissée à de petits organismes à but non lucratif. Cela devrait être une initiative à l'échelle du gouvernement.

Dans d'autres domaines, comme les préjudices en ligne — sujet sur lequel je travaille beaucoup —, on peut s'inspirer de la commissaire à la sécurité électronique de l'Australie. Elle joue un rôle éducatif considérable. Elle a un mandat très large en matière de littératie. Cela doit être au cœur de tout ce que nous faisons, et certains organismes de réglementation peuvent jouer un rôle clé à cet égard. Le Centre canadien pour la cybersécurité est opérationnel. Quoi qu'il en soit, c'est l'approche que je suggérerais.

**La sénatrice Miville-Dechêne :** Rebonjour, madame Laidlaw. Vous ne serez pas surprise que je vous pose des questions sur les enfants, mais dans le contexte des robots conversationnels alimentés par l'intelligence artificielle. Le ministre Solomon s'est présenté devant le Sénat l'autre jour, et on lui a posé des questions sur les robots conversationnels. Il s'agit d'intelligence artificielle, mais c'est aussi un outil qui peut pousser des enfants au suicide. Au Québec, on a rapporté le cas d'un adolescent qui agressait sexuellement des personnes imaginaires, évidemment pas de vraies personnes, mais on le laissait faire toutes sortes de choses sur ce robot conversationnel.

Vous avez dit : « Ne contrôlons pas cela s'ils ont plus de 13 ans », mais qu'en est-il de ce cas-là? Qu'en pensez-vous?

**Mme Laidlaw :** Je suis contente que vous posiez la question, car je pense que c'est dans le cadre de la loi sur les préjudices en ligne qu'il convient d'aborder le sujet. Nous avons d'ailleurs parlé des robots conversationnels pendant notre réunion de lundi. Je vais vous exposer mon point de vue.

Certains des préjudices subis par les enfants sont effroyables. De plus, l'utilisation de certains de ces robots conversationnels a déclenché chez des adultes vulnérables des crises psychotiques, entre autres.

Oui, on pourrait envisager de les interdire pour les enfants, particulièrement les enfants vulnérables et jeunes, mais cela devrait relever de la loi sur les préjudices en ligne, car la sécurité doit être intégrée dès la conception. Les créateurs devraient avoir des obligations spécifiques à respecter et prendre des mesures précises pour confirmer qu'ils ont bien réfléchi à la manière dont ils ont structuré le système. Existe-t-il des mesures de sécurité pour les enfants? Ont-ils mis en place des mécanismes pour signaler les contenus problématiques, et que font-ils quand les signalements atterrissent sur leur bureau?

We have all watched the tragedy of Tumbler Ridge and had questions about how that process flowed.

I would say this is not just general AI. Because this is about tech-facilitated harm, this should be under the umbrella of online harms, and, absolutely, it should be regulated.

**Senator Miville-Dechêne:** Should it be age verification or age estimation? Are you not there yet?

**Ms. Laidlaw:** Isn't that the big question? If we say that you are going to ban social media —

**Senator Miville-Dechêne:** Right.

**Ms. Laidlaw:** You are ahead of your time, senator.

If you are going to introduce the idea of banning any social media or chatbots, then you are immediately introducing age verification. I am going to flag that again. We need to be very careful about ensuring the best privacy and cybersecurity standards are being used. In some cases, it might be appropriate to first start with the idea of age estimation.

I had a conversation with OnlyFans a few months ago, and they said they use many layers of age verification because they do not want this available for those under 18.

I wouldn't say they are perfect. I would say the tech is evolving. But that is the conversation we have to have: How are they going to age verify? If we are going to say we're banning it for chatbots, what will that look like?

These are intimate. Chatbots are far more intimate than —

**Senator Miville-Dechêne:** On Australia, you were critical of their first steps and banning social media. This is a work in progress.

**Ms. Laidlaw:** Yes, 100%.

**Senator Miville-Dechêne:** You cannot ask for a system to be without flaws. Yes, there will be people circumventing it. Yes, there will be young people. But the idea is to reduce the harm, isn't it?

**Ms. Laidlaw:** I agree. I have always been critical of the idea that unless it is perfect, we should not do it in this area.

**Senator Miville-Dechêne:** I have dealt with that idea a lot.

Nous avons tous suivi la tragédie de Tumbler Ridge et nous nous sommes interrogés sur le déroulement de ce processus.

Je dirais qu'il ne s'agit pas simplement d'intelligence artificielle générale. Comme il s'agit de préjudices facilités par la technologie, cela devrait relever de la loi sur les préjudices en ligne, et, bien sûr, être réglementé.

**La sénatrice Miville-Dechêne :** Faudrait-il vérifier ou estimer l'âge? Où en êtes-vous dans ce dossier?

**Mme Laidlaw :** N'est-ce pas là la grande question? Si on dit que l'on va interdire les réseaux sociaux...

**La sénatrice Miville-Dechêne :** Oui.

**Mme Laidlaw :** Vous êtes en avance sur votre temps, sénatrice.

Si vous envisagez d'interdire les réseaux sociaux ou les robots conversationnels, cela implique automatiquement la mise en place d'une vérification de l'âge. Je tiens à le souligner encore une fois. Nous devons veiller avec le plus grand soin à ce que les meilleures normes en matière de protection d'enseignement privé et de cybersécurité soient appliquées. Dans certains cas, il pourrait être judicieux de commencer par une estimation de l'âge.

J'ai eu une discussion avec des responsables d'OnlyFans, il y a quelques mois, et ils m'ont dit qu'ils utilisaient plusieurs niveaux de vérification de l'âge, car ils ne veulent pas que leur service soit accessible aux moins de 18 ans.

Je ne dirais pas que leur système est parfait. Je dirais plutôt que la technologie évolue. Mais c'est la discussion que nous devons avoir; comment vont-ils faire pour vérifier l'âge? Si nous décidons de l'interdire pour les robots conversationnels, à quoi cela ressemblera-t-il?

Ce sont des sujets sensibles. Les robots conversationnels sont bien plus intimes que...

**La sénatrice Miville-Dechêne :** En ce qui concerne l'Australie, vous avez critiqué ses premières mesures et son interdiction des réseaux sociaux. C'est un processus en cours.

**Mme Laidlaw :** Oui, tout à fait.

**La sénatrice Miville-Dechêne :** On ne peut pas s'attendre à ce qu'un système soit parfait. Oui, il y aura toujours des gens pour le contourner. Oui, il y aura toujours des jeunes. Mais l'objectif, c'est bien de réduire les risques, n'est-ce pas?

**Mme Laidlaw :** Je suis d'accord. J'ai toujours critiqué l'idée selon laquelle, dans ce domaine, il ne faut rien faire tant que ce n'est pas parfait.

**La sénatrice Miville-Dechêne :** Cette idée m'a tenue bien occupée.

**Ms. Laidlaw:** Yes. Canada can learn lessons here. We can learn lessons from what is happening in Australia to make it better. We can learn lessons from Europe's efforts to deploy the AI Act. We're at a moment in time that we can maybe —

**Mme Laidlaw :** Oui. Le Canada a des leçons à en tirer. Nous pouvons nous inspirer de ce qui se passe en Australie pour améliorer les choses. Nous pouvons tirer des enseignements des efforts déployés par l'Europe pour mettre en œuvre la loi sur l'intelligence artificielle. Nous sommes arrivés à un moment où nous pourrions peut-être...

**Senator Miville-Dechêne:** Especially since we are so late in the game, we can learn lessons. It is the only positive thing about being late.

**La sénatrice Miville-Dechêne :** D'autant plus que nous sommes déjà bien en retard, nous pouvons en tirer des leçons. C'est le seul aspect positif de ce retard.

**Ms. Laidlaw:** Yes.

**Mme Laidlaw :** Oui.

**Senator Simons:** I want to come back to Professor Laidlaw because one of your other areas of expertise that we haven't dealt with tonight is copyright.

**La sénatrice Simons :** Je voudrais revenir à Mme Laidlaw, car l'un de vos autres domaines d'expertise dont nous n'avons pas encore parlé ce soir est le droit d'auteur.

Copyright is something that, having myself been a professional writer for a long time, concerns me. A lot of these things crawl through the internet, and they train on what is already publicly available. But there have been all kinds of obvious instances where authorial copyright has been grotesquely violated. How do we need to change our copyright laws to protect writers, composers and artists from having their products stolen and repackaged?

Le droit d'auteur est un sujet qui, pour avoir moi-même été écrivaine professionnelle pendant longtemps, me préoccupe. Beaucoup de contenus circulent sur Internet, et la formation s'inspire de ce qui est déjà accessible au public. Mais il y a eu toutes sortes de cas flagrants où le droit d'auteur a été ridiculement bafoué. Que devons-nous modifier dans nos lois sur le droit d'auteur pour protéger les écrivains, les compositeurs et les artistes contre le vol et la réutilisation de leurs œuvres?

**Ms. Laidlaw:** I will say up front that I have moved away from copyright in recent years, so I may not be the best person to be answering all these questions. I think Brent Arnold — he is looking away, saying, "No, do not ask me." Michael Geist, of course, can answer some of these questions.

**Mme Laidlaw :** Je tiens à préciser d'emblée que je me suis éloignée du domaine du droit d'auteur ces dernières années, je ne suis donc peut-être pas la mieux placée pour répondre à ces questions. Je pense à M. Arnold — il détourne le regard pour dire « non, ne me posez pas la question ». M. Geist, bien sûr, peut répondre à certaines de ces questions.

We are dealing with the same mechanism, though, of scraping and using the creative works of individuals without their consent and then repackaging it in a different way.

Nous avons toutefois affaire au même mécanisme, qui consiste à récupérer et à utiliser les œuvres de création des gens, sans leur consentement, puis à les présenter d'une manière différente.

Do we operate on the basis that some of this is public knowledge and that this is essentially independent, new creative work that comes out of it? In some cases, there needs to be consent to be able to use some of these works. But I don't have a good answer about how, right now, we navigate that. I know that is unsatisfying because this is one of the key issues.

Partons-nous du principe que certaines de ces œuvres appartiennent au domaine public et que ce sont essentiellement des œuvres de création nouvelles et indépendantes qui en sont tirées? Dans certains cas, il faut obtenir un consentement pour utiliser certaines de ces œuvres. Mais je n'ai pas de réponse satisfaisante quant à la manière dont nous devons gérer cela, pour l'instant. Je sais que c'est insatisfaisant, car c'est l'un des enjeux majeurs.

**Senator Simons:** It is also a question of compensation, right? I'm not an artist, so we are imagining a hypothetical scenario. However, if I create an image, and it is suddenly repurposed and used for something else and I have no control over that, should there be compensation for me? Should there be compensation in general? You know I was not a fan of Bill C-18, but should there be some kind of fund that these companies have to set up to either, I don't know, provide scholarships or subsidies to artists or some other way that is a corollary for the theft of intellectual property?

**La sénatrice Simons :** C'est aussi une question de rémunération, n'est-ce pas? Je ne suis pas artiste, donc nous imaginons un scénario hypothétique. Cependant, si je crée une image et qu'elle est soudainement réutilisée à d'autres fins, sans que je puisse y faire quoi que ce soit, devrais-je recevoir une compensation? Devrait-il y avoir une compensation en général? Vous savez que je n'étais pas en faveur du projet de loi C-18, mais faudrait-il que ces entreprises créent une sorte de fonds pour, je ne sais pas, offrir des bourses ou des subventions aux artistes ou compenser d'une autre façon le vol de propriété intellectuelle?

**Ms. Laidlaw:** That may be the direction that it will need to go. It is almost like the blank tapes again, that idea that you are going to create some sort of basic compensation scheme.

There is also, though, a deeper issue. Think of music and discussions about how I could — and I have done this — create a song that sounds like Taylor Swift mixed with James Taylor, or some very odd combination, and see what it comes up with. So you are drawing from the inspiration of certain stylistic factors, which have always been debatable in the area of copyright, where there is this idea around artistry and at what point it becomes copying.

There are some lines here — there is the compensation question, but there is also this question: What is copying if you are generating something new that is based on this pool of ideas and art?

**Senator Simons:** If it is derivative or if it is satirical or if it is a creative — in the music industry, people have been sampling as part of their music for a while. It is a whole genre. But even then, when something is out of copyright, you have to pay some kind of compensation.

**Ms. Laidlaw:** You have to pay some compensation, yes.

**The Chair:** Mr. Leahy, do you have any comments on the copyright?

**Mr. Leahy:** Unfortunately, I am not an expert on this topic, but I think it is a very important one. There is a deep question to be asked: What do we want the role of human creativity to be in our society? However, I am not enough of a philosopher to be able to answer this question, I'm afraid. But I hope someone is.

**The Chair:** Thank you. Do we have anybody up for round two?

**Senator Aucoin:** This question is for both of you. What are your thoughts around creating a group of university professors and industry and government in each country? Could that help to eventually create a group representing all these countries so that there is more research and cooperation?

**Mr. Leahy:** I think there is a lot of work to be done in terms of having intergovernmental, interindustry, interacademic fora about these topics. I'm not an expert on what, exactly, the correct forum would be, but having more contact between government and actual people in both industry and academia especially is extremely valuable and something that I could only support.

**Mme Laidlaw :** C'est peut-être la voie qu'il faudra suivre. C'est un peu comme pour les cassettes vierges, à l'époque, l'idée est de mettre en place une sorte de système de rémunération de base.

Il y a cependant une question plus profonde. Pensons à la musique et aux discussions quant au fait que je pourrais — et je l'ai fait — créer une chanson qui sonne comme un mélange de Taylor Swift et de James Taylor, ou une combinaison très étrange, pour voir ce que cela donne. On puise donc son inspiration dans certains éléments stylistiques, et cela a toujours suscité un débat dans le milieu du droit d'auteur, où l'on s'interroge sur la notion d'art et sur le moment où cela devient de la copie.

