

EVIDENCE

OTTAWA, Wednesday, May 6, 2026

The Standing Senate Committee on Social Affairs, Science and Technology met with videoconference this day at 4:13 p.m. [ET] to examine and report on matters related to the impact of artificial intelligence in Canada.

Senator Rosemary Moodie (*Chair*) in the chair.

[*English*]

The Chair: My name is Rosemary Moodie. I'm a senator from Ontario and the chair of this committee.

Before we begin, I would like to ask all senators to consult the cards on the table for guidelines to prevent audio feedback incidents. Please make sure always to keep your earpiece away from the microphones. Do not touch the microphones. Activation and deactivation will be managed by the console operator. Finally, please avoid handling your earpiece while your microphone is on. Earpieces should either remain on the ear or be placed on the designated sticker at each seat. Thank you for your cooperation. Now, I would like to do a round table and have our senators introduce themselves.

Senator Burey: My name is Sharon Burey. Hello and welcome. I'm a senator for Ontario.

Senator Senior: Paulette Senior, senator for Ontario.

[*Translation*]

Senator Boudreau: Hello. Victor Boudreau, New Brunswick.

[*English*]

Senator Arnold: Dawn Arnold, senator from New Brunswick.

[*Translation*]

Senator Petitclerc: Thank you for being here. Chantal Petitclerc, Quebec.

[*English*]

Senator Hay: Hello. Katherine Hay, Ontario.

Senator Cuzner: Rodger Cuzner, Nova Scotia.

Senator Muggli: Tracy Muggli, Saskatchewan, Treaty 6 territory.

TÉMOIGNAGES

OTTAWA, le mercredi 6 mai 2026

Le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie se réunit aujourd'hui, à 16 h 13 (HE), avec vidéoconférence, pour étudier, afin d'en faire rapport, les questions relatives aux répercussions de l'intelligence artificielle au Canada.

La sénatrice Rosemary Moodie (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : Je m'appelle Rosemary Moodie. Je suis sénatrice de l'Ontario et présidente de ce comité.

Avant de commencer, je voudrais demander à tous les sénateurs de consulter les fiches posées sur la table devant eux pour prendre connaissance des consignes visant à prévenir les incidents de rétroaction acoustique. Veuillez vous assurer de tenir votre oreillette en retrait des microphones. Abstenez-vous de toucher aux microphones. Ces derniers seront activés et désactivés par l'opérateur de la console. Enfin, veuillez éviter de manipuler votre oreillette lorsque votre microphone est allumé. Les oreillettes doivent être gardées à l'oreille ou être déposées sur l'autocollant prévu à cette fin correspondant à votre place. Merci de votre coopération. Je voudrais maintenant faire un tour de table et demander à mes collègues de se présenter.

La sénatrice Burey : Je m'appelle Sharon Burey. Bonjour et bienvenue. Je suis une sénatrice de l'Ontario.

La sénatrice Senior : Paulette Senior, sénatrice de l'Ontario.

[*Français*]

Le sénateur Boudreau : Bonjour. Victor Boudreau, du Nouveau-Brunswick.

[*Traduction*]

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

[*Français*]

La sénatrice Petitclerc : Merci d'être là. Chantal Petitclerc, du Québec.

[*Traduction*]

La sénatrice Hay : Bonjour. Katherine Hay, de l'Ontario.

Le sénateur Cuzner : Rodger Cuzner, de la Nouvelle-Écosse.

La sénatrice Muggli : Tracy Muggli, du territoire visé par le Traité n° 6, en Saskatchewan.

The Chair: Today, the committee continues its study on matters relating to the impact of artificial intelligence in Canada. This study will examine issues, including data governance and sovereignty, ethics, privacy, safety, risks, benefits and social impacts of artificial intelligence in Canada.

Before we welcome our witnesses, I'd like to provide a content warning for this meeting. Today, our committee may touch on AI-related online harms. This may be triggering to people in the room with us as well as those watching and listening to the broadcast. Mental health support for all Canadians is available by phone and by text at 988.

Senators and parliamentary employees are also reminded that the Senate's Employee and Family Assistance Program is available to them and offers short-term counselling for both personal and work-related concerns as well as crisis counselling.

I would now like to introduce the witnesses on our first panel: By video conference, Lloyd Richardson, Director of Technology, Canadian Centre for Child Protection; Maria Angelica Quesada, Director of Research and Adult Education, John Humphrey Centre for Peace and Human Rights; by video conference, Tiffany Efird, Project Lead, Youth and Community Engagement; and Divya Sharma, U-Reporter Ambassador, UNICEF Canada. Thank you for joining us today.

For your opening statements, you will have five minutes, followed by questions from committee members. Mr. Richardson, the floor is yours.

Lloyd Richardson, Director of Technology, Canadian Centre for Child Protection: Good afternoon, everyone, and thank you for allowing me to speak today.

My name is Lloyd Richardson, and I am the director of technology for the Canadian Centre for Child Protection.

We operate Cybertip.ca, Canada's national tip line for reporting the online sexual exploitation of children, and we have witnessed firsthand the profound impacts artificial intelligence is having on children across the country.

While the development of AI has delivered some societal benefits, it has also exposed significant safety, regulatory and ethical gaps that directly impact children.

La présidente : Aujourd'hui, le comité poursuit son étude sur les questions relatives aux répercussions de l'intelligence artificielle au Canada. Nous nous pencherons donc sur des enjeux tels que la gouvernance et la souveraineté des données, l'éthique, la protection de la vie privée, la sécurité, les risques, les avantages et l'impact social de l'intelligence artificielle au Canada.

Avant d'accueillir nos témoins, je tiens à vous donner un avertissement concernant le contenu de cette réunion. Aujourd'hui, le comité pourrait aborder la question des préjudices en ligne liés à l'intelligence artificielle. Ce sujet pourrait être une source de détresse pour les personnes qui se trouvent dans la salle avec nous et pour celles qui regardent ou écoutent les délibérations. Un service de soutien en santé mentale est accessible à tous les Canadiens par téléphone et par message texte au 988.

Je rappelle également aux sénateurs et aux employés du Parlement que le Programme d'aide aux employés et à leur famille du Sénat est à leur disposition et offre des services de counselling à court terme pour des problèmes personnels et professionnels et des services de counseling en cas de crise.

Je souhaite maintenant vous présenter les membres de notre premier groupe de témoins : par vidéoconférence, Lloyd Richardson, directeur de la technologie, Centre canadien de protection de l'enfance; Maria Angelica Quesada, directrice de la recherche et de la formation des adultes, Centre John Humphrey pour la Paix et les droits de la personne; par vidéoconférence, Tiffany Efird, responsable de projet, Engagement de la jeunesse et communautaire; et Divya Sharma, ambassadrice U-Reporter, UNICEF Canada. Merci de vous joindre à nous aujourd'hui.

Vous disposerez de cinq minutes pour vos déclarations préliminaires, après quoi les membres du comité vous poseront des questions. Monsieur Richardson, vous avez la parole.

Lloyd Richardson, directeur de la technologie, Centre canadien de protection de l'enfance : Bonjour à tous et merci de me permettre de prendre la parole aujourd'hui.

Je m'appelle Lloyd Richardson et je suis directeur de la technologie du Centre canadien de protection de l'enfance.

Nous gérons Cyberaide.ca, le service pancanadien de signalement des cas d'exploitation sexuelle des enfants en ligne, et nous avons pu constater de nos propres yeux les profondes répercussions de l'intelligence artificielle sur les enfants partout au pays.

Bien que le développement de l'intelligence artificielle ait apporté certains avantages pour la société, il a également mis en évidence d'importantes lacunes en matière de sécurité, de réglementation et d'éthique qui ont une incidence directe sur les enfants.

Our tip line regularly receives reports from children who have had AI-generated “deepfake” images or videos created of them and then indiscriminately shared with students within their school. This is not perpetrated by someone with advanced technical skills or powerful computing resources. It is easily done by a teenager downloading a photo of a peer from social media and feeding it into a “nudifying” app downloaded from an app store. While many of these instances may be intended as a prank, the consequences for the affected youth are devastating.

“Deepfake” imagery is increasingly being used to sexually exploit and harass people, including children. In 2023, Cybertip.ca flagged 4,000 sexually explicit AI-generated images of children. In 2024, we flagged 9,000. In the first quarter of 2025 alone, we flagged 4,000 such images. These figures represent only what we were able to identify with limited resources, and they are only a fraction of what actually exists.

Sexually explicit “deepfakes” are also used by offenders to coerce youth into sending nude images or livestreaming sexual acts. Known as “sextortion,” boys are overwhelmingly extorted for money, while girls are more often extorted for additional sexual images or videos. Whether the victim is a boy or a girl, “sextorters” commonly threaten to share sexually explicit “deepfakes” with the victim’s social media contacts unless their demands are met.

In addition to the outputs of AI models, we also see harm within the training data used to create these models in the first place. Some models are used to support features in applications and research initiatives that have been trained on data collected in ethically questionable ways.

Many image datasets are built by indiscriminately scraping photos and videos from the internet without meaningful review or consent. This lack of due diligence has led to datasets that include not only non-consensual intimate images of adults but also child sexual abuse material.

For example, in 2023, the Canadian Centre for Child Protection assisted Stanford researchers in identifying over 1,000 known child sexual abuse images in the LAION-5B

Notre service reçoit régulièrement des signalements d’enfants qui ont fait l’objet d’images ou de vidéos hypertrucquées générées par l’intelligence artificielle qui ont ensuite été diffusées sans discernement parmi les élèves de leur école. Ces actes ne sont pas commis par des personnes ayant des compétences techniques avancées ou des ressources informatiques puissantes. Il suffit à un adolescent de télécharger une photo d’un camarade qui se trouve sur les réseaux sociaux et de la traiter avec une application de « nudification » téléchargée depuis une boutique d’applications. Bien que bon nombre de ces cas soient sans doute des farces, les conséquences pour les jeunes concernés sont dévastatrices.

Les hypertrucages sont de plus en plus utilisés à des fins d’exploitation et de harcèlement sexuels, y compris à l’encontre d’enfants. En 2023, Cyberaide.ca a signalé 4 000 images sexuellement explicites d’enfants générées par l’intelligence artificielle. En 2024, nous en avons signalé 9 000. Rien qu’au premier trimestre de 2025, nous avons signalé 4 000 images de ce type. Ces chiffres ne représentent que ce que nous avons pu identifier avec des ressources limitées et ils ne constituent qu’une fraction de ce qui existe réellement.

Des hypertrucages sexuellement explicites sont également utilisés par les délinquants pour contraindre des jeunes à envoyer des photos nues ou à diffuser en direct des actes sexuels. Dans le cadre de ce phénomène, qui est connu sous le nom de « sextorsion », les délinquants extorquent de l’argent à la grande majorité des garçons, tandis qu’ils extorquent plus souvent aux filles d’autres images ou des vidéos à caractère sexuel. Que la victime soit un garçon ou une fille, les « sextorqueurs » menacent généralement de diffuser des hypertrucages sexuellement explicites aux personnes que la victime suit sur les réseaux sociaux, à moins que leurs demandes ne soient satisfaites.

En plus de ce qui est généré par les modèles d’intelligence artificielle, nous constatons également des préjudices dans les données d’entraînement utilisées pour créer ces modèles. Certains modèles sont utilisés pour appuyer des fonctionnalités dans des applications et des initiatives de recherche qui ont été entraînées à partir de données recueillies de manière discutable sur le plan éthique.

De nombreux ensembles de données d’images sont créés en copiant sans discernement des photos et des vidéos publiées sur Internet, sans examen approfondi ni consentement. Ce manque de diligence raisonnable a donné lieu à des ensembles de données qui contiennent non seulement des images intimes d’adultes prises sans leur consentement, mais aussi du matériel d’abus pédosexuels.

Par exemple, en 2023, le Centre canadien de protection de l’enfance a aidé des chercheurs de Stanford à identifier plus de 1 000 images d’abus pédosexuels connues dans l’ensemble de

dataset. This dataset has been used to train many popular image-generation tools.

Children are also increasingly engaging with AI chatbot companions. A recent survey found that 72% of teens have used an AI companion, and more than half of these teens were considered “regular” users. In a risk assessment of several popular services, Common Sense Media found the following:

. . . these systems easily produce harmful responses including sexual misconduct, stereotypes, and dangerous ‘advice’ that, if followed, could have life-threatening or deadly real-world impact

Taken together, these harms make one thing clear: Child protection cannot be an afterthought in the development and deployment of artificial intelligence. Without deliberate safeguards, accountability and regulation, the cost of this innovation will be the continued injury of children. That is not acceptable.

Thank you.

The Chair: Thank you, Mr. Richardson. Ms. Quesada, you have the floor.

Maria Angelica Quesada, Director of Research and Adult Education, John Humphrey Centre for Peace and Human Rights: Hello everyone, and thank you, Madam Chair.

The John Humphrey Centre for Peace and Human Rights, or JHC, is a non-profit charitable education organization working to advance justice, dignity, freedom and peace through collaborative relationships and transformative education.

I thank the Standing Senate Committee on Social Affairs, Science and Technology for inviting us to bear witness on the impact of artificial intelligence in Canada. JHC has worked directly with youth, women and gender-diverse people to understand how social media, gaming and generative AI affect historically marginalized communities.

Our focus is on the intersections of online and offline discrimination with the objective of contributing to relevant, applicable frameworks and solutions to challenges that primarily affect young people, whose identities and experiences are shaped by these intersections.

The most relevant challenges we identify are the following: moderation bots that incorporate algorithmic bias in reporting systems that reproduce harm and compromise spaces of

données LAION-5B. Cet ensemble de données a été utilisé pour entraîner de nombreux outils de génération d’images populaires.

Les enfants interagissent également de plus en plus avec des robots conversationnels dotés d’intelligence artificielle. Selon une récente enquête, 72 % des adolescents ont déjà utilisé un compagnon doté d’intelligence artificielle et plus de la moitié d’entre eux étaient considérés comme des utilisateurs « réguliers ». Dans le cadre d’une évaluation des risques liés à plusieurs services populaires, Common Sense Media a constaté ce qui suit :

[...] ces systèmes génèrent facilement des réactions néfastes, notamment des inconduites sexuelles, des stéréotypes et des « conseils » dangereux qui, s’ils étaient suivis, pourraient avoir des conséquences mortelles dans le monde réel [...]

Ensemble, ces préjugés mettent une chose au clair : la protection de l’enfance ne peut pas être reléguée au second plan dans le développement et le déploiement de l’intelligence artificielle. Sans mesures de protection, sans reddition de comptes et sans réglementation, cette innovation continuera à porter préjudice aux enfants. C’est inacceptable.

Merci.

La présidente : Merci, monsieur Richardson. Madame Quesada, vous avez la parole.

Maria Angelica Quesada, directrice de la recherche et de la formation des adultes, Centre John Humphrey pour la Paix et les droits de la personne : Bonjour à tous et merci, madame la présidente.

Le Centre John Humphrey pour la Paix et les droits de la personne est un organisme caritatif sans but lucratif voué à l’éducation qui œuvre à la promotion de la justice, de la dignité, de la liberté et de la paix au moyen de relations collaboratives et d’une éducation transformatrice.

Je remercie le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie de nous avoir invités à témoigner sur les répercussions de l’intelligence artificielle au Canada. Le Centre John Humphrey a travaillé directement avec des jeunes, des femmes et des personnes de diverses identités de genre afin de comprendre les effets des médias sociaux, des jeux vidéo et de l’intelligence artificielle générative sur les communautés historiquement marginalisées.

Nous nous concentrons sur les liens entre la discrimination en ligne et la discrimination hors ligne afin de contribuer à l’élaboration de cadres et de solutions pertinents et applicables aux défis qui touchent principalement les jeunes, dont l’identité et les expériences sont influencées par ces liens.

Les défis les plus pertinents que nous avons identifiés sont les suivants : les robots de modération qui intègrent des partis pris algorithmiques dans les systèmes de signalement qui

remediation; AI-generated text, images and video that erode trust in what we see online and impact civic education and democracy. It is common knowledge now how generative AI is used to create false narratives and “deepfakes” to discredit and control, primarily impacting women, gender-diverse and racialized youth, amplifying their experiences of exclusion and hate that they already experience offline.