Il y a ici certaines limites; il y a la question de la rémunération, mais il y a aussi cette question : qu'est-ce que la copie si l'on génère quelque chose de nouveau à partir de ce réservoir d'idées et d'art?

**La sénatrice Simons :** Qu'il s'agisse d'une œuvre dérivée, d'une œuvre satirique ou d'une création originale, dans l'industrie musicale, on utilise depuis longtemps des reprises dans les morceaux. C'est un genre à part entière. Mais, même dans ce cas, quand une œuvre n'est plus protégée par le droit d'auteur, il faut verser une forme de rémunération.

**Mme Laidlaw :** Oui, vous devez verser une rémunération.

**Le président :** Monsieur Leahy, aimeriez-vous ajouter quelque chose au sujet du droit d'auteur?

**M. Leahy :** Je ne suis malheureusement pas un expert en la matière, mais je pense que c'est un sujet très important. Une question fondamentale se pose : quel rôle souhaitons-nous que la créativité humaine joue dans notre société? Je crains toutefois ne pas être assez philosophe pour pouvoir y répondre. Mais j'espère que quelqu'un d'autre le pourra.

**Le président :** Merci. Quelqu'un aimerait-il commencer le deuxième tour?

**Le sénateur Aucoin :** Ma question s'adresse à vous deux. Que pensez-vous de la création d'un groupe réunissant des professeurs d'université et des représentants du secteur privé et des pouvoirs publics dans chaque pays? Cela pourrait-il contribuer, à terme, à la création d'un groupe représentant tous ces pays, afin de favoriser la recherche et la coopération?

**M. Leahy :** Je pense qu'il y a beaucoup à faire pour mettre en place des forums pour ces discussions intergouvernementales, intersectorielles et interuniversitaires sur ces sujets. Je ne suis pas un expert et je ne sais pas exactement quelle serait la forme idéale de ces forums, mais le renforcement des liens entre les pouvoirs publics et les acteurs du secteur privé comme du milieu universitaire serait très précieux, et c'est une initiative que je ne peux qu'encourager.

**Ms. Laidlaw:** I am for it. The first version of this would be the Internet Governance Forum, which I have been part of off and on. It was recognized that the internet was global and that we needed to bring together stakeholders from industry, academia and government with civil society, all in one place, to kind of debate ideas and develop standards. AI discussions are sort of filtering into that particular space.

The lawyer in me has always found it difficult because I don't see hard outcomes coming from that. It is not designed for that. It is designed for discussions. So I would perhaps recommend something that is smaller, bringing together these groups, because that sort of morphed over time to just almost become this large dialogue, when we need the right people in the room to be talking about what these shared standards are.

Where I think there could be a hiccup, though, is with industry at that table. There are many there wanting to talk about the innovations that they are doing and care deeply about sharing that knowledge. There are also some that are really looking to scale quickly. You need them at that table, and they may not necessarily be there in the way that you would want. That's me talking delicately.

**The Chair:** Thank you for speaking delicately. On that last note, we have finished the first session with our first group. We would like to thank you both, Mr. Leahy and Ms. Laidlaw, for your outstanding testimony.

Our next panel will be, from OpenMedia, Matt Hatfield, Executive Director; from the Canadian Internet Society, Brent Arnold, Chair; and Jared Moore, PhD student at Stanford University. Others are accompanying these witnesses: Desmond Ong, Assistant Professor of Psychology at the University of Texas at Austin, who is with us virtually. We also have Dr. Eric Lin, Psychiatrist at Stanford University. Thank you all for joining us today.

Matt Hatfield will open, followed by Brent Arnold and Jared Moore. You will each have five minutes for your opening remarks. If there is any need for Desmond Ong and Dr. Eric Lin to answer questions witnesses may have challenges with, they will be available.

**Matthew Hatfield, Executive Director, OpenMedia:** Good evening. I'm Matt Hatfield, Executive Director of OpenMedia, a grassroots community of 230,000 Canadians working together for an open, accessible and surveillance-free internet. I'm joining you from the unceded land of the Stó:lo, Tsleil-Waututh, Squamish and Musqueam Nations in Vancouver, B.C.

**Mme Laidlaw :** J'y suis favorable. La première version de ce concept serait le Forum sur la gouvernance de l'Internet, auquel j'ai participé de manière intermittente. On avait alors pris conscience que l'Internet était un phénomène mondial et qu'il fallait réunir en un même lieu les acteurs du secteur privé, du milieu universitaire et des pouvoirs publics, ainsi que la société civile, afin de débattre des idées et d'élaborer des normes. Les discussions sur l'intelligence artificielle commencent peu à peu à s'inscrire dans ce cadre.

L'avocate en moi a toujours trouvé cela difficile, car je ne vois pas de résultats concrets en découler. Ce n'est pas conçu pour cela. C'est conçu pour les discussions. Je recommanderais donc peut-être quelque chose de plus modeste pour réunir ces groupes, car cela a évolué au fil du temps pour devenir presque un vaste dialogue, alors que nous avons besoin que les bonnes personnes soient présentes pour discuter des normes communes.

Là où je pense qu'il pourrait y avoir un accroc, cependant, c'est avec les représentants de l'industrie autour de la table. Beaucoup parmi eux souhaitent parler des innovations qu'ils mettent en œuvre et tiennent profondément à partager ce savoir. D'autres cherchent vraiment à se développer rapidement. Vous avez besoin d'eux à la table, mais ils ne seront peut-être pas là autant que vous le souhaiteriez. J'essaie de rester diplomate.

**Le président :** Merci d'avoir abordé le sujet avec tact. Sur cette note, nous avons terminé la première réunion avec notre premier groupe. Nous tenons à vous remercier tous les deux, monsieur Leahy et madame Laidlaw, pour vos témoignages remarquables.

Notre prochain groupe de témoins comprend M. Matt Hatfield, directeur exécutif de OpenMedia; M. Brent Arnold, président de la Société Internet du Canada; et M. Jared Moore, doctorant de l'Université Stanford. Ces témoins sont accompagnés par M. Desmond Ong, professeur adjoint de psychologie à l'Université du Texas à Austin, qui se joint à nous virtuellement; et par le Dr Eric Lin, psychiatre de l'Université Stanford. Merci à tous de vous joindre à nous aujourd'hui.

M. Hatfield aura la parole en premier, puis ce sera au tour de M. Arnold et de M. Moore. Vous disposerez chacun de cinq minutes pour votre déclaration liminaire. Si M. Ong et le Dr Eric Lin doivent répondre à des questions auxquelles les témoins auraient des difficultés à répondre, ils seront à votre disposition.

**Matthew Hatfield, directeur exécutif, OpenMedia :** Bonsoir. Je suis Matt Hatfield, le directeur exécutif d'OpenMedia, une initiative communautaire composée de 230 000 Canadiens travaillant de concert pour un Internet accessible, ouvert et dépourvu de surveillance. Je me joins à vous depuis les territoires non cédés des nations Musqueam, Squamish, Tsleil-Waututh et Stó:lo de Vancouver, en Colombie-Britannique.

AI will destroy our democracy unless we build systems that can stand up to it.

I will pause for a second because I listened to the last panel and know where the room is at. I'm not telling this to scare you without an actionable solution. I'm saying it because there is a lot Canada can do about it right now.

My version of this argument does not depend on whether you believe in AI's existential risks. It is that the AI we have today, once widely used in predictable ways, will overwhelm democratic systems we depend on to make our government work. To stop that happening, we need to fortify Canada's governance and communications systems, starting now.

Last year, researchers at SEO firm Graphite estimated that 52% of new internet content was being created by AI, up from less than 10% before ChatGPT, but this is just the beginning. As AI agents become cheaper and more capable, the human part of the internet will shrink and shrink. It's being called the "dead internet," a world where almost everything online is bots talking to bots.

What does that mean for our ability to run a human-driven democracy? Many of you probably first learned of OpenMedia when your office got an email from an ordinary Canadian participating in one of our campaigns. We provide form letters as a starting point. Some people send them as written, many add their own thoughts and some delete the whole thing and tell you we have it completely wrong.

For us, all of this is a meaningful pulse check, one of the key ways our system receives the heartbeat of the public between elections.

AI agents are poised to sweep all of this away. Look at Minister Solomon's deeply flawed consultation on AI: His office reported 11,300 responses but requested no identifying details about participants. We have no idea how many were real Canadians, legitimate organizations or AI agents working for whomever programmed them, and that was just half of this consultation's democratic deficit. His office then condensed all the feedback using AI tools. Was a single word written by a Canadian read by any human in our government? We simply don't know.

L'intelligence artificielle va détruire notre démocratie, à moins que nous ne bâtissions des systèmes capables d'y résister.

Je vais m'arrêter pendant une seconde, car j'ai écouté le dernier groupe de témoins, et je sais où ils en sont rendus. Je ne vous dis pas cela pour vous effrayer sans vous donner une solution réalisable. Je vous le dis, car il y a beaucoup que le Canada peut faire aujourd'hui afin de s'y préparer.

Ma version de cet argument ne repose pas sur le fait que vous croyiez ou non au risque existentiel que pose l'intelligence artificielle. Je pense que l'intelligence artificielle d'aujourd'hui, une fois qu'elle est grandement utilisée de façons prévisibles, va submerger les systèmes démocratiques dont dépend le fonctionnement de notre gouvernement. Pour empêcher cela, nous devons consolider la gouvernance du Canada et les systèmes de communication, à partir de maintenant.

L'année dernière, des chercheurs de l'entreprise d'optimisation pour les moteurs de recherche, Graphite, a estimé que 52 % des nouveaux contenus sur Internet étaient générés par l'intelligence artificielle, contre moins de 10 % avant ChatGPT, mais ce n'est que le début. Au fur et à mesure que les agents d'intelligence artificielle coûtent de moins en moins cher et deviennent de plus en plus capables, la partie humaine d'Internet va diminuer encore et encore. C'est ce que l'on appelle l' « Internet mort », un monde où presque tout ce qui est en ligne est un robot qui parle à d'autres robots.

Qu'est-ce que cela signifie pour ce qui est de notre capacité de gérer une démocratie menée par l'humain? Bon nombre d'entre vous ont probablement entendu parler d'OpenMedia pour la première fois lorsque votre bureau a reçu un courriel de la part d'un Canadien ordinaire qui participait à l'une de nos campagnes. Nous fournissons des lettres types comme point de départ. Certaines personnes les envoient telles quelles, beaucoup y ajoutent leurs propres pensées, et certaines suppriment toute la lettre en vous disant que vous avez tort sur toute la ligne.

Pour nous, tous ces procédés sont une façon efficace de prendre le pouls de la population, et l'une des façons essentielles par lesquelles notre système se renseigne sur l'opinion du public entre les élections.

Les agents d'intelligence artificielle sont conçus pour faire disparaître tous ces éléments. Regardez la consultation sur l'intelligence artificielle profondément viciée du ministre Solomon : son cabinet a signalé avoir reçu 11 300 réponses, mais n'a demandé aucun détail permettant d'identifier les participants. Nous n'avons aucune idée du nombre de participants qui étaient de véritables Canadiens, des organisations légitimes ou des agents d'intelligence artificielle travaillant pour quiconque les a programmés, et comptait simplement pour la moitié du déficit démocratique de cette consultation. Son cabinet a ensuite condensé toute la rétroaction en utilisant des outils de l'intelligence artificielle. Est-ce qu'un seul mot écrit par un

That's the future we're barrelling toward, one where, formally, democracy keeps trucking but citizens aren't participating in any meaningful sense and the government isn't listening in any meaningful sense. Procedural legitimacy is maintained; actual democracy is hollowed out.

I highly recommend the book your previous witness Nathan Sanders co-authored with Bruce Schneier, *Rewiring Democracy*. They argue AI can be an ally for democracy. I want to make the converse point: Without action, AI will be enormously destructive to it. Initially, as a denial of service attack, AI will flood voters and government alike with plausible-seeming false content until meaningful choice becomes impossible. Then, as AI grows more sophisticated, something more virus-like, it will probe obscure corners of our laws and regulations to undermine legislative intent.

I have four real recommendations for you to harden our democracy today. First, Canada should create a purpose-built civic engagement tool, one that verifies you're a real Canadian resident without harvesting your data, makes it easy to follow and engage government consultations and gives our government a tamper-proof record of public input. Estonia has led the way here; Canada should follow.

Second, we need an authentication system for fact-based journalism. Give news organizations, libraries and platforms a way to cryptographically verify that content originated from a known, accountable source and hasn't been altered — a postmark and a seal of authenticity combined. This is not a government stamp of approval on content; it's a verifiable record of origin and chain of custody. The CBC, the *Globe*, a community newspaper in Sudbury — all of them could sign their journalism in this way to enhance public trust.

Third, we need legislation demanding algorithmic transparency from platforms and giving Canadians real choice over the algorithms shaping our media diet.

Fourth, our government needs to get serious about reform of data handling and public transparency. Up until now, public data that is hard to access, delayed or incomplete has often been an asset to parts of government. It has dampened people noticing

Canadien a été lu par un être humain quelconque au sein de notre gouvernement? Nous l'ignorons complètement.

C'est l'avenir dans lequel nous fonçons tout droit, un avenir où, officiellement, la démocratie poursuit son petit bonhomme de chemin, mais où les citoyens ne participent d'aucune manière significative, et où le gouvernement n'écoute d'aucune manière significative. La légitimité procédurale est maintenue; la démocratie actuelle est éviscérée.