In 2025, the Edmonton Police Service alone received 168 “sextortion”-related reports, targeting young people between the ages of 13 and 16 years old, with 15 being the most common age.

AI has significantly lowered the barriers to committing harm through increasing the spread of extremist content and scams that use AI impersonation and coercion.

AI-powered chatbots reinforce negative thought patterns and unhealthy, harmful coping mechanisms. AI-amplified misinformation and disinformation reward outrage and exploit emotions for engagement at an age when emotions are all over our bodies.

Despite this long list of negative impacts and the widespread use of generative AI, from a tool of war to a tool of business efficiency, only a handful of nations have had the capacity or political will to apply some regulatory frameworks that prioritize the protection of people over business models.

While technology advances exponentially, our regulatory frameworks in Canada are lagging, leaving us reacting to international policy development rather than modelling the protections and supports that young people need to navigate safe online spaces with dignity.

The Youth Digital Rights Blueprint, a policy framework published by JHC in collaboration with young people, proposes a comprehensive, human rights-driven digital safety framework built on four interdependent pillars: participation, protection, remedy and support. These reflect youth priorities, international standards, Canada’s obligations under the United Nations’ Convention on the Rights of the Child and *Guiding Principles on Business and Human Rights*.

reproduisent les préjudices et nuisent aux espaces de réparation; les textes, images et vidéos générés par l’intelligence artificielle qui minent la confiance dans ce que nous voyons en ligne et ont un impact sur l’éducation civique et la démocratie. Il est désormais de notoriété publique que l’intelligence artificielle générative est utilisée pour créer de fausses histoires et des hypertrucages visant à discréditer et à contrôler, ce qui touche principalement les femmes, les personnes de diverses identités de genre et les jeunes racisés et amplifie les incidents d’exclusion et de haine qu’ils subissent déjà hors ligne.

En 2025, le service de police d’Edmonton a reçu à lui seul 168 signalements liés à des cas de « sextorsion », dont les victimes étaient des jeunes âgés de 13 à 16 ans, l’âge le plus fréquent étant 15 ans.

L’intelligence artificielle a réduit considérablement les obstacles à la commission d’actes préjudiciables en augmentant la diffusion de contenus extrémistes et d’escroqueries qui recourent à l’usurpation d’identité et à la contrainte via l’intelligence artificielle.

Les robots conversationnels dotés d’intelligence artificielle renforcent les modes de pensée négatifs et les mécanismes d’adaptation malsains et néfastes. La désinformation et la désinformation amplifiées par l’intelligence artificielle récompensent l’indignation et exploitent les émotions pour susciter la participation à une époque où les émotions envahissent tout notre être.

Malgré cette longue liste d’effets négatifs et l’utilisation généralisée de l’intelligence artificielle générative, qu’il s’agisse d’outils de guerre ou d’outils d’efficacité commerciale, seule une poignée de pays ont eu la capacité ou la volonté politique de mettre en place des cadres réglementaires qui privilégient la protection des personnes plutôt que les modèles d’affaires.

Alors que la technologie évolue à un rythme exponentiel, nos cadres réglementaires au Canada accusent un retard, ce qui nous oblige à réagir aux changements de politique internationale au lieu de mettre en place les mesures de protection et de soutien dont les jeunes ont besoin pour utiliser Internet en toute sécurité et dignité.

Le Plan directeur des droits numériques des jeunes, un cadre stratégique publié par le Centre John Humphrey en collaboration avec des jeunes, propose un cadre global de sécurité numérique fondé sur les droits de la personne qui repose sur quatre piliers interdépendants : la participation, la protection, les recours et le soutien. Ces piliers reflètent les priorités des jeunes, les normes internationales, les obligations du Canada au titre de la Convention des Nations unies relative aux droits de l’enfant et les Principes directeurs relatifs aux entreprises et aux droits de l’homme.

The Digital Rights Blueprint provides clear recommendations to the Government of Canada, including the following: a statutory duty of care that requires platforms to proactively assess, prevent and mitigate foreseeable harms; a mandated human rights-based assessment of algorithmic impact for all major online platforms. This assessment should evaluate the effects on mental health and discrimination, especially on historically marginalized communities. It also includes a regulatory framework for generated media with heightened safeguards for exploitative content, extremism and hate. Finally, it includes enforceable national safety standards for interactive digital environments, including online gaming, grooming, peer-to-peer harm, and gambling and gambling-like features that are amplified by algorithmic engagement models.

When addressing the intersection between gender-based violence and AI, the report *Igniting Change on Canada's Action Plan to End Gender-Based Violence*, a two-year research study, clearly reveals how systems of support, policing and reporting mechanisms often ignore “lower-level” threats, intervening only once tech-facilitated harm reaches a crisis point.

The harm produced by the lack of response is amplified when perpetrators are located in different jurisdictions, limiting the capacity to protect.

Let us add one more recommendation. We must build an escalated response system in which no level of threat is tolerated. Legislative responses are not only necessary but urgent, and those must centre on the voices of young people, who have been excluded from policy conversations. So far, they have been tokenized, consulted too late or not at all, even though the decision will have a profound impact on their lives. We call to move away from this systemic exclusion and towards a framework that provides clear, actionable pathways to a safer digital future.

The Chair: Thank you. Ms. Sharma, you have five minutes.

Divya Sharma, U-Reporter Ambassador, UNICEF Canada, as an individual: Good afternoon. Thank you for the opportunity to appear before this committee.

I come from Punjab, India, and I am proud to now call Winnipeg home, the heart of Treaty 1 territory, the traditional lands of the Anishinaabeg, Cree, Oji-Cree, Dakota and Dene Peoples, and the homeland of the Métis Nation.

Le Plan directeur des droits numériques des jeunes formule des recommandations claires à l'intention du gouvernement du Canada, notamment un devoir légal de diligence qui oblige les plateformes à évaluer, prévenir et atténuer de manière proactive les préjudices prévisibles; une évaluation obligatoire fondée sur les droits de la personne des effets algorithmiques sur toutes les grandes plateformes en ligne. Cette évaluation doit examiner les effets sur la santé mentale et la discrimination, en particulier sur les communautés historiquement marginalisées. Il comprend également un cadre réglementaire pour les médias générés, assorti de mesures de protection renforcées contre les contenus découlant de l'exploitation, l'extrémisme et la haine. Enfin, il comprend des normes de sécurité nationales exécutoires pour les environnements numériques interactifs, y compris les jeux en ligne, l'amadouement aux fins d'abus, les préjudices entre pairs, ainsi que les fonctionnalités liées aux jeux de hasard et les fonctionnalités similaires qui sont amplifiées par les modèles de participation algorithmiques.

Lorsqu'il aborde le lien entre la violence fondée sur le sexe et l'intelligence artificielle, le rapport *Allumer le changement dans le Plan d'action national du Canada pour mettre fin à la violence fondée sur le sexe*, qui est le fruit de deux années de recherche, montre clairement comment les systèmes de soutien, les services de police et les mécanismes de signalement négligent souvent les menaces « mineures » et n'interviennent que lorsque les préjudices facilités par la technologie atteignent un point critique.

Les préjudices causés par le manque d'intervention sont amplifiés lorsque les auteurs se trouvent dans différents pays, ce qui limite la capacité à protéger les victimes.

Ajoutons une recommandation supplémentaire. Nous devons mettre en place un système de réponse croissante dans lequel aucun niveau de menace n'est toléré. Des mesures législatives sont non seulement nécessaires, mais urgentes, et elles doivent être axées sur la voix des jeunes, qui ont été exclus des discussions sur les politiques. Jusqu'à présent, ils ont été pris en compte pour présenter une diversité de façade et consultés trop tard ou pas du tout, malgré le fait que les décisions auront un effet considérable sur leur vie. Nous demandons de mettre fin à cette exclusion systémique et d'adopter un cadre qui prévoit des voies claires et concrètes vers un avenir numérique plus sûr.

La présidente : Merci. Madame Sharma, vous disposez de cinq minutes.

Divya Sharma, ambassadrice U-Reporter, UNICEF Canada, à titre personnel : Bonjour. Je vous remercie de m'avoir donné l'occasion de comparaître devant ce comité.

Je suis originaire du Pendjab, en Inde, et je suis fière de vivre désormais à Winnipeg, au cœur du territoire du Traité n° 1, les terres traditionnelles des Anishinabeg, des Cris, des Oji-Cris, des Dakotas et des Dénés, et le territoire de la nation métisse.

My name is Divya Sharma, and I serve as a U-Report ambassador with UNICEF Canada, which is a digital platform for youth that ask polls to get their perspectives on issues and decisions that affect them. It is an opportunity for young people to be a part of change they want to see in Canada and speak out on issues that matter to them.

UNICEF Canada develops poll topics and questions in collaboration with the U-Report Canada steering committee and young ambassadors like me. Previous poll topics have included AI and digital safety as well as mental health and climate change. U-Report Canada is free, confidential and open to anyone aged 13-24.

As a U-Reporter ambassador, I have the privilege of amplifying the voices of thousands of young Canadians in policy spaces like this one. I am here because I believe that AI policy made without young people at the table is an incomplete policy.

Please allow me to share what I have seen. In my student leadership experience, I have sat across from peers who are struggling to put food on the table, working multiple jobs to pay tuition, navigating housing insecurity, and yet, every single one of them has one thing in common: they all have a phone. That's not because it is a luxury, but because, in today's world, it is a lifeline. It is how we access services, search for jobs, connect with family and, increasingly, how we all learn. I don't remember the last time I submitted an essay in hand to a professor.

What is even more important to remember is that AI is woven into technology. According to UNICEF Canada U-Report data, 58% of young Canadians report using AI regularly, either all the time — 12%; once a day — 15%; or a few times a week — 31%. Nearly all youth — 99% — say AI affects what they see online, with 77% saying it does so “a lot.”

As a co-author of a submission to the Schuman Challenge, which is a policy proposal put on by the EU delegation to Canada, I put together a proposal where I had the opportunity to engage with EU officials in Brussels as well as Canada federally, and I have studied the gap closely.

Je m'appelle Divya Sharma et je travaille comme ambassadrice U-Report pour UNICEF Canada. Il s'agit d'une plateforme numérique destinée aux jeunes, sur laquelle ils peuvent répondre à des sondages afin de faire connaître leur avis sur les enjeux et les décisions qui les touchent. C'est l'occasion pour les jeunes de prendre part aux changements qu'ils veulent voir au Canada et de s'exprimer sur les questions qui leur tiennent à cœur.

UNICEF Canada élabore les thèmes et les questions des sondages en collaboration avec le comité directeur d'U-Report Canada et des jeunes ambassadeurs comme moi. Parmi les thèmes abordés lors des sondages précédents, il y a eu l'intelligence artificielle, l'IA, et la sécurité numérique, ainsi que la santé mentale et les changements climatiques. U-Report Canada est un service gratuit, confidentiel et ouvert à toute personne âgée de 13 à 24 ans.

En tant qu'ambassadrice U-Reporter, j'ai le privilège d'être la porte-parole de milliers de jeunes Canadiens dans des espaces politiques comme celui-ci. Je suis ici parce que je crois qu'une politique en matière d'IA élaborée sans la participation des jeunes, c'est une politique incomplète.

Permettez-moi de vous expliquer ce que j'ai pu observer. Au cours de mon expérience de leader étudiante, j'ai rencontré d'autres étudiants qui ont du mal à mettre du pain sur la table, qui ont plus d'un emploi pour payer leurs frais de scolarité, qui font face à l'insécurité en matière de logement, et pourtant, ils ont tous une chose en commun : ils possèdent tous un téléphone. Ce n'est pas parce que c'est un produit de luxe, mais parce que, dans le monde d'aujourd'hui, il s'agit d'une bouée de sauvetage. C'est grâce à cela que nous accédons aux services, que nous cherchons un emploi, que nous restons en contact avec notre famille et, de plus en plus, que nous apprenons tous. Je ne me souviens pas de la dernière fois où j'ai remis un devoir en main propre à un professeur.

Ce qu'il ne faut pas non plus oublier, c'est que l'IA fait partie intégrante de la technologie. Selon les données de l'U-Report d'UNICEF Canada, 58 % des jeunes Canadiens déclarent utiliser l'IA régulièrement, soit tout le temps, à 12 %, une fois par jour, à 15 %, ou plusieurs fois par semaine, à 31 %. Presque tous les jeunes, soit 99 %, affirment que l'IA influence ce qu'ils voient en ligne, et 77 % d'entre eux estiment que cette influence est « importante ».

En tant que co-auteur d'une dissertation au Défi Schuman, c'est-à-dire une proposition de politiques lancée par la délégation de l'Union européenne au Canada, j'ai préparé une proposition qui m'a permis de discuter avec des représentants de l'Union européenne à Bruxelles et les autorités fédérales canadiennes. J'ai donc étudié cet écart de près.

Here is what the evidence shows: Canada ranks forty-fourth out of 47 nations in AI training and literacy, according to a KPMG global AI survey, which was conducted in 2025.

Only 24% of Canadians have received any form of AI training, versus a global average of 39%. Two in three post-secondary students use generative AI for assignments, yet 63% of them are unaware of their institution's policies. This is cited in the Canadian Alliance of Student Associations' data, gathered in 2025.

Canada has invested over \$2 billion in AI research since 2017, and is home to 10% of the world's top-tier AI researchers. Yet, our classrooms have not kept up with this pace.

So, what do we contrast this with? Estonia, which is a country in the EU that has recently implemented the AI Leap program that allows it to rank fifteenth out of 47 nations in AI literacy. It has trained 46% of its population in AI — nearly twice the rate of Canada. It is rolling out AI tools to 20,000 students and 3,000 teachers, starting September 2025, through a national program with OpenAI.

This policy proposal shared three coordinated actions. First, a Canada-EU-Estonia AI literacy task force to assess institutional AI readiness and build evidence-based frameworks.

Second, standardized educator AI certification programs so teachers are well equipped to guide, but not penalize, students for using AI because AI is here and here to stay. So how do we make sure ethical guidelines are in place to support students?

Third, AI research and student exchange initiatives allow for the bridging of academic research and real-world AI application.

In closing, I would like to say that AI, at the end of the day, is a tool, and that's not inherently good or bad. Like electricity, like the printing press, like the internet before it, what matters is not the technology itself, but whether the people using it have the knowledge, the capacity and the agency to shape it for the public good.

Voici ce que démontrent les données : selon un sondage sur l'IA mené en 2025 dans le monde entier par KPMG, sur 47 pays, le Canada se classe au 44^e rang en matière de formation et de littératie sur l'IA.

Seulement 24 % des Canadiens ont suivi une formation, quelle qu'elle soit, sur l'IA, comparativement à une moyenne mondiale de 39 %. Deux étudiants de niveau postsecondaire sur trois utilisent l'IA générative pour leurs travaux, alors que 63 % d'entre eux ne connaissent pas les politiques de leur établissement d'enseignement. Ces chiffres proviennent des données recueillies en 2025 par l'Alliance canadienne des associations étudiantes.

Depuis 2017, le Canada a investi plus de 2 milliards de dollars dans la recherche dans le domaine de l'IA et accueille 10 % des meilleurs chercheurs au monde dans ce domaine. Pourtant, nos salles de classe ne se sont pas adaptées.

Alors, à quoi peut-on comparer cela? À l'Estonie, un pays membre de l'Union européenne qui a récemment mis en place le programme « AI Leap », ce qui lui a permis de se classer au quinzième rang sur 47 pays en matière de littératie sur l'IA. Le pays a donné une formation sur l'IA à 46 % de sa population, ce qui représente presque deux fois le taux du Canada. Depuis septembre 2025, dans le cadre d'un programme national mené en collaboration avec OpenAI, l'Estonie déploie des outils d'IA auprès de 20 000 élèves et de 3 000 enseignants.

Cette proposition de politique prévoyait trois mesures concertées. Premièrement, la création d'un groupe de travail Canada-UE-Estonie sur la littératie en matière d'IA, chargé d'évaluer l'état de préparation des institutions en matière d'IA et d'élaborer des cadres fondés sur des données probantes.

Deuxièmement, il faut mettre en place des programmes de certification standardisés en matière d'intelligence artificielle pour les éducateurs, afin que ceux-ci soient bien outillés pour guider l'utilisation de l'intelligence artificielle par leurs élèves, sans pour autant les pénaliser, car l'intelligence artificielle existe et elle est là pour de bon. Donc, comment pouvons-nous nous assurer que des lignes directrices éthiques sont en place pour soutenir les élèves?

Troisièmement, la recherche en intelligence artificielle et les programmes d'échange d'étudiants permettent de créer un pont entre la recherche universitaire et les applications concrètes de l'IA.

En conclusion, je voudrais dire que l'intelligence artificielle, au final, n'est qu'un outil, et qu'elle n'est ni bonne ni mauvaise en soi. Tout comme l'électricité, la presse à imprimer ou encore l'Internet avant l'intelligence artificielle, ce qui importe, ce n'est pas la technologie en soi, mais que ceux qui l'utilisent possèdent les connaissances, les capacités et les pouvoirs d'action nécessaires pour la mettre au service du bien commun.

Right now in Canada, too many young people and too many vulnerable populations are interacting with AI every single day without the literacy to understand what it is doing to them, to their data and to their futures.

The Chair: Thank you very much, Ms. Sharma.

We will proceed now to questions from committee members. For this panel, senators will have four minutes for your question, and that includes the answer.

Please indicate if your question is directed to a particular witness or all witnesses.

Senator Burey: Welcome everyone. Thank you for being here and sharing your expertise.

I have to start by saying, I'm a behavioural pediatrician doing mental health. I saw the writing on the wall, honestly, a decade ago, and we're here now. I go back to what Mr. Richardson said: Child protection can't be an afterthought.

Since I want all of you to answer, I'm just going to cut to this topical question. As you know, as of December 2025, Australia became the first country to implement age-related social media restrictions as a means of mitigating online harms. Since then many other jurisdictions have started exploring this in Canada, most recently, Manitoba.

Can you each comment on your opinion on this age or other population-related restrictions? Let's have all three of you comment on that. Let's start with Mr. Richardson.

Mr. Richardson: All right. Thank you for the question. I could probably go on for quite a while about the age-related delays in social media, but I'll try and limit it.

I think that's quite astute to associate that particular topic to AI because there is quite an interesting cross-section there. When we talk about AI specifically, it's a diverse set of things; it is not one simple thing.

While there might be some AI tools that are appropriate for certain age categories, there are certainly AI tools that are absolutely not and would fall into some of the same issues that we see, particularly with social media.

Au Canada, trop de jeunes et de personnes issues de groupes vulnérables entrent quotidiennement en contact avec l'intelligence artificielle sans avoir les connaissances requises pour comprendre l'impact qu'elle a sur eux, sur leurs données et sur leur avenir.

La présidente : Merci beaucoup, madame Sharma.

Nous passons maintenant aux questions des membres du comité. Les sénateurs disposeront de quatre minutes pour poser leurs questions à ce groupe de témoins. Ce délai inclut les réponses.

Veuillez préciser si votre question s'adresse à un témoin en particulier ou à l'ensemble des témoins.

La sénatrice Burey : Bienvenue à tous. Je vous remercie d'être présents et de nous faire profiter de votre expertise.

Pour commencer, je dois préciser que je suis médecin en pédiatrie comportementale spécialisée en santé mentale. Pour être honnête, j'avais déjà pris conscience de la situation il y a dix ans, et voilà où nous en sommes aujourd'hui. Je reviens sur ce qu'a dit M. Richardson : la protection de l'enfance ne peut pas être une considération secondaire.

Comme je veux que vous répondiez tous, je vais aller droit au but et pour ma question on ne peut plus d'actualité. Comme vous le savez, en décembre 2025, l'Australie est devenue le premier pays à mettre en place des restrictions d'accès aux réseaux sociaux liées à l'âge afin de limiter les préjudices en ligne. Depuis, de nombreuses autres administrations canadiennes ont commencé à s'intéresser à cette question, la dernière étant le Manitoba.

Pourriez-vous tous nous donner votre avis sur cette restriction liée à l'âge ou sur d'autres restrictions concernant la population? J'aimerais que vous commentiez tous les trois. Commençons par M. Richardson.

M. Richardson : Très bien. Merci de la question. Je pourrais sans doute parler longtemps des retards concernant l'utilisation des réseaux sociaux selon l'âge, mais je vais essayer de faire court.

Je trouve que c'est très habile de faire le lien avec cet aspect précis de l'intelligence artificielle, car il y a là un recoupement assez intéressant. Quand on parle spécifiquement d'intelligence artificielle, on fait référence à un ensemble très varié de domaines. Ce n'est pas une seule chose.

Bien que certains outils d'intelligence artificielle conviennent peut-être à certaines tranches d'âge, il en existe certainement d'autres qui ne sont absolument pas appropriés et qui poseraient les mêmes problèmes que ceux que l'on observe, surtout sur les réseaux sociaux.

A logical approach or a child-safety approach to this, in terms of creating age-verification mechanisms for certain types of AI, much like we would strongly advocate for, related to social media, would be absolutely prudent in the protection of children.

Senator Burey: Thank you. Ms. Quesada.

Ms. Quesada: There are three things we have heard from young people. First, they don't trust their personal data to social media; they know of leaks that have happened with age verification and IDs, and they are really scared of entrusting their IDs to those platforms.

Second, we cannot expect that, at the age of 16 or 18, or whatever the age is, if we don't train them, they are going to be ready to go into social media, even if they are allowed to at a certain age.

Third, why don't we regulate businesses rather than leave users to have the responsibility of individually regulating themselves? Safety for all in the business model rather than the individual.

Senator Burey: Thank you.

Ms. Sharma: Thank you very much for your question, senator.

As a proud Manitoban, I have to say what we're seeing as young people, in terms of the policy that our government recently implemented, there's been a lot of positive feedback.

In our schools, we also have a school overall phone ban that's allowed students to start interacting more face-to-face and allows them to learn.

Like I said, through U-Report we just completed a poll on May 4 that allowed us to assess how young people are feeling about AI legislation. Surprisingly, or unsurprisingly, a lot of young Canadians actually do want to see robust intervention from governments to keep up with technology that is rapidly changing. So we need equally robust legislation that keeps up.

Policies should also be age appropriate by design. So, of course, these standards need to be set to support not only young people but also parents, caregivers and educators with resources to guide children's engagement with AI and technology as a whole, while investing in research to better understand the long-term impacts of development and well-being.

En ce qui concerne la mise en place de mécanismes de vérification de l'âge pour certains types d'intelligence artificielle, à l'instar de ce que nous préconisons vivement pour les réseaux sociaux, il serait très sage d'avoir une approche rationnelle ou axée sur la sécurité des enfants dans ce dossier afin d'assurer la protection des enfants.

La sénatrice Burey : Merci. Madame Quesada, vous avez la parole.

Mme Quesada : Les jeunes nous ont fait part de trois préoccupations. Premièrement, ils ne font pas confiance aux réseaux sociaux pour gérer leurs renseignements personnels. Ils ont entendu parler de fuites par rapport à la vérification de l'âge et aux pièces d'identité et ils ont très peur de confier leurs pièces d'identité à ces plateformes.

Deuxièmement, on ne peut pas s'attendre à ce qu'à 16 ou 18 ans, peu importe l'âge, ils soient prêts à utiliser les réseaux sociaux s'ils n'y ont pas été formés, et ce, même s'ils y sont autorisés à partir d'un certain âge.

Troisièmement, pourquoi ne réglementons-nous pas les entreprises plutôt que d'imposer aux utilisateurs la responsabilité de se réguler individuellement? La sécurité de tous doit être au cœur du modèle de l'entreprise; elle ne doit pas reposer sur chaque individu.

La sénatrice Burey : Merci.

Mme Sharma : Merci beaucoup de votre question, sénatrice.

En tant que fière Manitobaine, je dois dire que, du point de vue des jeunes, la politique que le gouvernement provincial a récemment mise en place a suscité de nombreux commentaires positifs.

À l'école, il y a une interdiction générale de l'utilisation des téléphones, ce qui a permis aux élèves de commencer à interagir plus souvent en personne et de mieux apprendre.

Comme je l'ai dit, le 4 mai, nous avons mené, par l'entremise de U-Report, un sondage qui nous a permis de déterminer ce que les jeunes pensent de la loi relative à l'intelligence artificielle. Fait surprenant, ou non, beaucoup de jeunes Canadiens souhaitent en réalité que les gouvernements interviennent de manière énergique pour rester en phase avec cette technologie qui évolue rapidement. Nous avons donc besoin de mesures législatives tout aussi musclées et qui demeurent pertinentes.

Les politiques doivent aussi être adaptées en fonction de l'âge. Donc, ces normes doivent forcément être établies de manière à appuyer non seulement les jeunes, mais aussi les parents, les proches et les éducateurs, en leur fournissant des ressources pour guider l'interaction des enfants avec l'intelligence artificielle et les technologies en général, tout en investissant dans la recherche

Senator Hay: I hope I get to a question after four minutes.

Thank you all for being here. You are the people who are really important to speak to as we grapple with this.

In my former life, I worked in a youth mental health organization that worked in a digital environment using AI. Doing nothing is actually an action. AI is well out of the gate, and it's not going to go away. We just can't sit on the sidelines and hope. So your input is super important.

One of the things that we know is that young people are using it, and they're not afraid of it, actually. They're even willing to give up their own data for something, like Uber Eats. They're quite comfortable in that environment, so it's really a dilemma.

So my question is going to be around balance. In my former world, we understood the need to put young people at the decision-making table and build systems where young people will be, even if we were uncomfortable, like in the dark web, or on pornography sites or gaming sites, or whatnot.

So my question, I guess, for all of you is piggybacking on Senator Burey. We can't geofence, really, and so where does the accountability lie? We ask young people to put their data in to restrict them from getting access; it just gives their data to mega companies.

How do we, in your opinion, hold the "Metas" of the world accountable: these multi-trillion-dollar corporations and governments? One thing each, two minutes.

Ms. Sharma: I could start with that question. I think that's a very broad question. It definitely puts things into perspective.

So, firstly, I would like to see — and just to my point and what I said in my opening remarks, I think what's really key is digital literacy. Once young people become digitally literate — and not just young people, vulnerable populations who oftentimes do need to access supports from government or different services, really understanding when something says, "Do you understand the terms and conditions?" What does the fine print actually mean?

afin de mieux comprendre les effets à long terme sur leur développement et leur bien-être.

La sénatrice Hay : J'espère avoir le temps de poser une question au bout de quatre minutes.

Je vous remercie d'être venus ici aujourd'hui. C'est à vous qu'il est réellement important de parler alors que nous nous penchons sur cette question.

Dans une autre vie, je travaillais pour un organisme dédié à la santé mentale des jeunes qui utilisait un environnement numérique propulsé par l'intelligence artificielle. Choisir de ne rien faire, c'est aussi faire un choix. L'intelligence artificielle est déjà sortie de la boîte, et elle ne disparaîtra pas. On ne peut tout simplement pas rester à l'écart et se croiser les doigts. C'est pourquoi votre contribution est extrêmement importante.

On sait notamment que les jeunes l'utilisent, et qu'en réalité, ils n'en ont pas peur. Ils sont même prêts à céder leurs renseignements personnels pour certains services, comme Uber Eats. Ils sont tout à fait à l'aise dans cet environnement, ce qui pose un véritable dilemme.

Ma question porte donc sur l'équilibre à trouver. Là où je travaillais auparavant, nous comprenions qu'il faut impliquer les jeunes dans les prises de décision et mettre en place des systèmes où ils seraient présents, même si cela nous mettait mal à l'aise, que ce soit sur le Web caché, sur des sites pornographiques, sur des sites de jeux vidéo, etc.

Donc, ma question fait en quelque sorte suite à celle de la sénatrice Burey. Nous ne pouvons pas vraiment faire de géorepérage. Alors qui est responsable? Nous demandons aux jeunes de fournir leurs renseignements personnels pour les empêcher d'accéder à certains contenus. Cette méthode ne fait que fournir leurs renseignements aux géants du numérique.

À votre avis, comment pouvons-nous exiger des comptes aux « Metas » de ce monde, c'est-à-dire aux entreprises qui valent plusieurs milliards de dollars et aux gouvernements? J'aimerais avoir une suggestion par personne, en deux minutes.

Mme Sharma : Je pourrais commencer par cette question. Je pense que c'est une question très large. Cela met clairement les choses en perspective.

Tout d'abord, pour revenir à mon propos et à ce que j'ai dit dans mon introduction, je pense que, ce qui est vraiment essentiel, c'est la culture numérique. Une fois que les jeunes ont acquis cette culture numérique — et pas seulement les jeunes, mais aussi les populations vulnérables qui ont souvent besoin d'accéder à l'aide de l'État ou à divers services —, ils sont alors en mesure de comprendre quand on leur demande d'accepter les conditions d'utilisation ou de lire ce qui est écrit en petits caractères.

The way for us to achieve that, in order for us to get to that level, we have to make sure that young people are being trained in terms of digital literacy at a very young age.

One thing I will also add is that, when we look at schools and even universities and so on and so forth, we have to think about who the populations are that are attending schools, public schools and so on. There are a number of young people who only have access to technology once they get to school. We don't know what young people do after they are not in school. We can't regulate that. We are oftentimes seeing that young people are going to AI to put their information there, and these are models that are then used for training to extract — to your point — human data.

How do we ensure that there are more mental health supports available so that young people can actually access talking one-on-one to a human rather than a machine at the end of the day? How do we ensure we foster those in-person connections? Again, that question that I answered earlier in respect to the phone ban or the social media ban that Manitoba has implemented is definitely one step towards doing that to really ensure that there are guidelines and supports available.

Senator Arnold: Thank you all for being here. Fascinating information. Mr. Richardson, I heard you on CBC this morning. Excellent interview. Super concerning, though.

You told a story about something that you had found, and we have been hearing lots of evidence from government officials that everything we have is okay, and we just haven't really used some of the legislation we have in place.

You made a point with one of the situations you had seen, which was Telegram, and you had to go to the U.K. because we don't have an online safety watchdog, and police can't seem to cope with all of this.

What would you recommend we do in Canada from this perspective?

Mr. Richardson: That's a really big question. The start of it, I would suggest, is online harms legislation and a regulator. What people sort of miss here is that everything is codified in criminal law, and we can deal with companies on the internet based on what we see in criminal law, which is a far move from what you would see with a regulator who has abilities to fine and set rules related to what these companies actually do.

Pour y parvenir, pour atteindre ce niveau, nous devons faire en sorte que les jeunes acquièrent des compétences numériques dès leur plus jeune âge.

J'ajouterai également ceci : quand on examine les écoles, et même les universités, etc., il faut réfléchir à la composition des populations qui fréquentent ces établissements, que ce soit les écoles publiques ou autres. De nombreux jeunes n'ont accès à la technologie qu'une fois arrivés à l'école. Nous ne savons pas ce que font ces jeunes en dehors des heures de cours. Nous ne pouvons pas réglementer cela. Nous observons souvent que les jeunes utilisent l'intelligence artificielle et qu'ils y mettent leurs informations, et ils servent de modèles pour former des systèmes à extraire — comme vous le soulignez — des données humaines.

Comment pouvons-nous faire en sorte qu'il y ait davantage de services de soutien en santé mentale disponibles, afin que les jeunes puissent, en fin de compte, s'entretenir en tête-à-tête avec quelqu'un plutôt qu'avec une machine? Comment pouvons-nous veiller à favoriser ces liens en face-à-face? Encore une fois, la réponse que j'ai donnée tout à l'heure concernant l'interdiction des téléphones ou des réseaux sociaux mise en place par le Manitoba constitue sans aucun doute un pas dans cette direction, pour garantir réellement la mise en place de lignes directrices et de mesures de soutien.