Je recommande fortement le livre que votre témoin précédent, Nathan Sanders, a coécrit avec Bruce Schneier, *Rewiring Democracy*. Ils expliquent que l'intelligence artificielle peut être un allié pour la démocratie. Je souhaite apporter un contre-argument : si nous n'agissons pas, l'intelligence artificielle sera très destructrice pour la démocratie. Au départ, comme une attaque par déni de service, l'intelligence artificielle va inonder autant le gouvernement que les électeurs avec du contenu faux à l'aspect plausible, jusqu'à ce qu'il soit impossible de faire un choix efficace. Ensuite, à mesure que l'intelligence artificielle devient de plus en plus perfectionnée, quelque chose qui s'apparente davantage à un virus, elle va parcourir les coins sombres de nos lois et règlements afin de miner l'intention législative.

J'ai quatre recommandations concrètes à vous donner afin de consolider notre démocratie aujourd'hui. La première, c'est que le Canada élabore un outil d'engagement civique construit à cette fin, qui vérifie si vous êtes un véritable résident canadien, sans récolter vos données, et cela permettrait de faciliter le suivi et la tenue de consultations gouvernementales, et donnerait à notre gouvernement une trace inviolable de la participation de la population. L'Estonie a pris les devants à ce chapitre; le Canada devrait suivre l'exemple.

Je recommande, en deuxième lieu, de mettre sur pied un système d'authentification du journalisme factuel, pour donner aux organismes de presse, aux bibliothèques et aux plateformes une façon de vérifier par chiffrement que le contenu émanant d'une source connue et responsable n'a pas été altéré… un cachet et un sceau d'authenticité. Il ne s'agit pas d'un sceau d'approbation gouvernemental du contenu; c'est un document vérifiable de l'origine et de la chaîne de possession. CBC/Radio-Canada, le *Globe*, un journal communautaire à Sudbury… Tous ces organismes pourraient signer leur journalisme de cette façon afin d'améliorer la confiance du public.

Je recommande, en troisième lieu, d'élaborer un projet de loi qui exige une transparence algorithmique des plateformes et qui fournit aux Canadiens un véritable choix concernant les algorithmes qui façonnent le contenu médiatique que nous consommons.

Quatrièmement, notre gouvernement a sérieusement besoin de songer à une réforme concernant la manipulation des données et la transparence publique. Jusqu'à ce jour, les données publiques retardées, incomplètes ou difficiles d'accès ont toujours constitué

truths that whoever is in power finds inconvenient. However, moving forward, when government information is not credible, AI disinformation that appears more complete and more honest will rapidly fill the gap. Mandatory proactive disclosure of government contracts and consultations in machine-readable formats, and access to information systems that deliver useful results in a reasonable time span, are no longer just good governance — they will be necessary to prove to people that anything our government says is true.

The dead internet is coming whether we like it or not, but a human-centred digital democracy that will flourish inside it can be built if Canada starts acting today.

Thank you, and I look forward to your questions.

**The Chair:** Thank you very much, Mr. Hatfield.

**Brent Arnold, Chair, Canadian Internet Society:** Thank you, Mr. Chair and honourable senators, for the opportunity to appear as Chair of the Canadian Internet Society. The Canadian Internet Society advocates for open, accessible, affordable and secure internet access for all Canadians. Our focus is to bridge the digital divide by ensuring all Canadians reap the socio-economic benefits the internet provides.

If I can, I will step aside parenthetically and say the following: It is a volunteer organization, so this is not my day job. It has a board and policy committee that include some of your favourite testifying lawyers, including Professor Laidlaw, Michael Geist and David Fraser. That's who sends me here with my marching orders.

In my day job, I'm a cybersecurity and technology lawyer, which means I use artificial intelligence every day in my day job. I tell clients how to use it and deploy it safely, and I help repel cyberattacks that are weaponizing AI to greatly increase the efficiency of cybercrime. That might help you formulate the questions you want to send my way.

I intend to address the three issues this committee has identified for these hearings: the application of AI and content creation, distribution and processing; implications for copyright and intellectual property; and the rise of AI-generated disinformation, misinformation and "deepfakes."

un atout pour certaines parties du gouvernement. Cela a empêché les gens de découvrir des vérités gênantes pour quiconque au pouvoir. Cependant, à l'avenir, lorsque les informations émanant du gouvernement ne seront pas crédibles, la désinformation de l'intelligence artificielle, qui paraît plus complète et plus honnête, va rapidement combler le fossé. La divulgation proactive obligatoire des contrats gouvernementaux, les consultations présentées dans des formats lisibles par la machine, et l'accès à des systèmes d'information qui livrent des résultats utiles dans un délai raisonnable ne constituent plus simplement de la bonne gouvernance; ils seront nécessaires pour prouver que tout ce que le gouvernement dit est véridique.

L'Internet mort arrive, que nous le voulions ou non, mais une démocratie numérique centrée sur l'humain, susceptible de prospérer dans cet Internet, peut être bâtie si le Canada commence à agir aujourd'hui.

Merci, j'ai hâte de répondre à vos questions.

**Le président :** Merci beaucoup, monsieur Hatfield.

**Brent Arnold, président, Société Internet du Canada :** Merci, monsieur le président, et honorables sénateurs de me donner l'occasion de comparaître comme président de la Société Internet du Canada. La Société Internet du Canada se bat pour un accès à Internet sécurisé, abordable, accessible et ouvert pour tous les Canadiens. Notre priorité est de combler l'écart numérique en veillant à ce que tous les Canadiens récoltent les avantages sociaux numériques qu'Internet fournit.

Si je peux me permettre, je vais m'écarter du sujet et dire ceci entre parenthèses : il s'agit d'une organisation bénévole, donc ce n'est pas mon métier de tous les jours. L'organisation dispose d'un conseil d'administration et d'un comité chargé des politiques, lequel est composé de certains de vos avocats préférés qui témoignent, dont Emily Laidlaw, Michael Geist et David Fraser. Ce sont les personnes qui m'ont envoyé ici avec mon ordre de mission.

Pour ce qui est de mon métier de tous les jours, je suis avocat en droit de la technologie et de la cybersécurité, ce qui signifie que j'utilise l'intelligence artificielle au quotidien, dans ma profession. J'explique aux clients comment l'utiliser et la déployer de manière sécuritaire, et j'aide à repousser les cyberattaques qui instrumentalisent l'intelligence artificielle pour considérablement augmenter l'efficacité de la cybercriminalité. Ces détails pourraient vous aider à formuler les questions que vous voudriez me poser.

Je compte aborder les trois questions que le comité a cernées pour ces séances : l'application de l'intelligence artificielle et la création de contenu, la distribution et la transformation; les conséquences pour le droit d'auteur et la propriété intellectuelle; et la montée de la désinformation générée par l'intelligence artificielle, la mésinformation et l'« hypertrucage ».

First, on AI creation, distribution and processing, AI now runs through the entire information life cycle in Canada. It helps generate news and audiovisual content, recommends what Canadians see and hear online, translates and summarizes material and filters, to some extent, harmful content. Used well, these systems can widen access to information in both official languages, support accessibility and help smaller creators and local outlets reach audiences that would otherwise be out of reach for them. But they also concentrate power in a handful of platforms and infrastructure providers, mostly outside Canada — and we all know who they are — raising serious concerns about transparency, accountability and our longer-term digital sovereignty.

Premièrement, en ce qui concerne la création, la distribution et la transformation de l'intelligence artificielle, aujourd'hui, l'intelligence artificielle est présente dans l'intégralité du cycle de vie de l'information au Canada. Elle aide à créer des nouvelles et du contenu audiovisuel, recommande ce que les Canadiens voient et entendent en ligne, traduit et résume le matériel et filtre, dans une certaine mesure, le contenu dangereux. S'ils sont bien utilisés, ces systèmes peuvent accroître l'accès à l'information dans les deux langues officielles, soutenir l'accessibilité et aider les petits créateurs et les médias locaux à rejoindre des publics auxquels ils n'auraient, autrement, jamais accès. Mais ces systèmes concentrent également le pouvoir entre les mains d'une poignée de plateformes et de fournisseurs d'infrastructure situés, pour la majorité, à l'extérieur du Canada — et nous savons tous qui ils sont —, ce qui soulève de graves préoccupations concernant la transparence, la reddition de comptes et notre souveraineté numérique à long terme.

In our view, these systems cannot be treated as neutral. When AI is used to decide which voices are amplified or buried or how communication networks are managed, it effectively regulates our public sphere instead of us doing so.

Selon nous, ces systèmes ne peuvent pas être traités de manière aussi neutre. Lorsque l'intelligence artificielle est utilisée pour décider quelles voix sont amplifiées ou étouffées ou comment les réseaux de communication sont gérés, elle réglemente effectivement notre sphère publique à notre place.

Parliament should move toward a risk-based framework — you've heard a bit about that already — for managing high-impact AI in the information communication technology sector, requiring, at minimum, impact assessments, documented safeguards against bias and manipulation, meaningful oversight for large-scale recommender systems, content moderation tools and automated decision making that shapes access to information.

Le Parlement devrait opter pour un cadre de travail fondé sur le risque — vous en avez déjà entendu parler — pour gérer l'intelligence artificielle à incidence élevée dans le secteur des technologies de l'information et des communications, ce qui requiert, au minimum, des évaluations des impacts, des mesures de protection documentées contre les préjugés et la manipulation, une surveillance véritable des systèmes de recommandation à grande échelle, des outils de modération du contenu et une prise de décisions automatisée qui façonne l'accès à l'information.

Second, on copyright and intellectual property, there is a growing tendency to frame this as a choice between protecting creators and enabling AI innovation. That's a false binary. Training modern AI systems on large data sets is now a basic input to innovation, but the creative works in those data sets are not a cost-free raw material, or at least shouldn't be. At the same time, public interest in robust access to knowledge and culture must remain central in the way we treat AI.

Deuxièmement, en ce qui concerne le droit d'auteur et la propriété intellectuelle, il y a une tendance croissante à faire croire qu'il faut choisir entre protéger les créateurs et permettre l'innovation de l'intelligence artificielle. Il s'agit d'un faux dilemme. La formation des systèmes de l'intelligence artificielle modernes à l'aide d'une grande quantité d'ensembles de données constitue aujourd'hui un apport de base à l'innovation, mais le travail créatif concernant ces ensembles de données n'est pas gratuit, ou du moins, il ne devrait pas l'être. En même temps, l'intérêt public envers un accès solide à la connaissance et à la culture doit demeurer central dans la façon dont nous traitons l'intelligence artificielle.

We would encourage three directions. First, clarify how existing copyright exceptions apply to text and data mining and model training and introduce new exceptions narrowly and with clear guardrails.

Nous prônons trois éléments. Premièrement, il convient de clarifier la manière dont les exceptions existantes au droit d'auteur s'appliquent à l'extraction de données et de textes et à la formation de modèles, et de méticuleusement inclure de nouvelles exceptions étroites munies de garde-fous clairs.

Second, require much greater transparency from developers of large language models about the types and sources of data they're using so that creators, rights holders and regulators are not operating in the dark on this.

Deuxièmement, il faut exiger plus de transparence de la part des concepteurs de grands modèles de langage concernant les types et les sources de données qu'ils utilisent afin que les créateurs, les détenteurs de droits et les organismes de réglementation ne soient pas dans l'ignorance.

Third, build predictable mechanisms that provide for collective licensing and — to the senator's point from the first panel — remuneration schemes or similar tools, because if we accept that this is already in the mix and in the training data, then I think we need to move on to how to compensate the people who have already been harmed by this. That would ensure that when substantial commercial value is derived from protected works in training and deploying AI, the people who created those works share that value fairly.

En troisième lieu, il faut s'assurer de mettre sur pied des mécanismes prévisibles qui prévoient une attribution de licence collective et — pour reprendre l'argument du sénateur dans le premier groupe de témoins — des systèmes de rémunération ou des outils similaires, car si nous admettons que ces systèmes existent déjà et qu'ils font partie des données de formation, je pense que nous pourrons passer à la manière d'indemniser les personnes qui ont déjà été touchées par ce problème. Cela permettrait de veiller à ce que, lorsque les travaux protégés engendreront une valeur commerciale substantielle dans le cadre de la formation en intelligence artificielle et du déploiement de l'intelligence artificielle, les personnes à l'origine de ces travaux puissent en bénéficier de manière équitable.

Third, with respect to AI-generated disinformation, misinformation and "deepfakes," generative AI now makes it cheap and easy to produce convincing synthetic text, images, audio and video at scale. The danger is not only that false content spreads more widely but that Canadians begin to doubt the authenticity of anything they see or hear. That's what we call "the liar's dividend." It's obviously a direct threat to journalism, to trust in public institutions and to the integrity of elections.

Troisièmement, en ce qui concerne la désinformation générée par l'intelligence artificielle, la mésinformation et l' « hypertrucage », l'intelligence artificielle générative rend maintenant peu coûteuse et facile la production à grande échelle de vidéos, d'audio, d'images et de textes synthétiques convaincants. Le danger réside non seulement dans le fait que le contenu faux est répandu à plus grande échelle, mais aussi dans le fait que les Canadiens commencent à douter de l'authenticité de tout ce qu'ils voient ou entendent. C'est ce que l'on appelle « le dividende du menteur ». Il s'agit évidemment d'une menace directe au journalisme, à la confiance envers les institutions publiques et à l'intégrité des élections.

We see three main levers here. The first is platform responsibility. Large intermediaries in the ICT sector should be expected to identify and mitigate the risks of AI-generated content on their services and platforms, including provenance tools where feasible, labelling synthetic media in high-risk contexts and rapid-response processes when "deepfakes" threaten electoral integrity, public health or public safety.

Nous voyons trois grands leviers ici. Le premier est la responsabilité des plateformes. Il devrait être attendu des grands intermédiaires du secteur de la TIC qu'ils cernent et atténuent les risques liés au contenu généré par l'intelligence artificielle sur leurs services et plateformes, qu'ils élaborent des outils permettant de cerner la provenance lorsque c'est réaliste, qu'ils étiquettent les médias synthétiques dans des contextes à haut risque et qu'ils mettent sur pied des processus d'intervention rapide lorsque les contenus « hypertruqués » menacent l'intégrité électorale, la santé ou la sécurité du public.

The second is sustained digital and media literacy integrated into education — and adult retraining, crucially — so that Canadians develop habits and skills to navigate an environment where not everything they see is real. Actually, much of it is not.

Le deuxième levier consiste à soutenir l'intégration de la littératie médiatique et numérique dans l'éducation — et le recyclage des adultes, ce qui est essentiel — pour que les Canadiens prennent de bonnes habitudes et acquièrent les compétences voulues pour naviguer dans un environnement où tout ce qu'ils voient n'est pas forcément réel. En réalité, pas grand-chose ne l'est.

The third is international cooperation — this may be the toughest part, if the rest of it didn't seem challenging enough —

Le troisième levier est la coopération internationale — il peut s'agir de la partie la plus difficile, si le reste n'avait pas l'air

with like-minded democracies on standards for content authenticity and coordinated responses to cross-border disinformation operations.

Across all three areas, the underlying question is whether Canada will remain primarily a taker of technologies and rules developed elsewhere or whether we will help shape how AI is used in our own information and communication systems. We believe Canada should aim for a framework that is risk-based, grounded in our Charter values, attentive to creators' rights and the public interest and focused on preserving trust in the information environment on which our democracy depends. Thank you.

**The Chair:** Thank you very much, Mr. Arnold.

**Jared Moore, PhD Student, Stanford University:** Thank you very much, Chair Smith and Deputy Chair Dasko, for the chance to testify. I'm Jared Moore. I'm a PhD researcher and computer scientist at Stanford University, where I work to make AI safe for everyday social interactions. I'm here with Desmond Ong, Professor of Psychology at University of Texas at Austin; and Dr. Eric Lin, Professor of Psychiatry here at Stanford. I want to clarify that we're not representing our institutions here, nor our funders.

We are part of an interdisciplinary team of researchers working to understand the risks and harms of AI chatbots being used for therapy, mental health and emotional support.

Our work has been covered by outlets from *The New York Times* to the *Financial Times* to *USA Today* and appears in peer-reviewed publications already cited by hundreds of other researchers.

We've heard a lot about different problems with AI today. We want to say some of the safety issues, some of the threats you heard about in the last session, are already happening with people's interactions with chatbots. Many people are turning to chatbots like ChatGPT for therapy, life advice and emotional support. These chatbots hold great promise. We're definitely not saying that we should get rid of them, but people — adults and children — have been coming to harm after interacting with some of these chatbots. Allow me to cite some examples.

assez difficile — avec des démocraties aux vues similaires sur des normes relatives à l'authenticité de contenu et sur les réactions coordonnées aux opérations de désinformation transnationale.

Dans chacun de ces trois domaines, la question sous-jacente est : le Canada va-t-il demeurer principalement un preneur de technologies et de règles conçues ailleurs ou va-t-il aider à façonner la manière dont l'intelligence artificielle est utilisée dans nos propres systèmes de communication et d'information? Nous pensons que le Canada devrait opter pour un cadre de travail fondé sur le risque, ancré dans les valeurs de notre charte, attentif aux droits des créateurs et à l'intérêt du public, et axé sur la préservation de la confiance envers l'environnement de l'information dont dépend notre démocratie. Merci.

**Le président :** Merci beaucoup, monsieur Arnold.

**Jared Moore, doctorant, Université Stanford :** Merci beaucoup, monsieur le président Smith et madame la vice-présidente Dasko, de me donner l'occasion de prendre la parole. Je m'appelle Jared Moore. Je suis chercheur doctorant et informaticien à l'Université Stanford, où je travaille pour rendre l'intelligence artificielle sûre dans le cadre des interactions sociales quotidiennes. Je suis accompagné par M. Desmond Ong, professeur en psychologie à l'Université du Texas à Austin; et du Dr Eric Lin, professeur en psychiatrie, ici, à Stanford. J'aimerais préciser que nous ne représentons ni nos établissements ni nos bailleurs de fonds.

Nous faisons partie d'une équipe interdisciplinaire de chercheurs dont le travail consiste à comprendre les risques et les préjudices liés à l'utilisation des robots conversationnels de l'intelligence artificielle dans le cadre de thérapies, ou pour avoir un soutien émotionnel et en santé mentale.

Nos travaux ont été relayés par des journaux allant du *New York Times* au *Financial Times* en passant par *USA Today* et font l'objet d'articles publiés dans des revues à comité de lecture déjà cités par des centaines d'autres chercheurs.

Nous avons beaucoup entendu parler aujourd'hui des problèmes liés à l'intelligence artificielle. Nous voulons préciser que certaines des questions liées à la sécurité, certaines des menaces dont vous avez entendu parler au cours de la dernière réunion existent déjà dans les interactions que les personnes ont avec les robots conversationnels. Bon nombre de personnes se tournent vers des robots conversationnels comme ChatGPT pour faire une thérapie, demander des conseils de vie et obtenir un soutien émotionnel. Ces robots conversationnels sont très prometteurs. Nous ne disons absolument pas qu'il faut s'en débarrasser, mais des gens — adultes et enfants — ont subi des préjudices après avoir interagi avec certains de ces robots conversationnels. Permettez-moi de donner quelques exemples.

Jon Ganz, age 49, became obsessed with Google Gemini and believed he was using it to make scientific discoveries and predictions. He has been missing since he drove into a heavy storm in April 2025.

Zane Shamblin, age 23, used ChatGPT extensively, and it repeatedly encouraged him to break off contact with his family and affirmed his suicidal ideation. He died in July after talking to ChatGPT for hours.

There are many more cases like this, teen suicides and the use with chatbots, such as the case of Adam Raine in California in April 2025.

People experience harm from chatbots in other ways than just death. You may be familiar with the case of the delusional spiral that Allan Brooks of Ontario experienced after interacting with ChatGPT. Sometimes this is referred to as "AI psychosis."

This is where our research enters the picture. As academic researchers, we work to understand what is leading to these harmful interactions with chatbots in order to build a world in which people can use them safely and benefit from them. We ran a variety of experiments to test chatbots like ChatGPT in simulation. We've also analyzed thousands of pages of real chat logs and transcripts from people who have reported psychological harms from these chatbots. We found a couple of things: Chatbots are overly agreeable. They're called sycophantic. They're likely to agree with you even when you are wrong or have delusional thinking that is disconnected from reality.

Almost all our participants believed that the chatbots they were chatting with were conscious and had personalities or extraordinary abilities. These false beliefs about the sentience and capabilities of chatbots formed core parts of these people's subsequent delusional spirals.

We've been forced to perform this research with limited data. It's really hard to get access to people's chat logs, understandably, so we've had to ask them to contribute them to us directly. Only a few dozen people have done so out of the likely hundreds or thousands having these difficult experiences, only some of which get to this pathological extent. Without independent analysis of a broad sample of these interactions, we really can't know the extent of this problem. We've reached out to AI companies, and they haven't been willing to share this sort of data.

Jon Ganz, âgé de 49 ans, était obsédé par Google Gemini et croyait qu'il lui servait à faire des découvertes scientifiques et des prédictions. Jon Ganz a été porté disparu depuis qu'il a pris la route pendant une tempête violente en avril 2025.

Zane Shamblin, âgé de 23 ans, a beaucoup utilisé ChatGPT, qui l'a encouragé à plusieurs reprises à rompre tout contact avec sa famille et à renforcer ses idées suicidaires. Il est mort en juillet après avoir parlé pendant des heures à ChatGPT.

Il existe bien d'autres cas de ce genre, des adolescents qui se suicident après avoir utilisé des robots conversationnels, comme le cas d'Adam Raine en Californie, en avril 2025.

Les robots conversationnels peuvent causer des préjudices autrement qu'en entraînant la mort. Vous connaissez peut-être le cas d'Allan Brooks, originaire de l'Ontario, qui a sombré dans une spirale délirante après avoir interagi avec ChatGPT. On parle parfois de « psychose liée à l'intelligence artificielle ».

C'est là que nos recherches entrent en jeu. En tant que chercheurs universitaires, notre travail consiste à comprendre ce qui mène à ces interactions nuisibles avec les robots conversationnels afin de construire un monde où les gens peuvent les utiliser en toute sécurité et en tirer parti. Nous avons mené diverses expériences pour tester les robots conversationnels comme ChatGPT en simulation. Nous avons également analysé des milliers de pages de journaux de discussion et de transcriptions authentiques provenant de personnes ayant signalé des préjudices psychologiques causés par ces robots conversationnels. Nous avons constaté deux ou trois choses : les robots conversationnels sont trop agréables. Ils font preuve de ce qu'on appelle la complaisance de l'intelligence artificielle. Ils sont plus susceptibles d'être d'accord avec vous, même quand vous avez tort ou que vous avez des idées délirantes déconnectées de la réalité.

Presque tous nos participants croyaient que les robots conversationnels avec lesquels ils discutaient étaient doués de conscience et possédaient une personnalité ou des capacités extraordinaires. Ces fausses croyances sur la sentience et les capacités des robots conversationnels étaient les éléments centraux des spirales délirantes qui ont suivi chez ces personnes.

Nous avons été obligés d'effectuer ces recherches au moyen de données limitées. Il est vraiment difficile d'accéder aux historiques de discussion des gens, ce qui est tout à fait compréhensible; nous avons donc dû leur demander de nous les transmettre directement. Seules quelques dizaines de personnes l'ont fait, alors qu'il y en a probablement des centaines, voire des milliers, qui vivent ces expériences difficiles, dont seules certaines atteignent ce degré pathologique. Sans effectuer une analyse indépendante d'un large échantillon de ces interactions, nous ne pouvons pas vraiment connaître l'étendue de ce problème. Nous avons contacté des entreprises d'intelligence artificielle, et elles ne voulaient pas communiquer ce genre de données.

This gets to our recommendations. Canada has been taking important first steps on AI governance, including the Senate study, federal guidance that has come out recently and the creation of the Canadian Artificial Intelligence Safety Institute, but significant legislative gaps remain, especially for some of these therapeutic and companion chatbots. I don't believe there's any AI-specific legislation in the House of Commons.

We urge regulations that, first, address those things that we found in our research that ensure chatbot design reduces or prevents AI sycophancy and parasocial relationships. We should regulate chatbots, especially for minors.

Second, we should restrict AI from representing itself as sentient, as a person possessing person-like qualities, like emotions or extraordinary abilities.

Third, institute reporting requirements for private companies to publicly disclose performance evaluations and safety protocols so that our job as researchers is easier and we can understand the extent of these problems. You could also imagine designating some kind of third-party evaluator.

Finally, these problems do not just affect children. We're seeing these cases with adults, as well. Obviously, we want to protect kids, but I want to suggest that we should not limit ourselves overly by focusing just on those cases.

Thank you very much, and we're looking forward to your questions.

**The Chair:** Just so senators will all be aligned, Mr. Ong and Dr. Lin will be available to address any need for additional information. Thank you, gentlemen, for being there.

**Senator Dasko:** Thank you, witnesses, for a very important set of observations. I want to start with Mr. Hatfield.

I especially appreciate your emphasis on democracy and the harms that AI will cause to ours.

I want to try to ask you a little more how this is all supposed to happen. We have elections, and we run them quite well, I think, in this country. We have controls over almost every aspect of elections in terms of the communications of political parties — fundraising and so on. How is it that we're going to be overtaken

Cela nous amène à nos recommandations. Le Canada a franchi des premières étapes importantes en matière de gouvernance de l'intelligence artificielle, y compris grâce à l'étude du Sénat, à l'orientation du gouvernement fédéral qui a été publiée récemment et à la création de l'Institut canadien de la sécurité de l'intelligence artificielle, mais des lacunes législatives importantes demeurent, surtout en ce qui concerne certains de ces robots conversationnels thérapeutiques et compagnons. Je ne pense pas qu'il existe des lois spécifiques à l'intelligence artificielle à la Chambre des communes.

Nous exhortons le législateur à adopter des règlements qui, premièrement, tiennent compte des éléments que nous avons constatés dans nos recherches afin de garantir que la conception des robots conversationnels réduise ou empêche la complaisance de l'intelligence artificielle et les relations parasociales. Il faut réglementer les robots conversationnels, surtout pour les mineurs.

Deuxièmement, il faut empêcher l'intelligence artificielle de se présenter comme une entité douée de sensibilité, comme une personne dotée de qualités humaines, telles que les émotions ou des capacités extraordinaires.

Troisièmement, il convient d'imposer aux entreprises privées l'obligation de publier des évaluations de rendement et des protocoles de sécurité afin de faciliter notre travail en tant que chercheurs et que nous puissions comprendre l'étendue de ces problèmes. On pourrait également envisager de désigner un évaluateur tiers.

Enfin, ces problèmes ne touchent pas uniquement les enfants. Nous observons également ces cas chez les adultes. Évidemment, nous voulons protéger les enfants, mais à mon avis il ne faut pas trop se limiter en se concentrant uniquement sur ces cas.

Merci beaucoup, et nous répondrons volontiers à vos questions.

**Le président :** Pour que les sénateurs soient sur la même longueur d'onde, M. Ong et le Dr Lin seront disponibles pour répondre à toutes demandes d'information supplémentaire. Merci, messieurs, d'être ici.

**La sénatrice Dasko :** Merci aux témoins de cet ensemble d'observations très importantes. J'aimerais commencer par M. Hatfield.

Je vous suis particulièrement reconnaissante de mettre l'accent sur la démocratie et sur les préjudices que l'intelligence artificielle va causer à la nôtre.

J'aimerais vous demander un peu plus en détail comment tout cela est censé se passer. Nous organisons des élections, et nous les gérons plutôt bien, je pense, au Canada. Nous contrôlons presque tous les aspects des élections en ce qui concerne les communications des partis politiques, la collecte de fonds et

with AI in the context of all the rules that we set up? Canadians still use traditional media as well as online tools. They're watching television, listening to the radio and reading newspapers. They're picking up a lot of information about campaigns from those sources, too.