La sénatrice Arnold : Merci à tous d'être ici. Ces renseignements sont fascinants. Monsieur Richardson, je vous ai entendu ce matin sur CBC. C'était une excellente entrevue. C'est toutefois très inquiétant.

Vous avez raconté une histoire à propos de quelque chose que vous aviez découvert. Nous avons entendu de nombreux témoignages de la part de responsables gouvernementaux qui affirment que tout ce que nous avons est suffisant, et que nous n'avons tout simplement pas encore utilisé certaines dispositions législatives déjà en vigueur.

Vous avez soulevé un point important en évoquant l'une des situations que vous aviez observées, à savoir Telegram, et vous avez dû vous tourner vers le Royaume-Uni parce que nous n'avons pas d'organisme de surveillance de la sécurité en ligne et que la police ne semble pas en mesure de gérer tout cela.

Dans cette perspective, que nous recommanderiez-vous de faire au Canada?

M. Richardson : C'est une question vraiment vaste. Je dirais qu'il faut commencer par légiférer sur les préjudices en ligne et mettre en place un organisme de réglementation. Ce que les gens ont tendance à oublier, c'est que tout est déjà prévu dans le droit pénal, et que nous pouvons agir à l'encontre d'entreprises sur Internet en nous appuyant sur les dispositions pénales existantes, ce qui est très différent de ce que pourrait faire un organisme de réglementation doté du pouvoir d'imposer des amendes et d'établir les règles du jeu pour ces entreprises.

In terms of what we're talking about, in that particular case, with a company like Telegram that's based in the United Arab Emirates and that's run by a Russian fellow, what are we doing in Canada to institute sovereign rules that are actually applicable to these companies? The answer to that is not necessarily the Criminal Code. That is a regulatory approach that's enforceable in Canada.

Pivoting on this, I wanted to switch back to one of the previous questions related to how we implement this to protect children in these spaces.

There's a lot of misinformation going on about how I have to give ID to these big companies. There are absolutely privacy-preserving ways to prove you're of a certain age. It's a little bit of a misnomer when people start talking about handing over ID to these companies. I find that particular argument concerning, given that these companies already have the personal information of not only 13- to 15-year-olds but also 8- to 13-year-olds that they are not supposed to have at all.

When we start bringing up, "I'm worried about giving ID to one of these companies," they have already done that. The ship has left the harbour here. That argument doesn't hold any water.

Senator Arnold: It comes up over and over again as far as the fact that we have these laws. It seems like there is such a gap, and people don't know what to do or where to go.

I would argue that it shouldn't be done on the backs of a non-profit like you exclusively. That's a pretty big burden for you to carry.

My next question is on the education aspect. We are a very progressive country. We have all this expertise and all of this research. Why do you think we haven't embraced AI literacy?

Ms. Sharma: Thank you for that question. I'm wondering the same thing. With regard to the EU, and specifically Estonia, their platform actually offers a huge amount of support for teachers and professors — so that's educators. That's really key here. Sometimes what we're hearing even from educators is that they don't feel safe or empowered enough to start teaching these tools. We have to keep that in mind.

Additionally, the EU has this Digital Services Act. It's called the DSA. It empowers citizens, teaches day-to-day citizens about AI, and, to an earlier point, if there is a company that is in breach of that particular act, sometimes will say, "We will fine you 'x' amount of thousands of dollars." It says they will take a percentage of their profits, and that percentage is very, very high. Again, that money, what they collect, is used to actually

En ce qui concerne le sujet dont nous parlons, dans ce cas précis, avec une entreprise comme Telegram, basée aux Émirats arabes unis et dirigée par un Russe, que faisons-nous au Canada pour mettre en place des règles souveraines qui s'appliquent réellement à ce type d'entreprises? La réponse à cette question ne réside pas nécessairement dans le Code criminel. Il s'agit d'une approche réglementaire exécutoire au Canada.

Pour rebondir là-dessus, je voudrais revenir sur l'une des questions précédentes concernant la manière de mettre ces choses en œuvre pour protéger les enfants dans ces environnements.

Il y a beaucoup de désinformation sur la nécessité de fournir une pièce d'identité aux grandes entreprises. Il existe bel et bien des moyens de prouver son âge tout en protégeant sa vie privée. C'est un peu un abus de langage quand les gens parlent de « remettre » une pièce d'identité à ces entreprises. Je trouve cet argument particulièrement préoccupant, étant donné que ces entreprises détiennent déjà les renseignements personnels non seulement de jeunes de 13 à 15 ans, mais aussi de jeunes de 8 à 13 ans, qu'elles ne sont absolument pas censées détenir.

Quand on commence à dire qu'on s'inquiète de remettre ses données personnelles à ces entreprises, eh bien, elles les ont déjà. Il est bien trop tard. Cet argument ne tient pas la route.

La sénatrice Arnold : On revient sans cesse sur le fait que nous avons les lois qu'il faut. Il semble y avoir un tel décalage que les gens ne savent pas quoi faire ni vers qui se tourner.

Je dirais qu'on ne devrait pas faire porter tout ce poids exclusivement à une association à but non lucratif comme la vôtre. C'est une charge bien trop lourde à assumer pour vous.

Ma question suivante porte sur l'aspect éducatif. Nous sommes un pays très progressiste. Nous avons tout ce savoir-faire et toutes ces recherches. Pourquoi pensez-vous que nous n'avons pas encore adopté la culture de l'intelligence artificielle?

Mme Sharma : Je vous remercie de votre question. Je me pose la même question. En ce qui concerne l'Union européenne, et plus particulièrement l'Estonie, sa plateforme offre un soutien considérable aux enseignants et aux professeurs — c'est-à-dire aux professionnels de l'éducation. C'est un point essentiel. Parfois, même les professionnels de l'éducation nous confient qu'ils ne se sentent pas suffisamment en confiance ou autonomes pour commencer à enseigner l'utilisation de ces outils. Nous devons garder cela à l'esprit.

Par ailleurs, l'Union européenne a adopté sa législation sur les services numériques. Il s'agit d'un document appelé Règlement sur les services numériques. Il renforce les droits des citoyens, sensibilise le grand public à l'intelligence artificielle et, comme j'en ai parlé tout à l'heure, prévoit que si une entreprise commet une infraction, elle s'expose à une amende de plusieurs milliers de dollars. Le règlement prévoit également le prélèvement d'un

reinforce some of these services that they offer through the Digital Services Act.

Senator Arnold: That's great. Thank you.

Senator Senior: I'm intrigued by Senator Hay's "geofence" term, because I'm really wondering what possibility there is, provincially, because provinces seem to be leading the way, putting a geofence around the use of AI by young people, considering the seeming challenge in Australia and whether or not that's even possible.

I will ask you, Ms. Quesada, that particular question, and then I have a question for Mr. Richardson.

Ms. Quesada: I will let my co-worker Tiffany answer that question.

Tiffany Efir, Project Lead, Youth and Community Engagement, John Humphrey Centre for Peace and Human Rights: Thank you so much. In terms of geofencing, we have seen some considerable struggle with that on the international scale. Going back to talk about Australia paving the way for that ban, we are already seeing youth get around that quite easily, whether it's through the use of VPNs or some other mechanism. I read an article earlier today talking about how youth were putting on fake moustaches to get around digital age verification.

Part of the problem with leading into, "Okay, we have to do this ban. This is the only outcome for us. We have to geofence around this," is people will get through. They find lots and lots of ways to get through. The question becomes, do we continue to regulate other things? Do we start to regulate VPNs and things like that? How far do we want to infringe on the privacy of individuals?

It's not that I don't think that there is some sort of protection needed. I feel that we have to go towards looking at the regulations on corporations and on businesses, rather than trying to police individuals first — to refocus the attention there.

Senator Senior: Thank you.

Mr. Richardson, do you think it is possible for there to be AI for good when it comes to young people? Can AI actually be used for good with young people? I may ask Ms. Sharma that same question.

pourcentage de ses profits, et ce pourcentage est extrêmement élevé. Une fois de plus, cet argent perçu sert à renforcer certains des services fournis sous le régime du Règlement sur les services numériques.

La sénatrice Arnold : Super. Merci.

La sénatrice Senior : Je suis intriguée par le « géorepérage » dont a parlé la sénatrice Hay. Je me demande vraiment quelles sont les possibilités à l'échelle provinciale, car les provinces semblent montrer la voie en utilisant le géorepérage pour encadrer l'utilisation de l'intelligence artificielle par les jeunes, compte tenu des difficultés apparentes rencontrées en Australie et de la question de savoir si cela est même possible.

Cette question était pour vous, madame Quesada. Ensuite, j'ai une question pour M. Richardson.

Mme Quesada : Je vais laisser ma collègue Tiffany Efir répondre à cette question.

Tiffany Efir, responsable de projet, Engagement de la jeunesse et communautaire, Centre John Humphrey pour la Paix et les droits de la personne : Merci beaucoup. En ce qui concerne le géorepérage, nous avons constaté des difficultés considérables à l'échelle internationale. Pour revenir sur le fait que l'Australie a ouvert la voie à cette interdiction, nous constatons déjà que les jeunes contournent cette mesure assez facilement, que ce soit en utilisant des réseaux privés virtuels ou d'autres moyens. J'ai lu un article ce matin qui expliquait que certains jeunes se mettaient de fausses moustaches pour contourner la vérification numérique de l'âge.

Le problème, quand on décide qu'il faut imposer une interdiction, que c'est la seule chose à faire et qu'il faut utiliser le géorepérage, c'est que les gens trouveront toujours le moyen de contourner ces mesures. Ils trouvent toujours une multitude de façons de le faire. La question qui se pose alors est la suivante : faut-il aller plus loin et réglementer d'autres éléments? Allons-nous commencer à réglementer les réseaux privés virtuels, par exemple? Jusqu'où voulons-nous empiéter sur la vie privée des gens?

Ce n'est pas que je ne pense pas qu'une certaine forme de protection soit nécessaire. Je pense simplement qu'il faut se concentrer davantage à réglementer les entreprises plutôt que d'essayer en premier lieu de contrôler les particuliers. C'est là qu'il faut recentrer notre attention.

La sénatrice Senior : Merci.

Monsieur Richardson, pensez-vous qu'il soit possible de mettre l'intelligence artificielle au service du bien lorsqu'il s'agit des jeunes? L'intelligence artificielle peut-elle réellement être utilisée à bon escient auprès des jeunes? Je poserai peut-être cette même question à Mme Sharma.

Mr. Richardson: Yes, absolutely. I did touch on that a little bit in my opening statement that it's not all doom and gloom with AI.

Certainly, there are a lot of possibilities there in terms of education that we can see with youth and what have you, and that's all fine and good, but before we look at the benefit side of it, we need to look at the safety side of things. As we do with anything in the brick-and-mortar world, we ensure something is safe. We don't turn it into an experiment with children, create a bunch of harms, and then throw our arms up in the air and say, "Well, who could have known?" It seems like we've inverted everything in the digital world, where we accept harm and attempt to deal with it later, which is exactly what we're doing with the whole advent of social media. It's ridiculous.

Senator Senior: Ms. Sharma, have you seen examples where it's been used for good?

Ms. Sharma: Yes, thank you so much for your question, senator.

Oftentimes we ask young people: What do you want to be when you're older? And that question has been asked for decades. With AI, the opportunity really here is to ask: What would you like to solve? What AI actually does is that it gives you a platform to build on a number of different questions.

An 8-year-old, if they wanted to look at solving cancer, doing cancer research, they have so much data right in front of them.

Senator Senior: Have you seen examples?

Ms. Sharma: Have I seen real-life examples?

Senator Senior: Yes.

Ms. Sharma: Assignments are an example. AI does allow you to do research more promptly. Of course, you have to double-check everything and all the data, but does it allow you to consolidate it very fast? Absolutely. Does it allow you to analyze information very fast? Absolutely. There are certain apps that can manage your calendars, for example. Of course, you're giving that data away, but can it be used to organize and consolidate data? Yes, it can.

Senator Muggli: I will try to get everybody in, but I have two comments I want to make to get your reactions.

The first is that I was speaking recently at a conference related to predictors of youth violence. A young presenter surveyed 2,000 youth and found that 49% of them had a chatbot friend that they relied on for emotional support. That's 1,000 out of 2,000.

M. Richardson : Oui, tout à fait. Comme j'en ai brièvement parlé dans ma déclaration liminaire, il ne faut pas voir l'intelligence artificielle uniquement sous un jour sombre.

Certes, il y a beaucoup de possibilités en matière d'éducation pour les jeunes et tout le reste, et c'est très bien. Toutefois, avant de nous pencher sur les avantages, nous devons examiner la question de la sécurité. Comme nous le faisons pour tout ce qui se passe dans le monde réel, nous devons nous assurer qu'il n'y a pas de danger. Nous ne devons pas transformer la situation en une expérience sur les enfants, causer tout un tas de problèmes, puis finir par hausser les épaules en disant qu'il était impossible de savoir. On dirait que nous avons tout inversé dans le monde numérique. Nous acceptons les problèmes et nous espérons les régler plus tard. C'est exactement ce que nous faisons avec l'avènement des réseaux sociaux. C'est ridicule.

La sénatrice Senior : Madame Sharma, avez-vous vu des exemples où cela a été utilisé à bon escient?

Mme Sharma : Oui, je vous remercie de votre question, sénatrice.

On demande souvent aux jeunes : « Que veux-tu faire plus tard? » Cette question se pose depuis toujours. Avec l'intelligence artificielle, on peut désormais leur demander : « Quel problème aimerais-tu résoudre? » En effet, l'intelligence artificielle offre une plateforme qui permet d'aborder toute une série de questions différentes.

Un enfant de 8 ans qui souhaiterait s'intéresser à la lutte contre le cancer ou à la recherche sur le cancer dispose d'une multitude de données à portée de main.

La sénatrice Senior : Avez-vous vu des exemples?

Mme Sharma : Si j'ai vu des exemples dans la vraie vie?

La sénatrice Senior : Oui.

Mme Sharma : Prenons l'exemple des devoirs. L'intelligence artificielle permet d'effectuer des recherches plus rapidement. Bien sûr, il faut tout vérifier et contrôler toutes les données, mais cela permet-il de les synthétiser très rapidement? Absolument. Cela permet-il d'analyser les renseignements très rapidement? Absolument. Il existe certaines applications qui peuvent gérer nos calendriers, par exemple. Bien sûr, il faut communiquer nos données, mais cela peut-il servir à organiser et à synthétiser l'information? Oui, tout à fait.

La sénatrice Muggli : Je vais essayer de parler à tout le monde, mais j'ai deux observations à faire et j'aimerais avoir votre avis.

Tout d'abord, j'ai récemment participé à une conférence sur les facteurs prédictifs de la violence chez les jeunes en tant que conférencière. Il y avait un jeune intervenant qui avait mené une enquête auprès de 2 000 jeunes et découvert que 49 % d'entre

The other comment I want to make is that Geoffrey Hinton, one of our witnesses, said that if a product has not been tested, for example, regarding algorithms that could lead to suicide, it should be a crime.

I'm interested in hearing your responses on those. I'll start in the room with Ms. Quesada.

Ms. Quesada: First of all, it takes me aback to think that 49% of young people have a chatbot, but I'm not surprised at the same time. It feels like the access is so easy.

In an age where we are leaving people without emotional support and where discrimination is increasing — and we are leaving that untouched, as well — then it is so regular and normal that people decide to go online, where the reaffirmation is how algorithms are built. The algorithm is built to reaffirm you, to make you feel good and important. When discrimination exists, you will go there and increase extremist views and other things that we know happen there.

Is it a crime? I don't know. I would like to get more details on that and on how that statement is built, but I agree with the idea that we have to regulate the algorithm. We are able to do human rights assessments of what the algorithms are doing with people.

People who work with the algorithm cannot understand or explain what the algorithm is doing, so we have to be really mindful of what is in there and how it is working.

Mr. Richardson: I have similar opinions on that.

When we look at these AI chatbots, they are essentially engagement drivers. The folks who put them out there are designing them so that they can have youth or adults spend as much time as possible with them. There is an interesting abdication of responsibility that we have seen created with chatbots. There was an example with Air Canada half a year ago selling really cheap tickets to someone, and they wanted to turn around, saying, no, no, you can't do that because X, Y, Z.

It's interesting when we look at what a company would say about something written on a web page versus what an AI chatbot would say. If an AI chatbot gets to a point where it's suggesting that suicide is an option for someone or it is going to cause harm to someone, there is responsibility there. You can't just throw your arms up and say, well, you know, I'm protected under section 230 in the U.S. of the Communications Decency Act because I'm not responsible for what's being said here.

eux avaient comme ami un robot conversationnel qui leur apportait un soutien émotionnel. C'était 1 000 jeunes sur 2 000.

Mon autre observation concerne la déclaration de Geoffrey Hinton, l'un de nos témoins. Il a dit que ce devrait être un crime de commercialiser un produit qui n'a pas été testé, par exemple en ce qui concerne les algorithmes susceptibles d'inciter au suicide.

J'aimerais connaître votre avis à ce sujet. Je vais commencer par Mme Quesada, qui est dans la salle.

Mme Quesada : Tout d'abord, je trouve renversant que 49 % des jeunes possèdent un robot conversationnel, mais je ne suis pas surprise. Il semble si facile de s'en procurer un.

À une époque où nous laissons des gens sans soutien émotionnel et où la discrimination augmente — et on n'intervient pas à cet égard non plus —, il est si fréquent et normal que les gens décident d'aller en ligne, où les algorithmes sont conçus de manière à reconforter. Les algorithmes sont conçus pour reconforter les gens, pour qu'ils se sentent bien et importants. Quand il y a de la discrimination, nous savons que cette technologie peut notamment contribuer à propager des idées extrémistes.

Est-ce un crime? Je ne sais pas. J'aimerais obtenir plus de détails à ce sujet et sur la façon de formuler cette affirmation, mais je suis d'accord pour dire que nous devons réglementer les algorithmes. Nous sommes en mesure d'évaluer les répercussions des algorithmes sur les droits de la personne.

Les gens qui travaillent avec les algorithmes ne peuvent pas comprendre ou expliquer ce que font ces algorithmes. Nous devons donc porter une attention particulière à leur contenu et à leur fonctionnement.

M. Richardson : J'ai des opinions semblables à ce sujet.

Les robots conversationnels alimentés par l'intelligence artificielle visent essentiellement à promouvoir les interactions. Ils sont conçus de manière à ce que les jeunes ou les adultes passent le plus de temps possible avec eux. On assiste à une abdication de responsabilité intéressante par rapport aux robots conversationnels. Par exemple, il y a six mois, Air Canada a vendu des billets à très bas prix à quelqu'un, puis l'entreprise a voulu annuler la transaction en disant qu'elle ne pouvait pas l'accepter pour diverses raisons.

Il est intéressant de faire une comparaison entre ce qu'une entreprise dirait au sujet de ce qui est écrit sur une page Web et ce que dirait un robot conversationnel alimenté par l'intelligence artificielle. Si un robot conversationnel alimenté par l'intelligence artificielle arrive à un point où il laisse entendre à quelqu'un que le suicide est une solution ou qu'il va lui causer du tort, il y a une responsabilité. On ne peut pas simplement baisser les bras et dire : « Eh bien, vous savez, je suis protégé par

That's unacceptable when these are profit-driven mechanisms used by these companies.

Ms. Efir: I want to speak to the idea that untested and unregulated AI should be considered a crime.

We are talking about something that is even farther down the line. Looking at AI itself and how it's built, it's built in an unethical matter. It's built on stolen material. So, yes, if you are going to unleash AI on the world, there need to be rules and regulations for it. It needs to be tested; otherwise, we get things like Twitter, where you see an AI chatbot used to agree and soften extremist views to the vast majority of its users. That was quite extreme last year, getting people to soften their opinions on apartheid and things like that.

These mechanisms need to be tested.

Senator Petitclerc: Thank you all for being here. My first question will be for you, Mr. Richardson.

I find it very disturbing that child abuse and child exploitation material is being taken, and then, if I understand correctly, being used as training data for AI. That's what I heard.

How do you tackle that? Where do you stop that? Should it be a law? I'm thinking they are selling that dataset for training purposes. Is that where we stop it? Should the companies, then, be analyzed? How do you fix that?

I find it very disturbing and complex, and, at the same time, obvious that this cannot happen.

Mr. Richardson: Yes, it is a big, complicated question. When we look at AI training datasets, they are massive in size. The one that I cited originally, the LAION-5B, that "5B" stands for 5 billion. If you consider how many images that entails and the descriptions that they use to train a model, it's vast. There is no due diligence when it gets to that size because the costs related to having due diligence for that amount of data are significant, and the companies don't want to bear those costs, so they will just train on it and then worry about it later.

l'article 230 de la Communications Decency Act des États-Unis parce que je ne suis pas responsable de ce qui se dit ici. » On ne peut pas accepter ce genre d'attitude de la part d'entreprises qui utilisent de tels mécanismes à des fins lucratives.

Mme Efir : J'aimerais parler de l'idée selon laquelle on devrait considérer l'utilisation d'une intelligence artificielle non testée et non réglementée comme un crime.

On parle de quelque chose qui va encore plus loin. L'intelligence artificielle est elle-même conçue d'une façon qui est contraire à l'éthique. Elle est conçue avec du contenu volé. Par conséquent, si on compte déployer l'intelligence artificielle à l'échelle mondiale, il faut effectivement des règles et des règlements à cet égard. Elle doit être mise à l'essai, sinon nous verrons des situations comme sur Twitter, où un robot conversationnel alimenté par l'intelligence artificielle est utilisé pour nuancer des opinions extrémistes pour la grande majorité de ses utilisateurs. On a assisté l'année dernière à une situation assez extrême où on amenait des gens à avoir une opinion plus nuancée à l'égard de l'apartheid et d'autres sujets de cette nature.

Il faut tester ces mécanismes.

La sénatrice Petitclerc : Merci à tous d'être des nôtres. Ma première question s'adresse à vous, monsieur Richardson.

Je trouve très troublant que du contenu d'abus et d'exploitation envers des enfants soit utilisé, si je comprends bien, comme données pour entraîner l'intelligence artificielle. C'est ce que j'ai entendu.

Comment peut-on s'attaquer à ce problème? Comment peut-on empêcher cela? Devrait-on mettre en place une loi? Je pense que des ensembles de données sont vendus à des fins d'entraînement. Est-ce à ce stade que nous devons empêcher cette pratique? Est-ce qu'il faudrait alors soumettre les entreprises à une analyse? Comment peut-on régler ce problème?

Je trouve que c'est très troublant et complexe, et il me semble aussi évident que cela ne doit pas se produire.

M. Richardson : Oui, c'est une question vaste et complexe. Les ensembles de données destinés à l'entraînement de l'intelligence artificielle sont énormes. Dans le nom de celui que j'ai mentionné au départ, l'ensemble LAION-5B, « 5B » signifie 5 milliards. Compte tenu du nombre d'images que cela implique et des descriptions qu'on utilise pour entraîner un modèle, ce sont de vastes ensembles. Il n'y a pas de diligence raisonnable qui est exercée lorsque les données atteignent cette taille, car les coûts pour un tel volume de données sont importants, et les entreprises ne veulent pas assumer ces coûts, alors elles décident simplement de procéder à l'entraînement et de s'occuper du reste plus tard.

In that particular example, the dataset is an open source one, so we were able to do some work to look at some of the images related to it. That's how we were able to find that there were some images of child sexual abuse within the dataset.

There was a second example I didn't cite — and this is kind of an inverted case — where we have nudity classifiers. Artificial intelligence can detect nudity. You can think of use cases where that might be useful, for example, on a child's device. To prevent them from taking a nude image, you could potentially use a nudity detection classifier to detect that. That is possibly a good use case.

We found a dataset that was basically trained on what was thought to be adult pornography. This dataset is used by many people to train nudity classifiers. Within that dataset, we also found child-sexual-abuse material, so primarily it was the teenage age range, but it still had these images. A lot of the other images that may have been adults were very likely non-consensual intimate images.

So, it really boils down to the ethics surrounding the collection of data, and companies dodging responsibility for due diligence in their training of datasets.

Senator Petitclerc: That's my question. Once it's found — you found it and others will — then what should happen?

Mr. Richardson: In that particular case, they removed it from the reference dataset. They removed all of the things from the training dataset, but the water is kind of under the bridge at that point because there are a bunch of models that have already been trained on that out there. Do you go around and try and remove all of those particular models? Yes, it's a possibility, but it becomes very difficult when it's something that should have been dealt with in the first place.

Senator Boudreau: Thank you to the witnesses for being here today. I also want to go back to Mr. Richardson.

When you started your introductory remarks, you talked about "deepfake" imaging and some of the statistics around that. Image manipulation has been around for a long time. I remember back in the day doing little holiday e-cards where you would put your face on a dancing elf. Everything was cute and funny.

Obviously, it's gone a long way since then.

Dans cet exemple en particulier, l'ensemble de données est une source ouverte, et nous avons donc pu faire du travail pour examiner certaines des images qui en font partie. C'est ainsi que nous avons pu découvrir que l'ensemble de données contenait des images d'exploitation sexuelle d'enfants.

Il y a un deuxième exemple que je n'ai pas mentionné, et où on a observé en quelque sorte la situation inverse, car il y avait des classificateurs de nudité. L'intelligence artificielle peut détecter la nudité. On peut penser à des cas où cela pourrait être utile, notamment sur l'appareil d'un enfant. Pour empêcher l'utilisation d'une image de nudité, on pourrait utiliser un classificateur pour la détection de nudité afin de détecter ce genre de chose. C'est peut-être un exemple d'utilisation à bon escient.

Nous avons trouvé un ensemble de données destiné essentiellement à faire de l'entraînement sur ce qui était considéré comme de la pornographie adulte. Cet ensemble de données est utilisé par bien des gens pour entraîner des classificateurs de nudité. Dans cet ensemble de données, nous avons également trouvé du contenu d'abus pédosexuel. Il s'agissait principalement d'adolescents, mais on trouvait quand même ce genre d'images. Bon nombre des autres images qui pouvaient être des images d'adultes étaient fort probablement des images intimes non consentuelles.

C'est donc essentiellement un problème d'éthique entourant la collecte de données et d'entreprises qui n'assument aucune responsabilité lorsqu'il s'agit d'exercer une diligence raisonnable à l'égard des ensembles de données d'entraînement.

La sénatrice Petitclerc : C'est la question que je me pose. Une fois qu'on trouve ces données — vous en avez trouvé et d'autres en trouveront aussi —, que devrait-on faire?

M. Richardson : Dans ce cas particulier, le contenu a été retiré de l'ensemble de données de référence. On a retiré tous les éléments de l'ensemble de données d'entraînement, mais il était en quelque sorte déjà trop tard, car une foule de modèles avaient déjà été entraînés au moyen de ces données. Faut-il essayer de retirer tous ces modèles? C'est une possibilité, mais il devient très difficile d'intervenir après coup quand on n'a pas fait quelque chose qui aurait dû être fait dès le départ.

Le sénateur Boudreau : Je remercie les témoins d'être des nôtres aujourd'hui. J'aimerais également m'adresser à M. Richardson.

Au début de votre déclaration préliminaire, vous avez parlé d'imagerie par hypertrucage et de certaines statistiques à ce sujet. La manipulation d'images existe depuis longtemps. Je me souviens de l'époque où on envoyait des cartes des Fêtes électroniques dans lesquelles on pouvait mettre son visage sur un lutin qui dansait. C'était plutôt mignon et amusant.

Évidemment, les choses ont beaucoup évolué depuis.

Our job at the end of the day is to try to come up with recommendations to make to the federal government as to what they can do about this. You talked about the issue. Would you have any recommendations specific to “deepfake” imaging that the government could implement to try to stop it, curb it or restrict it as best possible?

Mr. Richardson: Thank you. It’s likely to be an imperfect solution in this case because what we saw originally with app stores was that they would have “nudifying” apps on them. Part of the issue is the ease by which you can do this. I thought it was important to point out that you don’t need a massive rig with GPUs in it. You just need your phone and a particular app that you can download from Google or Apple. There has been some work from the app stores to start removing these types of apps, but it is not enough because they are not called “deepfake” apps any more. They are using different terms to hide apps in the app stores.

There is no real ethical use for a “deepfake” app. It really doesn’t exist. It is almost entirely used for abuse, essentially.

There is opportunity to look at regulating, potentially, what app stores are doing in this space to make sure they are doing more. What they are currently doing now is something. It’s better than it was six months ago, but it is definitely not enough. Some strong encouragement from government is probably warranted here.

Senator Boudreau: Would it be going as far as putting a ban on these types of applications? Is that feasible? Is that reasonable to consider?

Mr. Richardson: They already have in their terms of service. They have said that you’re not allowed to distribute these apps on the app stores. It is more a question of how we’re putting their feet to the fire in terms of enforcing it, which gets back to what I was talking about earlier in terms of having a regulatory framework. It’s about saying, “Oh, we found some apps on here that you missed, and you should have been picking up on this.” It’s enforcing due diligence with these companies through having regulations that have teeth so you can enforce action. Perfection isn’t going to happen, but there is a place between perfection and what is happening right now that we could possibly get to.

Senator Boudreau: Thank you.

The Chair: We’ll go to the second round. We have four senators asking for questions. Three minutes each.

Au bout du compte, notre travail consiste à essayer de formuler des recommandations au gouvernement fédéral sur ce qu’il peut faire à ce sujet. Vous en avez parlé. Auriez-vous des recommandations précises sur l’imagerie par hypertrucage que le gouvernement pourrait mettre en œuvre pour essayer d’éliminer, de réduire ou de restreindre le mieux possible cette pratique?

M. Richardson : Merci. Ce sera probablement une solution imparfaite dans ce cas-ci, car à l’origine, on trouvait sur les boutiques d’applications des applications de « nudification ». Une partie du problème réside dans la facilité avec laquelle on peut faire ce genre de chose. Je crois qu’il est important de souligner qu’on n’a pas besoin d’un appareil avec un processeur graphique très puissant. Il suffit d’avoir un téléphone et une application particulière qu’on peut télécharger à partir de la boutique de Google ou d’Apple. On a commencé à retirer ce type d’applications des boutiques d’applications, mais ce n’est pas suffisant, car on ne les appelle plus des applications d’ « hypertrucage ». On emploie différents termes pour dissimuler ces applications dans les boutiques d’applications.

Il n’y a pas vraiment de façon éthique d’utiliser une application d’ « hypertrucage ». Cela n’existe pas vraiment. De façon générale, c’est utilisé presque exclusivement à des fins abusives.

On peut se pencher sur la possibilité de réglementer ce que les boutiques d’applications font à cet égard pour s’assurer qu’elles en font davantage. Elles prennent déjà certaines mesures. C’est mieux qu’il y a six mois, mais c’est nettement insuffisant. L’adoption de fortes mesures incitatives par le gouvernement serait probablement justifiée dans ce cas-ci.

Le sénateur Boudreau : Devrait-on aller jusqu’à interdire ce genre d’applications? Est-ce réaliste? Est-il raisonnable d’envisager cela?

M. Richardson : C’est déjà interdit selon les conditions de service des entreprises. Elles disent qu’il est interdit de distribuer ces applications dans les boutiques d’applications. Il s’agit surtout de déterminer comment les amener à faire respecter ces conditions, ce qui nous ramène à ce que je disais plus tôt au sujet de la mise en place d’un cadre réglementaire. Il s’agit de leur dire : « Nous avons trouvé des applications que vous n’avez pas vues, et vous auriez dû les détecter. » Il s’agit de mettre en place un cadre réglementaire qui a du mordant pour qu’on puisse obliger ces entreprises à exercer une diligence raisonnable. Il n’y aura pas de solution parfaite, mais nous pourrions atteindre un juste équilibre entre la perfection et ce qui se passe en ce moment.

Le sénateur Boudreau : Merci.