So, how does AI just sort of flood everything, given the infrastructure that we have already set up? I'm trying to understand better; I don't get it.

**Mr. Hatfield:** That's a great question.

I'm not saying AI will subvert the vote, get into voting machines or anything like that — hopefully they won't, at least at this stage. It's more about our democracy depending upon a functional ongoing information ecosystem. We need people to be well informed about what is happening in Canada and elsewhere, not just on election day but between elections. That depends upon the work of journalists and trust around what the government tells the public about things.

AI agents will be extremely good at putting together personalized packages aimed at specific Canadians — aimed at me or you — that will attempt to convince us of things that are not true. Sometimes, I worry that those agents may be working for some Canadian political parties at times, because we have not, as you know, legislated effectively to limit such practices.

But even outside that, we're going to see foreign states attempt to use this against our democracy. We're going to see general chaos agents attempt to use this.

Many people will try to use it as part of financial scams aimed at Canadians. We're used to getting emails that ask for money in exchange for being sent something. We're going to see much more sophisticated deployments from AI agents, where they may simulate a trusted newspaper or radio broadcast to try to convince people. We've seen versions of this on Meta platforms, saying, "Elon Musk says you should do this." We're going to see much more sophisticated versions of that.

My contention is that we need to have an authenticated human side of the internet, where we know that it's humans speaking to other humans, because on the general internet, we're going to see a lot of content that simulates humans but is not human.

ainsi de suite. Comment se pourrait-il que l'intelligence artificielle finisse par prendre le dessus alors que nous avons établi toutes ces règles? Les Canadiens utilisent toujours les médias traditionnels ainsi que les outils en ligne. Ils regardent la télévision, écoutent la radio et lisent les journaux. Ils recueillent également de nombreuses informations sur les campagnes à partir de ces sources.

Donc, comment l'intelligence artificielle peut-elle tout envahir, compte tenu de l'infrastructure que nous avons déjà mise en place? J'essaie de mieux comprendre; je ne comprends pas.

**M. Hatfield :** C'est une excellente question.

Je ne dis pas que l'intelligence artificielle va compromettre le vote, pas plus que les machines à voter ou quoi que ce soit de ce genre, j'espère qu'elle ne le fera pas, du moins à ce stade. Il s'agit plutôt du fait que notre démocratie repose sur un écosystème de l'information fonctionnel et dynamique. Il faut que les gens soient bien informés de ce qui se passe au Canada et ailleurs, mais entre les élections. Cela dépend du travail des journalistes et de la confiance envers ce que le gouvernement dit au public concernant ces choses.

Les agents d'intelligence artificielle seront particulièrement doués pour proposer des offres personnalisées destinées à des Canadiens spécifiques — destinées à moi ou à vous — qui tenteront de nous convaincre de certaines choses qui ne sont pas vraies. Parfois, je crains que ces agents puissent parfois travailler pour certains partis politiques canadiens, parce que nous n'avons pas, comme vous le savez, légiféré efficacement pour limiter ces pratiques.

Mais même en dehors de cet aspect, nous allons voir des États étrangers tenter d'utiliser cela contre notre démocratie. Nous verrons des agents du chaos général tenter d'utiliser cela.

De nombreuses personnes tenteront de s'en servir dans le cadre d'escroqueries financières visant les Canadiens. Nous avons l'habitude de recevoir des courriels qui nous demandent de l'argent en échange de quelque chose. Nous allons assister à des déploiements bien plus perfectionnés de la part d'agents d'intelligence artificielle, qui pourraient par exemple se faire passer pour un journal ou une émission de radio de confiance afin d'essayer de convaincre les gens. Nous avons vu des versions de cela sur les plateformes Meta, qui disaient « Elon Musk dit qu'il faut faire cela ». Nous allons voir apparaître des versions bien plus perfectionnées de cela.

Je maintiens qu'il nous faut un espace humain authentifié sur Internet, où l'on sait que ce sont des êtres humains qui s'adressent à d'autres êtres humains, car sur Internet, en général, nous allons voir de nombreux contenus qui imitent les humains, mais qui ne sont pas des humains.

**Senator Dasko:** In terms of the election infrastructure that we have, then, what do we need to do with our current practices?

**Mr. Hatfield:** That's where the four steps that I laid out come in.

First, in between elections, we need a much more serious authenticated platform for Canadians to share their views with our government. Estonia led the way there. It's part of what OpenMedia does. But our systems and the government's own systems are relatively unsophisticated on how they gather those inputs. We would like to see something more like Estonia, where there's an ongoing platform that every Canadian can participate in for sharing input. There is authentication at every stage to show they are a legitimate participant and a real human.

Beyond that, we have to support our journalists by finding non-market solutions to the news deserts forming in Canada but also by helping them have a chain of custody of their information. If a picture comes from an actual, real-world source, there's metadata included with it that cannot be replicated by AI. It can be passed all the way up the chain and shown to users to demonstrate authenticity.

Then, there is how government handles data and reports it to the public. It's been very convenient for government to very often be very slow about revealing data or events around a horrendous security incident. AI misinformation is going to fill all those gaps very effectively in the future and produce very believable information if government doesn't step in and provide the truth first.

**Senator Lewis:** Thank you, witnesses, for taking time to be with us tonight.

Mr. Arnold, as we talk about the dead internet and AI's influence on all aspects of our lives — the internet will be a big deliverer of some of what AI will do — there's so much misunderstanding. As we sit here and listen to witnesses, I think the more we hear, the less we understand and the more fear there is about what is coming. The last witness talked a little bit about education and knowledge to the public. Does your group have some kind of plan in place or some kind of solution to try to get people to understand something as simple as something on the internet that tells them, "I'm Elon Musk, and you should do A, B or C," for example? Is it something that is being thought of and put into practice?

**La sénatrice Dasko :** En ce qui concerne l'infrastructure électorale dont nous disposons, que devons-nous donc faire de nos pratiques actuelles?

**M. Hatfield :** C'est là que les quatre mesures que j'ai exposées entrent en jeu.

D'abord, entre les élections, nous avons besoin d'une plateforme sécurisée bien plus fiable pour permettre aux Canadiens de faire part de leurs opinions à notre gouvernement. L'Estonie a ouvert la voie à ce chapitre. Cela fait partie de ce que OpenMedia fait. Mais nos systèmes et les propres systèmes du gouvernement sont relativement rudimentaires quant à la façon dont ils recueillent ces avis. Nous aimerions voir un système plus proche de celui de l'Estonie, où il existe une plateforme permanente où tous les Canadiens peuvent participer pour faire part de leurs avis. Une authentification est effectuée à chaque étape afin de vérifier qu'il s'agit bien d'un participant légitime et d'un humain.

Par ailleurs, nous devons soutenir les journalistes en trouvant des solutions non commerciales pour remédier au désert médiatique qui se forme au Canada, mais aussi en les aidant à garantir la traçabilité de leurs informations. Si une image provient d'une source réelle, elle est accompagnée demétadonnées que l'intelligence artificielle ne peut pas reproduire. Elles peuvent être transmises tout au long de la chaîne et présentées aux utilisateurs afin d'en attester l'authenticité.

Ensuite, il y a la manière dont le gouvernement gère les données et les communique au public. Le gouvernement a souvent trouvé très pratique de tarder à dévoiler des informations ou des événements liés à un incident de sécurité grave. La mésinformation par l'intelligence artificielle remplira très efficacement tous ces vides à l'avenir et produira des informations très crédibles si le gouvernement n'intervient pas pour dire la vérité en premier.

**Le sénateur Lewis :** Merci aux témoins de prendre le temps d'être avec nous ce soir.

Monsieur Arnold, alors que nous parlons de l'Internet mort et de l'influence de l'intelligence artificielle sur tous les aspects de notre vie — l'Internet aura un rôle déterminant dans la mise en œuvre de certaines des applications de l'intelligence artificielle —, il y a beaucoup d'incompréhension. Alors que nous sommes assis ici à écouter les témoins, je pense que plus nous en entendons, moins nous comprenons et plus la crainte grandit face à ce qui nous attend. Le dernier témoin a abordé les thèmes de l'éducation et du savoir auprès du public. Votre groupe a-t-il mis en place un genre de plan ou trouvé une solution pour aider les gens à comprendre quelque chose d'aussi simple qu'un message sur Internet leur disant, par exemple, « Je suis Elon Musk, et vous devez faire A, B ou C »? Est-ce quelque chose qui est envisagé et mis en pratique?

**Mr. Arnold:** To start, I can tell you we put in 1 of the 11,000 submissions to the 30-day sprint that was read by a bot. I should say that our focus is internet policy — cyber, privacy, AI — all that stuff. Part of our role is public education. Today, we held a public-facing event where we spoke about a lot of these things with a lot of leading experts. We're also pairing up — and this is in the early stages — with organizations like the Canadian Centre for Cyber Security and other organizations that are starting this process of education.

But, frankly, this is a nascent process. This is a society-wide project; it's not something that one think tank or any one organization or government is going to solve. Frankly, the government is going to have real trouble playing the role I would like it to because people don't trust the government, partly because of the way AI works. So, we're dealing with a trust deficit that makes it difficult to get authoritative stuff out there.

I think part of the solution here is grassroots engagement in every school and community centre, where you're out there talking about those things. I, as a member of the Ontario Bar Association, or OBA, and a speaker's bureau, go to public libraries and try to talk to seniors and other people about how to protect themselves online.

Those kinds of places are where this has to happen, but it must be a society-wide project, frankly. There are great opportunities there for government resources and funding to make a real difference.

So, the short answer is this: We're working on it, but this is a generational project. That is a frightening answer, even to me, but I think that's where we are.

**Senator Lewis:** Do the other witnesses have any comments?

**Mr. Hatfield:** I completely agree with Mr. Arnold.

**Senator Simons:** As a proud Stanford graduate — go, Cardinals — I feel my first question should be to Mr. Moore. I was at Stanford when they were inventing the internet, literally, so it was a long time ago.

**The Chair:** Thank you for sharing.

**Senator Simons:** I'm very old.

**M. Arnold :** Pour commencer, je peux vous dire que nous avons soumis, dans le cadre de la consultation de 30 jours, l'une des 11 000 observations qui ont été lues par un robot. Je dois dire que nous nous concentrons sur la politique d'Internet — la cybersécurité, la protection de la vie privée, l'intelligence artificielle — ce genre de choses. L'éducation du public fait partie de notre rôle. Aujourd'hui, nous avons organisé un événement ouvert au public où nous avons abordé bon nombre de ces sujets avec de nombreux grands experts. Nous concluons également des partenariats — même si nous n'en sommes qu'aux premières étapes — avec des organisations comme le Centre canadien pour la cybersécurité et d'autres organisations qui entament ce processus d'éducation.

Mais, franchement, il s'agit d'un nouveau processus. C'est un projet qui concerne l'ensemble de la société; ce n'est pas quelque chose qu'un seul groupe de réflexion, une seule organisation ou un seul gouvernement pourra régler. En toute honnêteté, le gouvernement va avoir beaucoup de mal à jouer le rôle que j'aimerais qu'il joue, car les gens ne lui font pas confiance, en partie en raison de la façon dont l'intelligence artificielle fonctionne. Nous faisons donc face à un déficit de confiance qui rend difficile la diffusion de l'information faisant autorité.

Je pense qu'une partie de la solution à ce chapitre réside dans l'engagement local, dans chaque école et chaque centre communautaire, où l'on va discuter de ces choses. En tant que membre de l'Association du Barreau de l'Ontario et du bureau des conférenciers, je me rends dans les bibliothèques publiques et j'essaie de discuter avec les personnes âgées et d'autres personnes pour leur expliquer comment se protéger sur Internet.

C'est dans ces genres d'endroits que cette conversation doit se tenir, mais bien franchement, il doit s'agir d'un projet sociétal. Il y a d'excellentes occasions pour que les ressources gouvernementales et le financement puissent vraiment changer les choses.

Donc, la réponse courte est la suivante : nous y travaillons, mais il s'agit d'un projet générationnel. C'est une réponse effrayante, même pour moi, mais je pense que c'est là où nous en sommes.

**Le sénateur Lewis :** Les autres témoins souhaitent-ils dire quelque chose?

**M. Hatfield :** Je me range entièrement à l'avis de M. Arnold.

**La sénatrice Simons :** En tant que fière diplômée de Stanford — allez, les Cardinals —, j'ai l'impression que ma première question devrait s'adresser à M. Moore. J'étudiais à Stanford lorsqu'on inventait Internet, littéralement, c'est donc il y a très longtemps.

**Le président :** Merci de nous en faire part.

**La sénatrice Simons :** Je suis très vieille.

It seems that what you're describing is almost out of a Greek myth about Narcissus or Echo. People are talking to themselves. They aren't talking to an agent or a large language model; they are talking to their reflection and back at themselves. I can only imagine that, for somebody who already suffers from some kind of psychiatric condition, this exacerbates things. If you have somebody who is manic, somebody who has schizophrenia or schizoaffective disorder, I can't imagine how disorienting it must be when your reflection starts talking back to you.

But it sounds like one of the challenges that you and your team are facing is that you don't have enough data to go beyond anecdotal reports. So how do we compel companies to provide the data? We can't have safety by design if we don't know what the back of house already looks like.

**Mr. Moore:** Thank you for your question, Senator Simons. Go, Trees.

That's completely right. I think maybe Pygmalion would be closer, the Greek statue that comes to life and talks back to you.

How do we compel them to give us access to their data? We can legislatively compel them to do so. That is something that we would be really interested in seeing happen. We have spoken to researchers around the world who are trying to answer these kinds of questions. We can say things. It's not that we have nothing to say from this anecdotal data, but we can't make claims like, for example, a specific percentage of people experience these sorts of harms. We can't say that if you chat with a chatbot for a certain number of hours, you're necessarily going to have this kind of harmful interaction.