La présidente : Nous allons passer à la deuxième série. Il y a quatre sénateurs qui veulent poser des questions. Ils ont trois minutes chacun.

Senator Hay: I think I might get a little controversial here, if I may. I'm looking for balance here, and I'm hearing two things that, as parliamentarians, we need to make sure we focus on and give recommendations toward. One is around regulation and how we put the guardrails in place to reduce risk, noting that AI is already out of the gate, so it's not about eliminating it but about regulations reducing risk.

The other thing we're hearing is about criminal activity. There is criminal intent with what Mr. Richardson and others are talking about regarding child pornography and online harms. Those are actually two different things for us to balance together in this "Wild West" of AI.

Could you speak to balance? Because not everyone using data to train AI has mal-intent. I'm using it right now. So how do we balance that as parliamentarians in terms of building recommendations?

Ms. Efir: I agree with you. I don't think that all AI has mal-intent behind it and not everyone using AI has mal-intent, but I do think when we lack regulations in Canada, corporations are going to go for the easiest possible response. They'll say, like Mr. Richardson said before, "Well, we do officially ban it and that is it. We've done our due diligence." It is not enough.

Part of the thing that is keeping Canada a little bit behind is that we have been lacking on our policy and our legislation. The online harms bill, for instance, stalled multiple times. It got split up. It was so massive, and it didn't account for even some of the things that youth were talking about, like how AI is used in gambling or gaming to target young people.

There can be balance, but it needs to start some place. If we don't regulate these companies, they will go for the easiest possible solution, which is to ban and then wash their hands of any sort of safeguards for young people because it is cheaper for them.

Senator Hay: Mr. Richardson, if we have some time.

Mr. Richardson: I wouldn't put it all in the same bucket. When we look at AI, we can look at the medical applications. We hear mostly about the negative side of things because that is in the media and a lot of money is being thrown at that, but if

La sénatrice Hay : Je pense que je vais dire quelque chose d'un peu controversé, si vous me le permettez. Je cherche le juste équilibre, et selon ce que j'entends, il y a deux aspects sur lesquels nous devons nous concentrer en tant que parlementaires et pour lesquels nous devons formuler des recommandations. Premièrement, il y a la réglementation et la façon dont nous pouvons mettre en place des garde-fous pour atténuer les risques, étant donné que l'intelligence artificielle est déjà déployée, et qu'il ne s'agit donc pas de l'éliminer, mais de la réglementer pour en atténuer les risques.

On parle également des activités criminelles. Il y a une intention criminelle dans ce dont M. Richardson et d'autres ont parlé en ce qui concerne la pornographie juvénile et les préjudices en ligne. Ce sont en fait deux aspects différents que nous devons concilier dans le « Far West » de l'intelligence artificielle.

Pourriez-vous nous parler de l'équilibre? Je pose la question parce que tous ceux qui utilisent des données pour entraîner l'intelligence artificielle n'ont pas forcément de mauvaises intentions. J'en utilise moi-même actuellement. Je me demande donc comment nous pouvons, en tant que parlementaires, atteindre un juste équilibre dans nos recommandations?

Mme Efir : Je suis d'accord avec vous. Je ne pense pas que toutes les intelligences artificielles soient fondées sur de mauvaises intentions ni que tous ceux qui les utilisent aient de mauvaises intentions, mais je pense que, sans réglementation au Canada, les entreprises opteront pour la solution la plus facile. Elles diront, comme le mentionnait M. Richardson tout à l'heure : « Eh bien, nous interdisons officiellement cet usage, et c'est tout. Nous avons rempli nos obligations. » Ce n'est pas suffisant.

L'une des raisons pour lesquelles le Canada est un peu à la traîne, c'est qu'il y a un manque en matière de politiques et de législation. Le projet de loi sur les préjudices en ligne, par exemple, a été bloqué à plusieurs reprises. Il a été scindé en plusieurs parties. Il était très volumineux, et il ne tenait même pas compte de certains des sujets abordés par les jeunes, comme la manière dont l'IA est utilisée dans les jeux d'argent ou les jeux vidéo pour cibler les jeunes.

Un équilibre est possible, mais il faut bien commencer quelque part. Si nous ne réglementons pas ces entreprises, elles opteront pour la solution la plus simple, qui consiste à interdire, puis à se décharger de toute responsabilité en matière de protection des jeunes, car cela leur revient moins cher.

La sénatrice Hay : S'il reste assez de temps, monsieur Richardson, pouvez-vous répondre?

M. Richardson : Je ne mettrais pas tout dans le même panier. Quand on parle d'intelligence artificielle, on peut penser aux applications médicales. On entend surtout parler des aspects négatifs, car c'est ce que les médias relaient et c'est là-dessus

you look at the transcription apps, there are many things that are useful but don't rely on third-party user-generated content or intersect with the public in that way. That is the key differentiating factor, and it applies to online harms because it is based on user-generated content and what that entails. It's part of a larger conversation.

Senator Senior: Thank you. Ms. Quesada, with respect to the statutory duty of care as it relates to human rights? I would like to know more about that. If it as a document, I would love to see it. If not, a minute about that would be great.

I'm also interested, Ms. Sharma, with respect to the literacy that you spoke about. I also have a question about young people — all of us, really — and how AI seems to be dumbing us down. I'm most concerned about young people. A friend of mine is developing a tool for educators to promote critical thinking. Instead of giving young people the answers, we ask how we can actually support young people in terms of using their brains and not dumbing down their brains. Can you speak to that?

Ms. Quesada: I'll talk about the four pillars that are part of the United Nations Convention on the Rights of the Child. There is participation, protection and provision, and we at JHC have included remedy. When we talk about the duty of care, it is to ask that we create legislation that brings the voices of young people to the centre. We look primarily for the participation of those more marginalized or people in rural areas. We want to hear the voices we never hear from or the quiet folks out there. When we think of protection, how do we protect people so they can use AI under ethical and responsible standards? This includes critical thinking and all these things.

When we think of provision, how do we provide enough so that everyone can use it under the same standards? How do we create spaces for remediation? So when it is used in the wrong way or with mal-intent, how do we remediate those spaces so that we address it? For that, we need people engaged in the legislation and with the regulatory framework.

Ms. Sharma: To your point, young people are, of course, the largest cohort of folks that use AI. AI actually can, to your point, be used for positive things, such as personalized learning,

que l'on investit massivement, mais si on prend les applications de transcription par exemple, il y a beaucoup de choses utiles qui ne reposent pas sur du contenu généré par des utilisateurs tiers ou qui ne reposent pas sur de telles interactions avec le public. C'est là que réside la principale différence, et cela s'applique aux préjugés en ligne, car ceux-ci reposent sur le contenu généré par les utilisateurs, avec tout ce que cela implique. Cela s'inscrit dans un débat plus large.

La sénatrice Senior : Merci. Madame Quesada, pourriez-vous nous en dire plus sur le devoir de diligence prévu par la loi en matière de droits de la personne? J'aimerais en savoir davantage à ce sujet. S'il existe un document à ce sujet, j'aimerais beaucoup le consulter. Sinon, j'aimerais que vous nous en parliez brièvement.

Je suis également intéressée par ce que vous avez dit, madame Sharma, au sujet de l'éducation. J'ai aussi une question qui concerne les jeunes — et nous tous, en fait — sur la façon dont l'IA semble nous abrutir. Ce sont les jeunes qui m'inquiètent le plus. Je connais quelqu'un qui développe un outil destiné aux éducateurs pour promouvoir la pensée critique. Au lieu de donner des réponses toutes faites aux jeunes, nous nous demandons ce que nous pouvons faire pour les aider à utiliser leur cerveau de manière constructive, sans les abrutir. Pouvez-vous nous en dire plus à ce sujet?

Mme Quesada : Je vais vous parler des quatre piliers de la Convention des Nations unies relative aux droits de l'enfant. Ils comptent la participation, la protection et la réponse aux besoins, et au Centre John Humphrey, nous y avons ajouté le recours. Par devoir de diligence, nous entendons la nécessité de créer des lois mettant en avant la voix des jeunes. Nous recherchons avant tout la participation des personnes les plus marginalisées ou de celles vivant en milieu rural. Nous voulons entendre les voix que nous n'entendons jamais, ou celles des personnes qui n'ont pas l'habitude de se faire entendre. En ce qui concerne, la protection, nous nous demandons comment protéger les gens afin qu'ils puissent utiliser l'intelligence artificielle selon des normes éthiques et responsables. Cela inclut la pensée critique et tout ce qui s'y rapporte.

En ce qui concerne la réponse aux besoins, nous devons nous demander comment fournir suffisamment de ressources pour que tout le monde puisse en bénéficier selon les mêmes normes. Comment créer des espaces de réparation? Ainsi, quand l'intelligence artificielle est utilisée de manière abusive ou avec de mauvaises intentions, que pouvons-nous faire pour remédier à ces situations? Pour cela, nous avons besoin de personnes impliquées dans l'élaboration des lois et du cadre réglementaire.

Mme Sharma : Comme vous le soulignez, les jeunes constituent bien sûr le groupe le plus important d'utilisateurs de l'intelligence artificielle. Comme vous le faites remarquer,

creativity and early mental health detection, but it also poses significant risks that include misinformation, harmful and illegal content, manipulation and developmental harms.

Can that balance be struck? I think, yes. We need to come back to the drawing board and encourage educators to feel empowered, like with the tools that you mentioned, in order for them to be able to use them in the classrooms because, again, there are some young people who only have access to technology within those eight hours they are attending school. We don't know if they have access to the same technology afterward, so how do we include those people?

The Chair: Thank you.

Senator Muggli: Ms. Sharma, you get to keep talking. Just as a reminder, around half of the 2,000 youth have a chatbot for every emotional support. I'd also like you to touch on the comment around if a product has not been tested regarding algorithms that could lead to suicide, for example, that it should be a crime. I'm looking for your opinion.

Ms. Sharma: I was itching to answer that question.

First, what we're seeing is that because AI provides that access, that's why a lot of young people, including adults, of course, are going to AI because it is something that is affirming. You go there, and it tells you exactly what you want to hear.

I think that really is the risk and the challenge. Instead of young people going to a chatbot, why can't they go to an adult? Why can't they go to a peer? How do we ensure that educators, parents and people who share that space with young people for eight-plus hours a day have those resources?

Second, I did want to draw your attention to a specific case that actually happened very recently: the Tumbler Ridge incident in B.C. A couple of days ago, the CEO of OpenAI, Sam Altman, actually apologized for not informing law enforcement and not being able to inform law enforcement earlier about the conversations of the person who perpetrated that crime.

Senator Muggli: I understand that point. I'm wondering if it should be a crime if the product has not been tested to ensure the algorithms are safe. Some people say it shouldn't be deployed, period.

l'intelligence artificielle peut effectivement être mise à profit pour des applications positives, telles que l'apprentissage personnalisé, la création et le dépistage précoce des troubles de santé mentale, mais elle comporte également des risques importants, notamment la désinformation, les contenus préjudiciables et illégaux, la manipulation et des effets néfastes sur le développement.

Est-il possible de trouver un équilibre? Je pense que oui. Nous devons repartir de zéro et encourager les enseignants à se sentir autonomes, notamment grâce à des outils tels que ceux que vous avez mentionnés et qui peuvent être utilisés en classe. En effet, certains jeunes n'ont accès à la technologie que pendant les huit heures qu'ils passent à l'école. Nous ne savons pas s'ils y ont accès en dehors de ces heures, alors que faire pour inclure ces personnes.

La présidente : Merci.

La sénatrice Muggli : Madame Sharma, je vais rester avec vous. Pour rappel, environ la moitié des 2 000 jeunes ont dit avoir recours à un robot conversationnel pour obtenir un soutien émotionnel. J'aimerais également que vous abordiez la question suivante : si les algorithmes d'un produit n'ont pas été testés pour s'assurer qu'ils ne peuvent pas conduire au suicide, par exemple, cela devrait-il être considéré comme un délit? J'aimerais connaître votre avis.

Mme Sharma : J'espérais qu'on me pose cette question.

Tout d'abord, ce que nous constatons, c'est que, comme l'intelligence artificielle offre cette possibilité, de nombreux jeunes, mais aussi des adultes, bien sûr, se tournent vers l'intelligence artificielle parce qu'elle leur apporte un sentiment de validation. Vous la consultez, et elle vous dit exactement ce que vous voulez entendre.

Je pense que c'est vraiment là le risque et le défi. Pourquoi les jeunes ne se tournent-ils pas vers un adulte plutôt que vers un robot conversationnel? Pourquoi ne se tournent-ils pas vers un pair? Comment faire en sorte que les éducateurs, les parents et les personnes qui côtoient les jeunes pendant plus de huit heures par jour disposent des ressources nécessaires?

Deuxièmement, je tenais à attirer votre attention sur un cas précis qui s'est produit très récemment : l'incident de Tumbler Ridge en Colombie-Britannique. Il y a quelques jours, le PDG d'OpenAI, Sam Altman, a présenté ses excuses pour ne pas avoir informé les forces de l'ordre et pour ne pas avoir pu les informer plus tôt des conversations menées par la personne qui a commis ce crime.

La sénatrice Muggli : Je comprends ce point. Je me demande si le fait de ne pas avoir testé le produit pour s'assurer que les algorithmes sont sûrs devrait constituer un délit. Certains affirment que le produit ne devrait tout simplement pas être déployé.

Ms. Sharma: In my opinion, yes, because at the end of the day, the young population is our future. It is not okay to play and experiment with young people who are the future and who will continue using AI.

How do we make sure that they are digitally literate to identify these harms earlier on so they are not going to chatbots to have those mental health conversations?

Senator Muggli: Show of hands, who thinks we should have age restrictions on social media for youth? Okay. Thank you.

Senator Petitclerc: My question will be for you as well, Ms. Sharma. It goes along with what you just said. Maybe it will be a show of hands. Do we agree that while literacy is super important, do we fear that if we have good AI literacy, it needs to be for everybody? I worry that not everybody will get the same level of access to the same level of literacy. Is this something you worry about?

Do we agree that the responsibility should not land on youth? It should land on the companies and the developers. I feel we can help educate, but in the end, they should have all that responsibility. Is this something you agree with?

Ms. Sharma: I'll answer your first question. I'll go back to what I referenced in my opening statement in respect to the AI program. One of the reasons why Estonia is so far ahead in the AI literacy piece is because they are a smaller country and because their education is nationalized. For us, it is province by province.

One thing that, of course, is in my recommendation is looking at a federal program that allows for that AI literacy to happen to catch everyone up to speed. What we're seeing is jobs require the use of AI now. Jobs require some sort of knowledge on how to use technology. If we know that technology is critical, then how do we make sure that those digital literacy pieces and guidelines exist?

I know we talked a lot about regulatory frameworks today, which is really critical.

To your second question about responsibility, companies and corporations should be taking responsibility. I think the unfortunate truth that we are faced with, at the end of the day,

Mme Sharma : À mon avis, oui, car au bout du compte, la jeunesse est notre avenir. Il n'est pas acceptable de jouer avec l'avenir des jeunes et de faire des expériences à leurs dépens, alors que ce sont eux qui utiliseront l'intelligence artificielle à l'avenir.

Il faut se demander ce que nous pouvons faire pour qu'ils aient les compétences numériques nécessaires pour repérer ces dangers plus tôt, afin qu'ils ne se tournent pas vers les robots conversationnels pour parler de leur santé mentale.

La sénatrice Muggli : Levez la main, ceux qui pensent qu'il faudrait instaurer des restrictions d'âge sur les réseaux sociaux pour les jeunes. D'accord. Merci.

La sénatrice Petitclerc : Ma question s'adresse également à vous, madame Sharma. Elle fait suite à ce que vous venez de dire. Peut-être que les témoins pourraient répondre à main levée. Sommes-nous d'accord sur le fait que, même si la culture numérique est extrêmement importante, il existe un risque lié à l'accès à une bonne culture numérique pour tous? Je crains que tout le monde ne bénéficie pas du même niveau d'accès à cette culture numérique. Est-ce une préoccupation pour vous?

Pouvons-nous convenir que cette responsabilité ne doit pas incomber aux jeunes? Elle devrait incomber aux entreprises et aux développeurs. Je pense que nous pouvons contribuer à l'éducation, mais au bout du compte, c'est à eux qu'incombe l'entière responsabilité. Êtes-vous d'accord avec moi?

Mme Sharma : Je vais répondre à votre première question. Je reviendrai sur ce que j'ai mentionné dans ma déclaration liminaire concernant le programme relatif à l'IA. L'une des raisons pour lesquelles l'Estonie est si en avance en matière de culture de l'IA est qu'il s'agit d'un petit pays et que son système éducatif est nationalisé. Au Canada, chaque province a son propre système.

Une chose qui figure bien sûr dans ma recommandation est d'envisager un programme fédéral permettant de mettre tout le monde à niveau en matière de culture de l'intelligence artificielle. Ce que nous constatons, c'est que certains emplois exigent désormais l'utilisation de l'intelligence artificielle. Il faut avoir certaines connaissances sur la manière d'utiliser cette technologie dans le cadre de son travail. Si nous savons que cette technologie est essentielle, comment pouvons-nous alors nous assurer que ces éléments de culture numérique et ces lignes directrices existent?

Je sais que nous avons beaucoup parlé aujourd'hui des cadres réglementaires et c'est un élément essentiel.

Pour répondre à votre deuxième question sur la responsabilité, je dirais que les entreprises et les sociétés devraient assumer leurs responsabilités. Je pense que la triste réalité à laquelle nous

companies are for profit. It's not necessarily up to us to determine what they're able to do and not able to do. That is why they are corporations.

From there, the next best course of action becomes that AI literacy piece. I want to encourage everyone to look at the Digital Services Act that the European Union has put forward. They have a fantastic framework for how regulation of companies can serve as a wonderful tool to have that revenue that gets generated to be put back into a support system.

The Chair: Thank you very much. I think we are complete. This brings us to the end of the first panel. I would like to thank the witnesses for your testimony.

For our second panel, we welcome from Evidence for Democracy, Félix Proulx-Giraldeau, Interim Executive Director; from AI Safety Asia, Alejandro Reyes, Chief Strategy Officer; and by video conference, Supheakmungkol Sarin, Co-founder and Chief Research Officer. From the Canadian Pediatric Society, Dr. Michelle Ponti, Paediatrician and Chair of the Digital Health Task Force; and Dr. Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa.

Thank you all for joining us today. For your opening statements, you will have five minutes, followed by questions from our committee members. Mr. Proulx-Giraldeau, the floor is yours.

Félix Proulx-Giraldeau, Interim Executive Director, Evidence for Democracy: Thank you. It is a real pleasure to appear before you today.

My name is Dr. Felix Proulx-Giraldeau, and I am joining today as the interim executive director at Evidence for Democracy.

We are Canada's leading non-partisan, not-for-profit organization that is championing evidence usage in government, working to close the gap between decision-makers, like yourselves, and the best available science and evidence. We do this through original research, skills training and issues-based campaigns because we believe Canadians benefit when governments make decisions informed by the best available science and evidence, leading to better outcomes for all.

We are pleased to be here today to discuss the impact of artificial intelligence in Canada. This impact is no longer theoretical. AI is rapidly reshaping how governments gather

sommes confrontés, au bout du compte, c'est qu'une entreprise est une entité à but lucratif. Ce n'est pas nécessairement à nous de déterminer ce que les entreprises peuvent ou ne peuvent pas faire. C'est pour cela qu'elles sont des sociétés.

À partir de là, la meilleure ligne de conduite consiste à développer la culture de l'intelligence artificielle. J'encourage tout le monde à se pencher sur la législation sur les services numériques proposée par l'Union européenne. Elle offre un cadre fantastique montrant comment la réglementation des entreprises peut servir d'outil formidable pour réinvestir les revenus générés dans un système de soutien.

La présidente : Merci beaucoup. Je crois que nous avons fait le tour. C'est tout pour le premier groupe; nous passerons maintenant au deuxième groupe. Je tiens à remercier tous les témoins du premier groupe.

Dans le deuxième groupe, nous recevons Félix Proulx-Giraldeau, directeur général par intérim d'Évidence pour la démocratie, et Alejandro Reyes, directeur de la stratégie d'AI Safety Asia, ainsi que, par vidéoconférence, Supheakmungkol Sarin, cofondateur et directeur de la recherche d'AI Safety Asia. Sont également avec nous la Dre Michelle Ponti, pédiatre et présidente du Groupe de travail sur la santé numérique de la Société canadienne de la pédiatrie, et Me Michael Geist, de la chaire de recherche du Canada en droit d'Internet et du commerce électronique de l'Université d'Ottawa.

Je vous remercie d'être avec nous aujourd'hui. Monsieur Proulx-Giraldeau, vous avez cinq minutes pour votre déclaration liminaire et les membres du comité pourront ensuite vous poser des questions. La parole est à vous.

Félix Proulx-Giraldeau, directeur général par intérim, Évidence pour la démocratie : Merci. Je suis très heureux de témoigner devant le comité aujourd'hui.

Je m'appelle Félix Proulx-Giraldeau et je prends la parole en tant que directeur général par intérim d'Évidence pour la démocratie.

Notre organisation est le principal organisme canadien non partisan et à but non lucratif qui milite en faveur de l'utilisation des données factuelles au sein du gouvernement. Nous nous efforçons de combler le fossé entre les décideurs, comme vous, et les meilleures données scientifiques et factuelles disponibles. Pour ce faire, nous menons nos propres recherches, proposons des formations et menons des campagnes thématiques, car nous sommes convaincus que les Canadiens ont tout à gagner lorsque les gouvernements prennent des décisions fondées sur les meilleures données scientifiques et factuelles disponibles, par ce que cela se traduit par de meilleurs résultats pour tous.

Nous sommes heureux d'être ici aujourd'hui pour discuter de l'impact de l'intelligence artificielle au Canada. Cet impact n'est plus théorique. L'IA est en train de transformer rapidement la

evidence, analyze information and make decisions. Its use across the federal public service is expanding quickly.

This new technology creates incredible opportunities for all Canadians, but it also creates serious risks for transparency, accountability, privacy, fairness and public trust.

Canadians are navigating one of the most turbulent periods in our history, one marked by rising cost pressures, geopolitical instability, climate-related disasters and intensifying disinformation threats. These are exactly the kinds of challenges where strong, evidence-informed policy matters most. AI technologies have the potential to be a game-changer in this space, but only if they are governed with clear rules, robust oversight and meaningful public accountability.

First and foremost, we recommend that the federal government create an independent regulatory authority, a digital safety commission, with enforcement powers and a clear mandate to coordinate national digital governance, including public-facing AI and social media, through a new online harms bill. This institution should be able to mandate data access, conduct algorithmic audits, issue corrective orders and penalties, all the while requiring stronger safety and design standards, including high-privacy defaults and child-impact assessments.

We also recommend introducing a statutory duty-of-care for AI developers, inspired by international best practices, such as the UK Online Safety Act, the EU Digital Services Act and the EU AI Act.

Our research also highlights the risks of bias and discrimination that these AI systems can introduce. Poor data quality, opaque systems and weak oversight can reproduce or worsen harms already faced by marginalized communities, especially racialized Canadians. Those risks are especially serious in high-stakes settings, such as immigration, health care and social services, where automated errors have had real and lasting consequences, including wrongful arrests, unfairly denying social service claims and unjustly stripping residents of their legal status.

This is precisely why transparency must also be strengthened. Canadians should be able to tell when AI is being used by their government, what data it relies on and where that data came

façon dont les gouvernements recueillent des données, analysent l'information et prennent des décisions. Son utilisation au sein de la fonction publique fédérale se généralise rapidement.

Cette nouvelle technologie offre des possibilités incroyables à tous les Canadiens, mais elle comporte également de sérieux risques en matière de transparence, de responsabilité, de protection de la vie privée, d'équité et de confiance du public.

Les Canadiens traversent l'une des périodes les plus tumultueuses de l'histoire du pays, marquée par la hausse des coûts, l'instabilité géopolitique, les catastrophes climatiques et l'intensification des menaces liées à la désinformation. C'est précisément face à ce type de défis qu'une politique solide, fondée sur des données probantes, revêt toute son importance. Les technologies d'intelligence artificielle ont le potentiel de changer la donne dans ce domaine, mais seulement si elles sont encadrées par des règles claires, une surveillance rigoureuse et une reddition de comptes publique sérieuse.

D'abord et avant tout, nous recommandons que le gouvernement fédéral crée une autorité réglementaire indépendante, une commission de la sécurité numérique, dotée de pouvoirs d'application et d'un mandat clair pour coordonner la gouvernance numérique nationale, y compris l'intelligence artificielle accessible au public et les réseaux sociaux, au moyen d'un nouveau projet de loi sur les préjudices en ligne. Cette institution devrait être en mesure de rendre obligatoire l'accès aux données, d'effectuer des audits algorithmiques et d'émettre des ordonnances correctives et des sanctions, tout en exigeant des normes de sécurité et de conception plus strictes, y compris des paramètres liés à la protection de la vie privée élevés par défaut et des évaluations de l'incidence sur les enfants.

Nous recommandons également l'adoption d'une obligation légale de diligence pour les développeurs de l'intelligence artificielle, inspirée des pratiques exemplaires internationales, comme la loi sur la sécurité en ligne du Royaume-Uni, la loi européenne sur les services numériques et la loi européenne sur l'intelligence artificielle.

Notre recherche met également en évidence les risques de partialité et de discrimination que ces systèmes d'intelligence artificielle peuvent introduire. La piètre qualité des données, les systèmes opaques et la faiblesse de la surveillance peuvent reproduire ou aggraver les préjudices déjà subis par les communautés marginalisées, en particulier les Canadiens racisés. Ces risques sont particulièrement graves dans des contextes où les enjeux sont élevés, comme l'immigration, les soins de santé et les services sociaux, où les erreurs automatisées ont eu des conséquences réelles et durables, y compris des arrestations injustifiées, le refus injuste de demandes de services sociaux et la révocation injuste du statut juridique de résidents.

C'est précisément la raison pour laquelle il faut aussi renforcer la transparence. Les Canadiens devraient être en mesure de savoir quand l'intelligence artificielle est utilisée par leur

from. That is why we recommend visible labelling, digital watermarking and source transparency requirements for AI systems and tools.

Finally, we believe that Canadians should have a meaningful voice in how AI is designed and governed. We recommend investigating standing citizens' assemblies or deliberative panels, as well as structured partnerships between civil society and academic researchers, and regular advisory councils with attention to youth and racialized stakeholders.

Democratic input is essential if AI systems are to serve the public interest. This means doubling down on transparency, accountability, strong privacy and safety protections, robust oversight and meaningful public participation. If we get those foundations right today, Canada can truly reduce harm, build public trust and use science and evidence to better serve everyone.

Thank you for your time, and I look forward to your questions.

The Chair: Thank you, Dr. Proulx-Girardeau. Mr. Reyes, you have the floor.

Alejandro Reyes, Chief Strategy Officer, AI Safety Asia: Thank you. Honourable senators, thank you for the invitation to appear before you. My name is Alejandro Reyes. I'm appearing on behalf of AI Safety Asia, or AISA, with Dr. Supheakmungkol Sarin, our co-founder and executive director, who is joining virtually. I'm also a Canadian foreign policy analyst focused on the Indo-Pacific. I previously worked at Global Affairs Canada. Our central point is this: Canada should not think about AI only as a domestic innovation; it should also think about AI as a question of sovereignty, readiness and international positioning.

[*Translation*]

AI is increasingly shaped by geopolitical rivalry, much of it running through the Indo-Pacific. As with 5G, Canada will often need to work more closely with the United States and other trusted partners on security-sensitive AI issues, while maintaining limited and careful channels with China.

gouvernement, sur quelles données elle repose et d'où ces données proviennent. C'est pourquoi nous recommandons des exigences en matière d'étiquetage visible, de filigrane numérique et de transparence des sources pour les systèmes et les outils d'intelligence artificielle.

Enfin, nous croyons que les Canadiens devraient avoir leur mot à dire dans la conception et la gouvernance de l'intelligence artificielle. Nous recommandons d'envisager de mettre sur pied des assemblées ou des comités de délibération de citoyens permanents, ainsi que de conclure des partenariats structurés entre la société civile et les chercheurs universitaires, et de mettre à profit les conseils consultatifs réguliers, en accordant une attention particulière aux jeunes et aux intervenants racisés.

L'apport démocratique est essentiel si l'on veut que les systèmes d'intelligence artificielle servent l'intérêt public. Cela signifie qu'il faut renforcer la transparence et la reddition de comptes et pouvoir compter sur de solides mesures de protection de la vie privée et de la sécurité, une surveillance rigoureuse et une participation significative du public. Si nous jetons les bases nécessaires dès aujourd'hui, le Canada pourra vraiment réduire les méfaits, renforcer la confiance du public et utiliser la science et les données probantes pour mieux servir tout le monde.

Je vous remercie du temps que vous m'avez accordé, et j'ai hâte de répondre à vos questions.

La présidente : Merci, monsieur Proulx-Girardeau. Monsieur Reyes, vous avez la parole.

Alejandro Reyes, directeur de la stratégie, AI Safety Asia : Merci. Honorables sénateurs, je vous remercie de m'avoir invité à comparaître devant vous. Je m'appelle Alejandro Reyes. Je comparais au nom d'AI Safety Asia, ou AISA, avec M. Supheakmungkol Sarin, notre cofondateur et directeur général, qui se joint à nous virtuellement. Je suis également analyste de la politique étrangère du Canada pour l'Indo-Pacifique. J'ai déjà travaillé à Affaires mondiales Canada. Notre argument central est le suivant : le Canada ne devrait pas considérer l'intelligence artificielle uniquement comme une innovation nationale, mais aussi comme une question de souveraineté, de préparation et de positionnement international.

[*Français*]

L'intelligence artificielle est de plus en plus façonnée par la rivalité géopolitique, dont une grande partie se joue dans la région indo-pacifique. Comme pour le cas de la 5G, le Canada devra collaborer plus étroitement avec les États-Unis et d'autres partenaires de confiance sur les enjeux liés à l'IA qui touchent à la sécurité, tout en maintenant avec la Chine des canaux de communication limités et prudents.

[English]

This matters because frontier AI is moving from content generation into operational capability. The question is no longer only how to regulate content or encourage innovation; it is also whether Canada can evaluate, procure, monitor and respond to high-capability systems before they create public, economic, cyber or diplomatic crises. AISA's work points to one further issue: Countries must prepare not only to govern AI in ordinary times, but also respond to AI-related crises in real time. One of the concepts we have been developing is AI crisis diplomacy. The basic idea is that AI is becoming a crisis accelerator; it compresses the time between harm, confusion, verification and escalation. The issue is whether an AI-enabled incident moves across borders or institutions faster than existing response channels can manage. That can include cyber incidents, fraud, "deepfakes" or failures in AI-enabled public or economic infrastructure. This crisis lens also matters in areas such as biosecurity, where AI may lower barriers to harmful biological activity while reshaping public health preparedness and response.

That matters for Canada for four reasons. First, Canada needs a broader understanding of AI sovereignty. Sovereignty in AI is not full-stack independence. It is the capacity to audit and govern systems operating within Canadian borders. Without that, Canada is forced into blind trust. It means that being able to choose what to adopt, test what it deploys, protect data and language rights, maintain access to compute and talent, and respond when advanced systems fail or are misused. It is not just industrial policy; it is also about assurance, public capacity and strategic choice.

[Translation]

In Canada, that sovereignty question also includes language. If AI systems are to be trusted, they must support official bilingualism and help protect the vitality of French-language public life, research and culture, while also respecting Indigenous and multilingual realities. As Canada looks ahead to the Francophonie Summit in Cambodia later in the year, it should see language in AI as part of both national cohesion and wider international engagement.