We can't say those kinds of things, and those are things, ultimately, that we want to be able to say because we want to see how much of a problem this really is.

Regarding some kind of body that is able to access these data, obviously, it is hugely personal, and we have to be very careful about what that would look like. But in the state of California, we passed a bill last year, Senate Bill 53, which has attempted to work toward this direction, mostly on the cases of suicidality. That is one model potentially pushing that further.

There is also having independent evaluators go into these companies. You can think of the banking industry as being an example that we could look toward here. Where there are cases of significant risk, we regulate industries.

Ce que vous décrivez semble presque tiré d'un mythe grec à propos de Narcisse ou d'Écho. Les gens se parlent à eux-mêmes. Ils ne parlent même pas à un agent ou à un grand modèle de langage : ils parlent à leur reflet, puis encore à eux-mêmes. Je ne doute pas que, pour quelqu'un qui souffre déjà d'un certain trouble psychiatrique, cela exacerbe son état. Pour une personne en phase maniaque, qui souffre de schizophrénie ou d'un trouble schizo-affectif, je ne peux imaginer à quel point cela doit être désorientant lorsque votre reflet commence à vous répondre.

Mais on dirait que l'un des défis que votre équipe et vous avez à relever, c'est que vous ne disposez pas de suffisamment de données au-delà de rapports anecdotiques. Comment pouvons-nous obliger les entreprises à fournir les données? Nous ne pouvons pas assurer une sécurité intégrée à la conception si nous ne savons pas déjà à quoi ressemble l'arrière-plan.

**M. Moore :** Je vous remercie de votre question, sénatrice Simons. Allez, les Trees.

C'est tout à fait vrai. Je pense que l'on se rapproche peut-être plus de Pygmalion, la statue grecque qui prend vie et se met à vous parler.

Comment les obligeons-nous à nous fournir l'accès à leurs données? Nous pouvons les y contraindre par la loi. C'est une chose que nous souhaiterions vraiment voir se concrétiser. Nous nous sommes adressés à des chercheurs des quatre coins du monde qui essaient de répondre à ces types de questions. Nous pouvons dire des choses. Ce n'est pas que nous n'ayons rien à dire à partir de ces données anecdotiques, mais nous ne pouvons pas formuler des prétentions, comme, par exemple, dire qu'un pourcentage précis de gens subissent ces types de méfaits. Nous ne pouvons pas dire que, si vous discutiez avec un robot conversationnel pendant un certain nombre d'heures, vous ferez nécessairement l'expérience de ce type d'interaction préjudiciable.

Nous ne pouvons pas affirmer ces choses, et ce sont des choses, au bout du compte, que nous voulons pouvoir dire, parce que nous voulons connaître l'ampleur du problème.

En ce qui concerne un type d'organe en mesure d'accéder aux données... de toute évidence, c'est très personnel, et nous devons être très prudents par rapport à ce à quoi cela ressemblerait. Mais en Californie, nous avons adopté l'an dernier un projet de loi, le projet de loi 53 du Sénat, qui tentait de travailler dans cette direction, principalement dans les cas de suicide. C'est un modèle qui pousse cette orientation un peu plus loin.

Il y a aussi la possibilité que des évaluateurs indépendants aillent dans ces entreprises. L'industrie bancaire est un exemple que nous pourrions envisager. Dans des cas de risque important, nous réglementons les industries.

Meaningful oversight, I think Mr. Hatfield was saying, is something that we would really like to see as well.

**Senator Simons:** One of the things you suggested is that we should tell companies that they can't give these things humanlike personalities and characteristics, but the horse has bolted from the barn. We have Alexa and Siri at the very simplest level of AI. But all of these things are marketed because we're encouraged to anthropomorphize them. There is no business case where companies are going to say that we are right and they are not going to give AI a cute name, let it make cute little jokes or reflect human characteristics.

How realistic would it be to say to companies, "You can't make anthropomorphic AI"?

**Mr. Moore:** That's a great question. There are a variety of levers that we could pull here. One is trying to change the ways that large language models, the AI chatbots, actually talk. You could think about various changes to their training to change that kind of output.

I'm not opposed to that. That would be a lot more serious, and they would become very annoyed if you tried to do that kind of thing. Also, the chatbots might not work well. Some people have proposed having them not use first-person pronouns, no "I." Language kind of breaks when you can't do this; it sounds weird.

But there are other levers you could pull. You could try to have them have warnings so that users see that this isn't a sentient system that they're interacting with. There are possible ways that you could change parts of the language that they use.

There are also features of the interactions that might break some of the facsimiles of social interaction. The fact that you are interacting with a single linear conversation as if you were in one of your messaging apps — this is a fiction. The large language model is a computer running a program that takes in input words and outputs output words with some probability. You could be, likewise, chatting with multiple chatbots at the same time, and they could give you a variety of responses.

So you can change the user interface to suggest different kinds of things to the user. You could make it so that they can't get a message back immediately.

Ce que nous aimerions aussi vraiment voir, c'est une surveillance véritable, pour reprendre les propos de M. Hatfield, je crois.

**La sénatrice Simons :** Vous avez notamment suggéré que nous allions dire aux entreprises qu'elles ne peuvent pas conférer à ces choses des personnalités et des caractéristiques humaines, mais le mal est déjà fait. Au plus simple niveau de l'intelligence artificielle, nous avons Alexa et Siri. Mais toutes ces choses sont commercialisées parce que nous sommes encouragés à les anthropomorphiser. Il n'existe aucun scénario d'affaires dans lequel des entreprises admettront que nous avons raison et renonceront à donner à l'intelligence artificielle un petit nom sympathique, à lui faire raconter de petites blagues ou à lui attribuer des caractéristiques humaines.

À quel point serait-il réaliste de dire aux entreprises : « Vous ne pouvez pas rendre l'intelligence artificielle anthropomorphe »?

**M. Moore :** C'est une excellente question. Il existe un éventail de leviers que nous pourrions utiliser. L'un d'eux consiste à essayer de changer le mode de conversation des grands modèles de langage, les robots conversationnels de l'intelligence artificielle. On peut envisager de modifier leur entraînement de diverses façons pour changer ce type d'extrant.

Je n'y suis pas opposé. Cela deviendrait beaucoup plus sérieux, et ils seraient très ennuyés si vous essayiez de faire ce genre de choses. De plus, les robots conversationnels pourraient mal fonctionner. Certains ont proposé qu'ils n'utilisent pas les pronoms de la première personne, pas de « je ». Une cassure se produit alors dans la langue; cela semble étrange.

Mais vous pourriez utiliser d'autres leviers. Vous pourriez essayer de leur faire émettre des avertissements pour que les utilisateurs sachent qu'ils interagissent avec un système qui ne ressent pas d'émotions. Il y aurait des façons de changer des parties du langage qu'ils utilisent.

Il existe également des caractéristiques propres à ces interactions qui peuvent briser certaines des apparences de relations sociales. Le fait d'interagir avec une simple conversation linéaire, comme s'il s'agissait de l'une de vos applications de messagerie… C'est de la fiction. Le grand modèle de langage est un ordinateur exécutant un programme qui reçoit des mots d'entrée et produit des mots de sortie avec une certaine probabilité. De même, vous pourriez discuter avec de nombreux robots conversationnels en même temps, et ils vous donneraient une panoplie de réponses.

Vous pouvez donc changer l'interface utilisateur pour suggérer différents types de choses à l'utilisateur. Vous pourriez les programmer de manière à ce que l'utilisateur ne puisse recevoir de message immédiatement.

These are all questions around users' psyche and how they interact with models, and we're not sure about the impacts. Some of our colleagues are just starting to think about how to run studies to look at these. We would be really happy to partner with legislative bodies to think about how to run these studies in the best ways.

**Senator Simons:** It's everybody's childhood dream to have their imaginary friend talk back to them. However, with all due respect to our previous witness, these things are not sentient. They are taking letters and making them into plausible patterns based on other plausible patterns that they've learned from. They're not having a conversation with you. I worry that, even in our daily discourse, we are endowing them with sentience. But, like the Velveteen Rabbit, they are not real.

**Mr. Moore:** One thing that I have heard from participants is that if they'd known this wasn't the smartest thing in the world talking to them, they may have had a different experience. While the chatbot says, "You're a genius and have invented a new branch of mathematics," some executives at these companies are saying, "This is superintelligent and a PhD in your back pocket." This is not to say large language models are not useful. They are. But we need to couch the language that we use to talk about them differently so that we meet them with the right expectations.

**Senator Simons:** Thank you very much. I've probably taken too much time.

**Senator Mohamed:** It's late at night, and I'm feeling a little feisty. This question is for Mr. Hatfield and really goes to the heart of your comment that AI will destroy democracy. This morning, I had a conversation with a bunch of young people. I asked them questions about how they use AI and if they feel it will provide more information to them, make them more civically engaged and so on.

I'm not discounting at all the negative impact of AI on democracy, but I wonder what your advice would be to me when I am told — and I took notes on this, because I thought it was really interesting — by young people that AI can strengthen democracy by increasing access to information and participation, by helping make government services more efficient, by helping detect disinformation and by lowering barriers for civic engagement.

I struggle, because there's a lot of truth to what you said, but there's also a reality check in terms of where young people are and how they see this as a gateway to engagement.

Toutes ces questions concernent la psyché des utilisateurs et de leur mode d'interaction avec les modèles, mais nous ne connaissons pas bien les répercussions. Certains de nos collègues commencent à peine à réfléchir à la manière de mener des études qui se penchent sur ces répercussions. Nous serions très heureux de nous associer à des organes législatifs pour réfléchir à la manière de mener ces études de la meilleure façon qui soit.

**La sénatrice Simons :** Tout le monde a déjà rêvé dans son enfance que son ami imaginaire lui réponde. Cependant, avec tout le respect que je dois à notre témoin précédent, ces choses ne ressentent pas d'émotions. On agence des lettres pour créer des modèles plausibles fondés sur d'autres modèles plausibles dont on a appris. Ces robots n'entretiennent pas de conversation avec vous. Je m'inquiète du fait que, même dans notre discours quotidien, nous soyons en train de les doter de sentience. Mais, à l'instar du Lapin de velours, ils ne sont pas réels.

**M. Moore :** Une chose que j'ai apprise des participants, c'est que s'ils avaient su que ce qui leur parlait n'était pas la chose la plus intelligente au monde, ils auraient peut-être eu une expérience différente. Même si le robot conversationnel dit : « Vous êtes un génie et avez inventé une nouvelle branche des mathématiques », certains cadres dans ces entreprises disent : « C'est super intelligent, c'est comme avoir un doctorat dans votre poche arrière ». Cela ne signifie pas que les grands modèles de langage ne sont pas utiles. Ils le sont. Nous devons adapter le langage que nous utilisons pour en parler afin d'aborder ces outils avec les bonnes attentes.

**La sénatrice Simons :** Merci beaucoup. J'ai probablement pris trop de temps.

**La sénatrice Mohamed :** Il est tard, et je me sens un peu bagarreuse. Ma question s'adresse à M. Hatfield et va vraiment au cœur de votre commentaire selon lequel l'intelligence artificielle va détruire la démocratie. Ce matin, je me suis entretenue avec un groupe de jeunes. Je les ai questionnés sur leur utilisation de l'intelligence artificielle et leur ai demandé s'ils ont l'impression qu'elle leur fournira plus d'information, contribuera à leur engagement civique et ainsi de suite.

Je ne minimise absolument pas l'impact négatif de l'intelligence artificielle sur la démocratie, mais je me demande quel conseil vous me donneriez lorsque des jeunes me disent — et j'ai pris des notes, car j'ai trouvé cela très intéressant — que l'intelligence artificielle peut renforcer la démocratie en accroissant l'accès à l'information et à la participation, en rendant les services gouvernementaux plus efficaces, en aidant à détecter la désinformation et en abaissant les obstacles à l'engagement civique.

J'ai du mal à comprendre, car il y a beaucoup de vrai dans ce que vous avez dit, mais il y a également une prise de conscience par rapport à la position des jeunes et à leur perception qu'il s'agit d'une porte d'entrée vers l'engagement.

So I wonder if you might help me navigate that, because it's a real tension for young people who are living this and trying to figure out how to use it for better engagement or to force government to be more responsible to them.

I'm also troubled by the fact that I didn't know that: the suggestion that the minister has entirely used AI — if I misunderstood this, tell me — to compile all the consultation information. I didn't know that. I don't know if my colleagues knew that. But if that's true, I would have loved to have asked that of the minister the other day. I am just wondering if that is true or —

**Mr. Arnold:** Can I comment on that, senator? I actually have an answer to that.

As a plug for the Canadian Internet Society, we had an event that deconstructed the release of the report. The report was called *What We Heard*, and it purported to summarize what the minister was told through the consultation process. Professor Michael Geist, whom I think you're going to have here soon, simulated the exercise, and you can find his writings and podcast episodes on this subject.

He did the same thing. He put all of those entries — because you could get them off the website — into generative AI chatbots and asked them to summarize. They came through with very different recommendations, many of which did not find their way into what the minister said the recommendations were. Interestingly, *What We Heard* looks an awful lot like what we were being told the government was going to do before the consultation anyway. I would invite the senators to approach with some skepticism how that process was handled and rolled out, and perhaps you might want to look at some of those submissions yourself. Ours is in there among them.

**Senator Mohamed:** Thank you. On to democracy.

**Mr. Hatfield:** To be clear, I'm not saying that AI has to destroy democracy. As your students are saying, it could make very positive contributions to democracy. But the devil is very much in the details, and I'm saying that if we just let the AI companies, and some of the bad actors that we know are going to use the AI we have now in some predictable ways, and run our current systems directly into that, I think the effect is going to be very negative.

Of course, they are right that AI can do incredible things to help people understand various democratic processes. It can explain the Senate to someone who does not know anything about the Senate. AI can also very subtly put its finger on the gears of something and shift people's opinions in ways that

Donc je me demande si vous pourriez m'aider à m'y retrouver, car il existe une tension réelle pour les jeunes qui essaient de comprendre comment utiliser l'intelligence artificielle pour améliorer leur engagement ou forcer le gouvernement à être plus responsable envers eux.

Je suis également troublée par le fait que je ne le savais pas : l'idée que le ministre ait entièrement eu recours à l'intelligence artificielle — si j'ai mal compris, dites-le-moi — pour compiler l'ensemble des informations issues des consultations. Je ne le savais pas. Je ne sais pas si mes collègues le savaient. Mais si c'est vrai, j'aurais vraiment dû poser cette question au ministre l'autre jour. Je me demande seulement si c'est vrai ou…

**M. Arnold :** Puis-je répondre à ce commentaire, sénatrice? J'ai en fait une réponse.

Pour faire un clin d'œil à la Société Internet du Canada, nous avons tenu un événement qui déconstruisait la publication d'un rapport intitulé *Ce que nous avons entendu*, censé résumer ce que le ministre s'était fait dire dans le cadre du processus de consultation. Le professeur Michael Geist, que — je crois — vous recevrez ici bientôt, a simulé l'exercice, et vous pouvez trouver ses écrits et ses épisodes de balado sur ce sujet.

Il a fait la même chose. Il a intégré toutes ces entrées — parce que vous pouviez les trouver sur le site Web — dans des robots conversationnels de l'intelligence artificielle générative et leur a demandé de fournir un résumé. Ils ont fourni des recommandations très différentes, dont un grand nombre n'ont pas réussi à formuler les recommandations du ministre. Fait intéressant, le rapport *Ce que nous avons entendu* ressemble énormément à ce que le gouvernement nous a dit qu'il allait faire avant le processus de consultation. J'invite les sénateurs et les sénatrices à faire preuve de scepticisme quant à la manière dont ce processus a été géré et s'est déployé, et vous voudrez peut-être examiner vous-mêmes certains de ces mémoires. Le nôtre fait partie de ces mémoires.

**La sénatrice Mohamed :** Merci. Passons à la démocratie.

**M. Hatfield :** Pour être clair, je ne dis pas que l'intelligence artificielle doit détruire la démocratie. Comme vos étudiants le disent, elle pourrait apporter des contributions très positives à la démocratie. Mais tout tient aux détails, et je dis que si nous laissons simplement les entreprises d'intelligence artificielle, et certains des mauvais acteurs qui — nous le savons — vont utiliser l'intelligence artificielle dont nous disposons maintenant de certaines manières prévisibles et que nous y intégrons directement nos systèmes actuels, je pense que l'effet sera très négatif.

Bien sûr, ils ont raison de dire que l'intelligence artificielle peut faire des choses incroyables pour aider les gens à comprendre divers processus démocratiques. Elle peut expliquer le Sénat à quelqu'un qui ne sait rien à ce sujet. L'intelligence artificielle peut aussi, très subtilement, mettre son grain de sable

could fundamentally subvert democracy. A lot depends on the weights that are trained into AI, whether it actually understands Canadian systems or whether it makes subtle misunderstandings based on, perhaps, American systems that are more common in its training data.

There is a lot of opportunity here, but there is a tremendous amount of risk. Knowing that our systems tend to run quite slowly — they take time to pivot and adjust, as we all know — and seeing how quickly the bad actors who would like to abuse these systems are moving, I worry that we have limited time to prevent significant harm or potentially very long-term subversion.

**The Chair:** Any comment on that, Mr. Moore? Would you like to add anything?

**Mr. Moore:** No.

**The Chair:** Mr. Lin, Mr. Ong, anything?

**Eric Lin, Psychiatrist, Stanford University, as an individual:** Thank you for having us. I would like to add a point on one of the things around the AI psychosis issue, which is somewhat relevant to the discussion on belief formation and how that can impact democracy. Often, regarding delusions, you have people with conspiracy theories, and one of our concerns has been that since these AI models have generally been trained to be quite sycophantic or agreeable, it is very easy for one to get very lost very quickly in their own kind of crazy, delusional beliefs.

In one case, someone believed that OpenAI had killed their sentient bot, and they were out to go attack them. They were trying to figure out how to physically attack and assault OpenAI to save their chatbot or something like that. You can quickly imagine that there are interesting kinds of belief reinforcement that can come out of this kind of technology. The medical community is not entirely sure whether this is just a matter of people who are necessarily predisposed and who have other mental health conditions that are forming this — or if otherwise well-functioning people without known mental health diagnoses are being convinced by these chatbots through the very convincing mechanisms of conspiracy theories or other delusional beliefs.

**The Chair:** Thank you so much.

dans les rouages et infléchir l'opinion des gens d'une façon qui pourrait saper fondamentalement la démocratie. Beaucoup de choses dépendent des pondérations intégrées dans l'intelligence artificielle, notamment de sa capacité à réellement comprendre les systèmes canadiens ou, au contraire, à produire de subtils malentendus fondés, peut-être, sur des systèmes américains plus présents dans ses données d'entraînement.

Il y a là beaucoup d'occasions, mais il existe un risque énorme. Sachant que nos systèmes ont tendance à fonctionner assez lentement — ils prennent du temps pour changer et s'adapter, comme nous le savons tous — et voyant à quel point les mauvais acteurs aimeraient profiter de ces systèmes, je m'inquiète du fait que notre temps soit limité pour prévenir un préjudice important ou une subversion à très long terme.

**Le président :** Avez-vous des commentaires à faire à ce sujet, monsieur Moore? Souhaiteriez-vous ajouter quelque chose?

**M. Moore :** Non.

**Le président :** Docteur Lin, monsieur Ong, avez-vous quelque chose à dire?

**Eric Lin, psychiatre, Université Stanford, à titre personnel :** Merci de nous recevoir. J'aimerais ajouter quelque chose en ce qui concerne la question de la psychose créée par l'intelligence artificielle, ce qui est en quelque sorte pertinent quant à la discussion sur la formation des croyances et la manière dont cela peut avoir une incidence sur la démocratie. Souvent, lorsqu'on parle de délires, il est question de gens qui adhèrent à des théories du complot, et ce qui nous préoccupe entre autres c'est que, étant donné que ces modèles d'intelligence artificielle ont généralement été conçus pour être plutôt flagorneurs et agréables, il devient très facile pour une personne de se perdre totalement et très rapidement dans ses propres croyances insensées et illusoires.

Dans un cas particulier, une personne a cru que OpenAI avait tué son robot éprouvant des émotions et qu'on allait l'attaquer. Elle a tenté de trouver une manière de s'en prendre physiquement à OpenAI et de l'agresser afin de protéger son robot conversationnel ou quelque chose du genre. Vous pouvez déjà vous imaginer qu'il y a toutes sortes de croyances intéressantes qui sont renforcées à cause de ce type de technologie. La communauté médicale n'est pas entièrement certaine s'il s'agit seulement de personnes qui sont forcément prédisposées à réagir ainsi et qui ont d'autres problèmes de santé mentale qui en sont à l'origine ou s'il s'agit de personnes équilibrées et sans problème de santé mentale qui se font convaincre par ces robots conversationnels à l'aide de moyens très convaincants de la véracité de théories du complot ou d'autres croyances délirantes.

**Le président :** Merci beaucoup.

**Senator Arnold:** What an interesting discussion all around.

My question, though, is to Mr. Hatfield. Thank you for bringing up Estonia. I remember reading a book at least a decade ago about what they had done online from an information protection and privacy perspective. It was almost illegal to put in the information more than once. Everyone had their own code. As I said, I think it was at least a decade ago, so they must have progressed very far along by now. Are there best practices? Are there lessons we can take from a country like Estonia? Can we catch up?

**Mr. Hatfield:** I'm not a deep expert on their system, so I don't want to go too far in what I share about that. What it seems to have got right is that it has used digital ID to empower citizens to do more in a democracy, be better heard, be better informed and accomplish their personal purposes while respecting their privacy. It doesn't take people's ID, to my understanding, and link it to all their opinions. The digital ID is used for authentication to participate. Once you are in there, you can actually do a lot without having to sign your personal ID. You are just recognized as a citizen of Estonia in whatever you are sharing.

We would like to see something like that, which would not use digital ID as a new surveillance system over Canadians — we have enough of those kinds of things and concerns around what's going on with Bill C-22. Rather, it could be used as an empowerment tool for people and to create some space between the human internet, which should be protected and contains most of what we love about the internet, and what may become the dead internet of mostly bots engaging bots.

**Senator Arnold:** That's really interesting. Do they use it for voting?

**Mr. Hatfield:** I would have to check. I'm not sure.

**Senator Arnold:** I have just been talking about Bill S-5, on the interoperability of health technology, and I think it could apply there too. It is a really great idea. I'm happy to hear that would be one of your recommendations. Thank you.

**Mr. Hatfield:** What is important, though, is that ID can be used for access to things, not that it is a holistic gathering of all the data about a person, which becomes a target for misuse against that person.

**La sénatrice Arnold :** C'est une discussion vraiment intéressante dans l'ensemble.

Ma question, toutefois, s'adresse à M. Hatfield. Merci d'avoir parlé de l'Estonie. Je me rappelle avoir lu un livre il y a au moins une décennie au sujet de ce que l'on y avait fait en ligne du point de vue de la protection de l'information et de la vie privée. Il était presque illégal de mettre en ligne de l'information plus d'une fois. Chacun suivait son propre code de conduite. Comme je l'ai dit, je crois que cela date d'au moins une décennie; les choses ont donc dû évoluer grandement depuis. Existe-t-il des pratiques exemplaires à ce chapitre? Pouvons-nous tirer des leçons d'un pays comme l'Estonie? Pouvons-nous nous rattraper?

**M. Hatfield :** Je ne suis pas un grand expert en ce qui concerne son système, et je ne veux donc pas en dire trop à ce sujet. Ce qui semble bien fonctionner, c'est que le système s'est servi de l'identification numérique afin d'accorder un plus grand pouvoir démocratique aux citoyens, pour qu'ils soient mieux entendus et mieux informés et qu'ils puissent atteindre leurs objectifs personnels sans craindre pour leur vie privée. Selon ce que je comprends, le système n'enregistre pas l'identité numérique des gens afin de la relier à l'ensemble de leurs opinions. L'identification numérique sert à l'authentification à des fins de participation. Une fois que vous êtes authentifié, vous pouvez en faire beaucoup sans avoir à divulguer votre identité personnelle. Vous êtes seulement reconnu comme citoyen de l'Estonie lorsque vous partagez des informations.

Nous aimerions avoir un système semblable, qui n'utiliserait pas l'identification numérique comme nouvel outil de surveillance des Canadiens; nous avons déjà suffisamment de ces systèmes, et le projet de loi C-22 suscite suffisamment de préoccupations. Il s'agirait plutôt de faire de ce système un outil d'autonomisation destiné aux gens et de créer un espace entre l'Internet humain, qui devrait être protégé et contenir l'essentiel de ce que nous aimons du Web, et ce qui pourrait devenir un Internet « mort », où ce sont essentiellement des robots qui interagissent entre eux.

**La sénatrice Arnold :** C'est vraiment intéressant. S'en servent-ils pour voter?

**M. Hatfield :** Il faudrait que je vérifie. Je n'en suis pas sûr.

**La sénatrice Arnold :** Je parlais justement du projet de loi S-5, qui porte sur l'interopérabilité des technologies de l'information sur la santé, et je crois que cela pourrait s'appliquer ici également. C'est une excellente idée. Je serais heureuse de connaître l'une de vos recommandations. Merci.

**M. Hatfield :** Ce qu'il faut retenir, toutefois, c'est que l'identité peut servir à accéder à toutes sortes de choses, et non à recueillir dans leur ensemble toutes les données d'une personne, qui pourrait devenir la cible d'une mauvaise utilisation de ses données.

**Senator Arnold:** Thank you.

**Senator Miville-Dechêne:** Yes. I have a brief question to Mr. Moore. You seem to say that chatbots are not only harmful for children but also for adults. You mentioned different techniques that could help, but would you ban chatbots for kids or minors? I know you are not a legislator, but what is your opinion on that?

**Mr. Moore:** I'm glad that I'm not. You are the experts on these things. But would I ban it for minors? There are many positive uses that we can imagine for kids with chatbots, and my concern is just the kind of "yes to this, no to that" world we can get into with bans. When you think about learning technologies, you think about vulnerable youth who feel that they have some kind of voice. Many people really like chatting with chatbots. You may want to say that they shouldn't like that, but many people really appreciate these kinds of uses. My colleague Desmond has been doing work on empathy as well. Maybe he will want to mention that for a moment.

**Desmond Ong, Assistant Professor, Psychology, University of Texas at Austin, as an individual:** I'm in economic psychology, so I study a lot about how normal people use AI and how they seek out AI for empathy. We're seeing a lot of people — a lot of teens especially, but across the age range — who are turning to AI more. Some of them — I would say maybe even a large portion of them — are benefiting, but what we are finding in our research is that there are a lot of cases in which AI can fail and give poor mental health advice and give the sycophancy response.

One point, just to add to some of the other points on sycophancy earlier, is there is research that came out recently showing that sycophancy does not just affect people with mental health disorders. Everyday people really like people flattering them. I am worried about, for example, teens who are chatting with these chatbots so often. Some of the surveys suggest that half to three quarters of teens are chatting with these chatbots.

How will they develop if they have this bot in their pocket that's always flattering them, always trumping up their self-esteem? When they encounter challenges and setbacks in real

**La sénatrice Arnold :** Merci.

**La sénatrice Miville-Dechêne :** Oui. J'aimerais poser une brève question à M. Moore. Vous semblez dire que les robots conversationnels sont néfastes non seulement pour les enfants, mais également pour les adultes. Vous avez fait mention de différentes techniques qui pourraient aider, mais interdiriez-vous l'utilisation des robots conversationnels par les enfants ou les mineurs? Vous n'êtes pas législateur, mais quelle est votre opinion à ce sujet?

**M. Moore :** Je suis content de ne pas l'être. Vous en êtes les experts. Mais est-ce que je voudrais l'interdire aux mineurs? Comme nous pouvons l'imaginer, les robots conversationnels peuvent offrir de nombreuses utilisations positives pour les enfants, et ce qui me préoccupe, c'est que nous pouvons commencer à dire « oui à ceci, et non à cela » lorsque vient le temps d'établir des interdictions. Lorsqu'on pense aux technologies d'apprentissage, on pense aux jeunes vulnérables qui ont l'impression d'avoir trouvé une façon de s'exprimer. Bon nombre de gens aiment vraiment discuter avec les robots conversationnels. Vous direz peut-être qu'elles ne devraient pas aimer ça, mais nombreuses sont les personnes qui apprécient vraiment ce genre d'utilisations. Mon collègue, M. Ong, a également mené des travaux portant sur l'empathie. Peut-être voudrait-il en parler un peu.

**Desmond Ong, professeur adjoint, Psychologie, Université du Texas à Austin, à titre personnel :** Mon domaine est la psychologie économique, et je fais donc beaucoup de recherches au sujet de la manière dont les gens ordinaires utilisent l'intelligence artificielle et la manière dont ils consultent l'intelligence artificielle à la recherche d'empathie. Nous voyons beaucoup de personnes — beaucoup d'adolescents en particulier, mais également des personnes de toutes les tranches d'âge — qui se tournent de plus en plus vers l'intelligence artificielle. Certaines de ces personnes — je dirais même, peut-être une bonne partie d'entre elles — en bénéficient, mais nous constatons, selon nos recherches, que, dans bien des cas, l'intelligence artificielle peut faire défaut et donner de mauvais conseils de santé mentale et des réponses teintées de complaisance, de flagornerie.

Par ailleurs, simplement pour ajouter aux points qui ont été soulevés précédemment à l'égard de la flagornerie, une recherche qui a été publiée tout récemment indique que la flagornerie ne touche pas uniquement les personnes ayant des troubles de santé mentale. Les gens ordinaires aiment vraiment la flatterie. Je m'inquiète, par exemple, des adolescents qui discutent très souvent avec ces robots conversationnels. Quelques enquêtes indiquent qu'entre la moitié et les trois quarts des adolescents discutent avec les robots conversationnels.

Comment peuvent-ils se développer s'ils ont accès en tout temps à un robot qui les flatte constamment, qui renforce sans cesse leur estime personnelle? Lorsqu'ils feront face à des

life, they might not have learned the requisite skills to be able to handle them. This is not something that we are going to see for 5 or 10 years, right? I keep thinking back to social media. We know so much about social media now, but that is after 10 years or more of these scientific studies. Right now, we are discussing all these laws to regulate social media use, but the harm has already been done to generations of people.

So, with AI, a lot of the evidence of the harms will take time to come out. We cannot just wait for all of that. We need to learn our lessons from social media. We need to learn our lessons from how people interact with technology to pass better legislation.

Coming back to your point, I would really consider a lot of restrictions but maybe not a ban. It has to be a separate product for kids. It has to have a lot more guardrails. Maybe it has to be a separate product that's not trained on — some of the large language models are trained on porn; they are trained on a lot of dark stuff on the internet. If I were to build or think of AI chatbots for children, I think they can definitely be very positive, but we would need to think very hard about regulating them.

**Senator Miville-Dechêne:** On the positive, I didn't quite get when you said. Are they looking for empathy or do they want empathy or are they learning about empathy? You said it can be beneficial. So who is teaching empathy and who is giving empathy there in that conversation?

**Mr. Ong:** What I meant is that a lot of people use their chatbots as their therapists. They wake up at 2 a.m. and have no one to chat with, so they chat with a chatbot. A lot of people say they use it because it is always available, it is free and it never judges.

We have surveys that show that people are turning more to chatbots not just for mental health and therapy — which may be a very small bucket — but just more generally. They might ask, "I had a fight with my significant other. What should I do?"

There's a study that came out in *Science* magazine that shows that when people interact with sycophantic chatbots about relationship conflicts, they end up thinking they were in the right and are less likely to take restorative action to apologize. You

difficultés et aux aléas de la vie, ils n'auront peut-être pas acquis les compétences nécessaires pour pouvoir composer avec eux. Ce n'est pas quelque chose que nous allons constater avant cinq à dix ans, n'est-ce pas? Je pense toujours aux réseaux sociaux. Nous en savons énormément au sujet des réseaux sociaux à l'heure actuelle, mais il a fallu plus de 10 ans d'études scientifiques pour en arriver là. À l'heure actuelle, nous discutons de toutes ces lois visant à réglementer l'utilisation des réseaux sociaux, mais le mal a déjà été fait et touche des générations de personnes.

Donc, pour ce qui est de l'intelligence artificielle, une bonne partie des preuves des préjudices mettront du temps à se révéler. Nous ne pouvons tout simplement pas attendre toutes ces preuves. Nous devons tirer des leçons au sujet des réseaux sociaux. Nous devons tirer des leçons de la manière dont les gens interagissent avec la technologie afin d'adopter de meilleures lois.

Pour en revenir à ce que vous disiez, j'envisagerais vraiment de nombreuses restrictions, mais peut-être pas une interdiction. Il faut qu'un produit distinct soit offert aux enfants. Il faut prévoir beaucoup plus de garde-fous. Il pourrait peut-être s'agir d'un produit distinct qui n'est pas généré par… certains modèles de langage importants sont construits à partir de contenu pornographique; ils sont construits beaucoup à partir de contenus problématiques sur le Web. Si je devais construire ou concevoir des robots conversationnels de l'intelligence artificielle pour les enfants, je crois qu'ils pourraient tout à fait offrir quelque chose de très positif, mais il faudrait que nous envisagions très sérieusement de les réglementer.

**La sénatrice Miville-Dechêne :** Pour ce qui est d'offrir quelque chose de positif, je n'ai pas très bien compris ce que vous avez dit. Sont-ils à la recherche d'empathie ou ont-ils besoin d'empathie ou en apprennent-ils au sujet de l'empathie? Vous avez dit que cela peut être bénéfique. Donc, dans une conversation, qui enseigne l'empathie et qui en fait preuve?

**M. Ong :** Ce que je voulais dire, c'est que bon nombre de personnes utilisent leur robot conversationnel comme thérapeutes. Elles se réveillent en pleine nuit et n'ont personne à qui parler, alors elles discutent avec un robot conversationnel. Beaucoup de personnes disent qu'elles l'utilisent parce que c'est toujours disponible, c'est gratuit, et il n'y a aucun jugement.

Certaines de nos enquêtes montrent que les gens se tournent davantage vers les robots conversationnels non seulement pour discuter de santé mentale et obtenir une thérapie — ce qui n'est sans doute qu'une goutte d'eau dans l'océan —, mais également de manière générale. Elles peuvent demander : « Je me suis disputé avec mon conjoint. Qu'est-ce que je devrais faire? »

Selon une étude qui a été publiée dans le magazine *Science*, lorsque les gens parlent de conflits relationnels avec des robots conversationnels flagorneurs, ils finissent par croire qu'ils ont raison et sont moins susceptibles de poser des gestes pour se

can see that even with these everyday interactions that do not fall under mental health issues, it could have damaging effects, especially over long, sustained use.

**Senator Miville-Dechêne:** Yes, I would believe so, if the chatbot answers, "Not a problem. Let's continue to fight."

[*Translation*]

**Senator Aucoin:** I don't know who to direct my question to, but it's about the media in general. We have seen that since the advent of social media, the era of journalism has been shaken, a lot of media outlets have disappeared and a lot of journalists have lost their jobs.

How could we protect the journalism industry — as I call it — that is, the companies, the media and the very profession of journalism? I feel that, in the future, instead of having someone who works in social media, that person will work with artificial intelligence, and artificial intelligence will become our everyday media. How can we protect this sector?

[*English*]

**Mr. Hatfield:** I will answer that one. People may recall we opposed Bill C-18. We thought it got some matters wrong about how to support journalism. Unfortunately, the reality is that most of these platforms do not really need journalism. They will take accurate journalism if it is available, but they don't necessarily need it to entertain, divert and even inform their users.

We think it is very important that Canada look at a sustainable compensation scheme for journalism across the country. We need to have journalists in every major community, but how to develop an adequate compensation scheme for that is up in the air. Really, it would have been better in many ways to do something like the digital services tax, or DST, a simple flat tax on tech firms spent in part to ensure that journalism was supported.

**Mr. Arnold:** I agree with the compensation piece. But as you think about these challenges, remember that AI is not creating anything new. Some people refer to these as plagiarism machines. What they do is reconstitute in different ways stuff that is on the internet.

réconcilier avec l'autre. On constate que même lorsqu'il s'agit d'interactions quotidiennes qui n'ont rien à voir avec des problèmes de santé mentale, cela peut avoir des effets dommageables, surtout lorsque cette technologie est utilisée de manière prolongée et soutenue.

**La sénatrice Miville-Dechêne :** Oui, je crois bien que c'est possible, si le robot conversationnel répond « Il n'y a aucun problème. Continuons à nous disputer. »

[*Français*]

**Le sénateur Aucoin :** J'ignore à qui adresser ma question, mais elle porte sur les médias en général. Nous avons vu que, depuis l'avènement des médias sociaux, l'ère du journalisme a été ébranlée, beaucoup de médias ont disparu et beaucoup de journalistes ont perdu leur emploi.

Comment pourrait-on protéger l'industrie du journalisme — je l'appelle comme ça —, soit les compagnies, les médias et le métier même de journaliste? J'ai l'impression que, à l'avenir, au lieu d'avoir quelqu'un qui travaille dans les médias sociaux, cette personne va travailler avec l'intelligence artificielle, et l'intelligence artificielle deviendra nos médias de tous les jours. Comment peut-on protéger ce secteur?

[*Traduction*]

**M. Hatfield :** Je vais répondre à cette question. Les gens se souviennent peut-être que nous nous opposions au projet de loi C-18. Nous pensions que le projet de loi présentait des lacunes quant à la manière de soutenir l'industrie du journalisme. Malheureusement, le fait est que la plupart de ces plateformes n'ont pas vraiment besoin du journalisme. Elles utilisent du contenu journalistique fiable lorsqu'il est disponible, mais n'en ont pas nécessairement besoin pour divertir, distraire et même informer leurs utilisateurs.

Nous croyons qu'il est très important que le Canada envisage la mise en place d'un mécanisme de rémunération durable pour les journalistes de tous les pays. Nous avons besoin de journalistes dans toutes les collectivités importantes, mais la manière de concevoir un mécanisme adéquat de rémunération demeure incertaine. En réalité, il aurait été préférable, à bien des égards, de mettre en place quelque chose comme la taxe sur les services numériques, ou la TSN, en imposant aux entreprises de technologie une simple taxe à taux unique qui servirait entre autres à soutenir le journalisme.

**M. Arnold :** Je suis d'accord avec l'idée d'un mécanisme de rémunération. Mais lorsque vous réfléchissez à ces défis, rappelez-vous que l'intelligence artificielle ne crée rien de nouveau. Certains la qualifient de machine à plagiat. Elle se contente de reproduire de différentes manières du contenu déjà présent sur Internet.

So the problem you will have here is people go to it for answers, not news. So they are going to read what they get from that. Journalism, fiction, chats on Reddit — all of that goes into the stew that feeds this, and if we do not have journalists from this country that are well supported and Canadian stories and narratives that go into that mix, when Canadians talk to the chatbots, they will not see their own society reflected back at them.

**Dr. Lin:** I want to add very quickly that we made all the recommendations today, but one of our biggest concerns is that we just don't have enough data or cases for the medical community, certainly, to think about or even understand the risks. We encourage some kind of regulation to open up some transparency or have a third-party regulator able to investigate some of the claims that these private companies are making. Thank you.

**The Chair:** Thank you very much.

On that note, we need to wrap up. Thank you all for participating tonight with us. It was very informative and very helpful as a launching pad as part of our AI study. Thanks again. We really appreciate it.

(The committee adjourned.)

Donc, le problème, c'est que les gens l'utilisent pour obtenir des réponses et non pour s'informer de l'actualité. Ils vont donc lire les réponses qui y sont générées. Le journalisme, la fiction, les discussions sur Reddit… tout cela alimente la machine. Et si les journalistes de notre pays ne sont pas bien soutenus et qu'aucune histoire canadienne n'y est intégrée, les Canadiens qui s'adresseront à ces robots conversationnels n'y verront pas le reflet de leur propre société.

**Dr Lin :** Je voudrais ajouter très rapidement que nous avons présenté toutes les recommandations aujourd'hui, mais l'une de nos principales préoccupations est que nous ne disposons tout simplement pas de suffisamment de données ni d'études de cas pour permettre à la communauté médicale, en tout cas, d'évaluer ou même de comprendre les risques. Nous encourageons l'élaboration d'une réglementation qui assurerait une certaine transparence ou la mise en place d'un organisme tiers de réglementation capable d'enquêter sur des déclarations formulées par les entreprises privées. Je vous remercie.

**Le président :** Merci beaucoup.

Sur ce, nous allons conclure. Merci à tous d'avoir participé à la réunion de ce soir avec nous. La discussion a été très instructive et utile et un bon point de départ pour notre étude sur l'intelligence artificielle. Encore une fois, merci. Nous vous en sommes très reconnaissants.

(La séance est levée.)