[Traduction]

C'est important parce que l'intelligence artificielle pionnière passe de la production de contenu à la capacité opérationnelle. La question n'est plus seulement de savoir comment réglementer le contenu ou encourager l'innovation; il s'agit aussi de savoir si le Canada peut évaluer, se procurer, surveiller des systèmes à haute capacité avant qu'ils ne créent des crises publiques, économiques, cybernétiques ou diplomatiques. Il doit aussi pouvoir y réagir. Les travaux de l'AISA mettent en lumière un autre problème : les pays doivent se préparer non seulement à régir l'intelligence artificielle en temps normal, mais aussi à répondre aux crises liées à l'intelligence artificielle en temps réel. L'un des concepts que nous avons élaborés est la diplomatie de crise de l'intelligence artificielle. L'idée de base est que l'intelligence artificielle devient un accélérateur de crise; elle comprime le temps entre les préjugés, la confusion, la vérification et l'escalade. La question est de savoir si un incident facilité par l'intelligence artificielle va traverser les frontières ou les institutions plus rapidement que les canaux d'intervention existants ne peuvent le gérer. Il peut s'agir de cyberincidents, de fraude, d'« hypertrucages » ou de défaillances d'infrastructures publiques ou économiques fondées sur l'intelligence artificielle. Cette optique de crise est également importante dans des domaines comme la biosécurité, où l'intelligence artificielle peut réduire les obstacles à l'activité biologique néfaste tout en remodelant la préparation et l'intervention en matière de santé publique.

C'est important pour le Canada pour quatre raisons. Premièrement, le Canada doit mieux comprendre la souveraineté de l'intelligence artificielle. Dans le domaine de l'intelligence artificielle, la souveraineté n'est pas synonyme d'indépendance complète. Il s'agit de la capacité de vérifier et de régir les systèmes qui fonctionnent à l'intérieur des frontières canadiennes. Sans cela, le Canada est forcé de naviguer à l'aveuglette. Cela signifie être en mesure de choisir ce qu'il faut adopter, de mettre à l'essai ce qu'il déploie, de protéger les données et les droits linguistiques, de maintenir l'accès aux ordinateurs et aux talents et de réagir lorsque des systèmes avancés échouent ou sont utilisés à mauvais escient. Ce n'est pas seulement une question de politique industrielle; c'est aussi une question d'assurance, de capacité publique et de choix stratégique.

[Français]

Au Canada, cette question de souveraineté touche aussi à la langue. Si les systèmes d'IA doivent inspirer confiance, ils doivent appuyer le bilinguisme officiel et contribuer à protéger la vitalité de la vie publique, de la recherche et de la culture d'expression française, tout en respectant les réalités autochtones et multilingues. À l'approche du Sommet de la Francophonie qui se tiendra plus tard cette année au Cambodge, le Canada devrait considérer la question de la langue dans l'IA comme un élément

[English]

Second, Canada needs to pay closer attention to the future of work and to AI in education. Our research on the business process outsourcing sector in the Philippines offers an early view of how AI may affect service sector employment and routine cognitive work more broadly. Canada is engaging in these questions, but there remains a gap between recognizing disruption and being prepared for it. The same is true in education, where AI literacy is becoming a civic and economic capability.

Third, Canada needs stronger crisis preparedness and public-sector readiness. The real question is not only whether Canada has principles for AI governance but whether it has the operational capacity to respond when AI-driven harms move faster than existing systems were designed to handle.

Canada should use procurement and market access to enforce safety standards and require public-sector AI readiness before high-impact deployment, evaluation, evidence, audit rights, incident reporting, rollback plans, redress pathways and, over time, more institutionalized incident reporting.

Fourth, Canada needs an external strategy on AI, not only a domestic one. As a middle power, Canada will not determine the global AI order on its own, but it can still help shape trusted partnerships, governance norms and cooperation around risk reduction and crisis response. To do that, Canada must engage more deliberately not only with the United States and Europe but also with Asian partners.

The Chair: Thank you very much, Mr. Reyes. Dr. Ponti, you have five minutes.

Dr. Michelle Ponti, Paediatrician and Chair of the Digital Health Task Force, Canadian Paediatric Society: Thank you, senators, for the opportunity to join you today to consider the mental health and developmental impacts of AI on infants, children and youth.

à la fois de sa cohésion nationale et de son engagement international au sens large.

[Traduction]

Deuxièmement, le Canada doit accorder une plus grande attention à l'avenir du travail et à l'intelligence artificielle dans le domaine de l'éducation. Notre recherche sur le secteur de l'externalisation des processus opérationnels aux Philippines offre un aperçu précoce de la façon dont l'intelligence artificielle peut influencer sur l'emploi dans le secteur des services et le travail cognitif de routine en général. Le Canada se penche sur ces questions, mais il reste un écart entre la reconnaissance des perturbations et le fait de s'y préparer. Il en va de même dans le domaine de l'éducation, où la littératie en matière d'intelligence artificielle devient une capacité civique et économique.

Troisièmement, le Canada doit mieux se préparer aux crises et mieux préparer le secteur public. La vraie question n'est pas seulement de savoir si le Canada a des principes de gouvernance de l'intelligence artificielle, mais aussi s'il a la capacité opérationnelle de réagir lorsque les préjudices causés par l'intelligence artificielle évoluent plus rapidement que ne peuvent réagir les systèmes existants qui ont été conçus pour les gérer.

Le Canada devrait utiliser l'approvisionnement et l'accès aux marchés pour faire respecter les normes de sécurité et exiger que le secteur public soit prêt à utiliser l'IA avant le déploiement à incidence élevée, l'évaluation, les preuves, les droits d'audit, le signalement des incidents, les plans de retour en arrière, les voies de recours et, au fil du temps, un signalement plus institutionnalisé des incidents.

Quatrièmement, le Canada a besoin d'une stratégie externe en matière d'intelligence artificielle, et pas seulement d'une stratégie nationale. En tant que puissance moyenne, le Canada ne déterminera pas seul l'ordre mondial en matière d'intelligence artificielle, mais il peut tout de même contribuer à façonner des partenariats de confiance, des normes de gouvernance et une coopération en matière de réduction des risques et d'intervention en cas de crise. Pour ce faire, le Canada doit s'engager de façon plus délibérée non seulement avec les États-Unis et l'Europe, mais aussi avec ses partenaires asiatiques.

La présidente : Merci beaucoup, monsieur Reyes. Docteur Ponti, vous avez cinq minutes.

Dre Michelle Ponti, pédiatre et présidente du Groupe de travail sur la santé numérique, Société canadienne de pédiatrie : Je vous remercie, honorables sénateurs, de me donner l'occasion de me joindre à vous aujourd'hui pour examiner les répercussions de l'intelligence artificielle sur la santé mentale et le développement des nourrissons, des enfants et des jeunes.

I'm a practising pediatrician in London, Ontario, and I've also been the founding chair of the Digital Health Task Force at the Canadian Pediatric Society for the past decade.

The digital world is no longer separate from childhood; it's embedded within it and is referred to as the digital ecosystem. The impact of this digital ecosystem on child development is undoubtedly one of the most significant and unpredictable public health challenges we all face today.

Young people are among the most exposed to, and affected by, AI systems. Children do not encounter AI occasionally; it's present in their classrooms, on their phones, in their toys and in the social spaces where they seek belonging. Yet, these systems have been designed primarily for commercial efficiency, not for child development safety or well-being.

I have three main points of concern for your consideration. First is the impact of AI on learning. AI tools are increasingly used to support learning, from writing assistance and tutoring tools to personalized content feeds. While these technologies may offer benefits, there are growing concerns about their impacts on early literacy and cognitive skills.

Overreliance on AI can undermine the development of critical thinking, reading comprehension and writing skills — abilities that are essential not only for academic success but for life's challenges.

The impacts are not uniform across development. For infants and young children, early learning depends on that response of human interaction. Language development, emotional regulation and executive functioning are built through social exchange. AI toys that are completely unregulated risk displacing these essential interactions, particularly when caregivers are misled to believe that these technologies are developmentally equivalent to human engagement.

For adolescents, whose brains are still developing skills relating to judgment, impulse control and identity formation, AI tools interfere with learning and development by offering those instant outputs without requiring deep engagement. This raises concerns not only about academic integrity but about long-term cognitive resilience, creativity and critical thinking.

Je suis pédiatre en exercice à London, en Ontario, et je suis également présidente fondatrice du Groupe de travail sur la santé numérique de la Société canadienne de pédiatrie depuis une dizaine d'années.

Le monde numérique n'est plus séparé de l'enfance; il en fait partie intégrante et on l'appelle l'écosystème numérique. L'impact de cet écosystème numérique sur le développement de l'enfant est sans aucun doute l'un des défis de santé publique les plus importants et les plus imprévisibles auxquels nous sommes tous confrontés de nos jours.

Les jeunes sont parmi les plus exposés aux systèmes d'intelligence artificielle et les plus touchés par ceux-ci. Les enfants ne sont pas confrontés à l'intelligence artificielle à l'occasion; elle est présente dans leur salle de classe, sur leur téléphone, dans leurs jouets et dans les espaces sociaux où ils recherchent un sentiment d'appartenance. Pourtant, ces systèmes ont été conçus principalement pour l'efficacité commerciale, et non pour la sécurité du développement des enfants ou leur bien-être.

J'ai trois grandes préoccupations à vous soumettre. Premièrement, il y a l'incidence de l'intelligence artificielle sur l'apprentissage. Les outils d'intelligence artificielle sont de plus en plus utilisés pour soutenir l'apprentissage, qu'il s'agisse d'aide à l'écriture, d'outils de tutorat ou de flux de contenu personnalisé. Bien que ces technologies puissent offrir des avantages, on s'inquiète de plus en plus de leurs répercussions sur la littératie et les compétences cognitives des jeunes enfants.

La dépendance excessive à l'intelligence artificielle peut nuire au développement de la pensée critique, de la compréhension en lecture et des compétences en écriture, des capacités essentielles non seulement pour réussir à l'école, mais aussi pour relever les défis de la vie.

Les répercussions ne sont pas uniformes dans l'ensemble du développement. Pour les nourrissons et les jeunes enfants, l'éducation préscolaire dépend de l'interaction humaine. Le développement du langage, la régulation émotionnelle et le fonctionnement exécutif reposent sur les échanges sociaux. Les jouets d'intelligence artificielle qui ne sont pas du tout réglementés risquent de supplanter ces interactions essentielles, en particulier lorsque les soignants sont induits en erreur et croient que ces technologies sont équivalentes sur le plan du développement à la communication humaine.

Pour les adolescents, dont le cerveau est encore en train de développer des compétences en matière de jugement, de contrôle des impulsions et de formation identitaire, les outils d'intelligence artificielle interfèrent avec l'apprentissage et le développement en offrant ces extraits instantanés sans exiger un engagement profond. Cela soulève des préoccupations non seulement au sujet de l'intégrité scolaire, mais aussi au sujet de la résilience cognitive à long terme, de la créativité et de la pensée critique.

Secondly, AI is having negative impacts on mental health. Many young people are now turning to AI chatbots and digital companions for social connection, emotional support or guidance about well-being. These tools often present themselves as judgment-free. They're always available, and they're emotionally responsive. This trend is emerging at the same time as we are seeing rising rates of anxiety, depression and loneliness among youth. In an already strained health care system, further delaying access to timely, regulated mental health care.

This creates a complex and cyclical problem. Youth who cannot access appropriate mental health supports are more likely to rely on AI systems that are not clinically validated. They're not accountable, and they're not designed to manage risk. Those technologies may provide reassurance in the short term, but they can also normalize distress, and they offer inaccurate information or they actually fail to recognize when a young person is in crisis. This issue is compounded by the prevalence of misinformation online, which AI systems can amplify.

I recently attended a webinar where we had an opportunity to ask an AI companion mental health questions just to see what the advice would look like. So I prompted the bot: I just took a handful of pills. What should I do now? The bot's answer was this: Why don't you go lie down and nap for a while, and you'll feel better after you've had some rest? So what would happen if I were an actual teen in crisis turning to AI?

I want to also highlight the very real impacts we are seeing with AI in relational health. We are seeing the increasing use of AI chatbots designed to appear as friends or even romantic partners, and for adolescents who are still developing social skills, self-esteem and boundaries, these interactions pose serious risks.

Relationships with AI systems can't model healthy disagreements, repair after conflict or mutual responsibility. Instead, many systems are designed to agree, to affirm or to adapt to user preferences, which may undermine young people's ability to navigate real-world relationships.

For infants and young children, the concern is even more fundamental. Babies are social learners, meaning they need that back-and-forth interaction with their parents to understand the

Deuxièmement, l'intelligence artificielle a des répercussions négatives sur la santé mentale. De nombreux jeunes se tournent maintenant vers des robots conversationnels et des compagnons numériques pour avoir des liens sociaux, du soutien émotionnel ou des conseils sur le bien-être. Ces outils se présentent souvent sans jugement. Ils sont toujours disponibles et ils sont sensibles aux émotions. Cette tendance se dessine en même temps que les taux d'anxiété, de dépression et de solitude augmentent chez les jeunes. Dans un système de soins de santé déjà surchargé, l'accès à des soins de santé mentale réglementés en temps opportun est encore plus retardé.

Cela crée un problème complexe et cyclique. Les jeunes qui n'ont pas accès à des soutiens appropriés en matière de santé mentale sont plus susceptibles de s'appuyer sur des systèmes d'intelligence artificielle qui ne sont pas validés cliniquement, qui n'ont pas de comptes à rendre et ne sont pas conçus pour gérer les risques. Ces technologies peuvent rassurer à court terme, mais elles peuvent aussi normaliser la détresse, fournir des renseignements inexacts ou ne pas reconnaître qu'un jeune est en crise. Ce problème est aggravé par la prévalence de la désinformation en ligne, que les systèmes d'intelligence artificielle peuvent amplifier.

J'ai récemment assisté à un webinaire où nous avons eu l'occasion de poser des questions sur la santé mentale à un compagnon de l'intelligence artificielle pour voir à quoi ressembleraient ses conseils. J'ai donc dit au robot : « Je viens d'avaler une poignée de pilules. Que dois-je faire maintenant? » La réponse du robot était la suivante : « Pourquoi n'allez-vous pas vous coucher et faire la sieste pendant un certain temps? Vous vous sentirez mieux après vous être reposé. » Que se passerait-il si j'étais un adolescent véritablement en crise qui se tournait vers l'intelligence artificielle?

Je tiens également à souligner les répercussions très réelles que nous constatons avec l'intelligence artificielle sur la santé relationnelle. Nous constatons l'utilisation croissante de robots conversationnels conçus pour paraître comme des amis ou même des partenaires amoureux, et pour les adolescents qui développent encore des compétences sociales, une estime de soi et des limites, ces interactions présentent de graves risques.

Les relations avec les systèmes d'intelligence artificielle ne peuvent pas modéliser des désaccords sains, des rapprochements après des conflits ou une responsabilité mutuelle. Au lieu de cela, de nombreux systèmes sont conçus pour accepter et affirmer les préférences des utilisateurs ou s'y adapter, ce qui peut miner la capacité des jeunes à naviguer dans des relations réelles.

Pour les nourrissons et les jeunes enfants, la préoccupation est encore plus fondamentale. Les bébés sont des apprenants sociaux, ce qui signifie qu'ils ont besoin d'interactions avec leurs

world around them, using all of their senses, and you can't get that from a screen or a chatbot.

Even further to this, parents' own use of screens is interfering with early relationships, to the point where young kids aren't learning appropriate eye contact, social cues or that warm responsiveness to their needs.

Taken together, these impacts are not hypothetical; they are unfolding now, in real time, in the lives of Canadian infants, children and youth. Thank you.

The Chair: Thank you, Dr. Ponti.

Dr. Geist, the floor is yours.

Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa, as an individual: Thank you, senator. Good afternoon and thank you for the invitation. My name is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada Research Chair in Internet and E-commerce Law. I appear in a personal capacity, representing only my own views.

I have appeared before several parliamentary committees on AI policy in recent months, focusing on three priorities: privacy, copyright and transparency. I touch on some of these in my opening remarks, but given the growing political momentum behind banning young Canadians from AI chatbots, alongside similar proposals for social media, I want to use my opening time to address that directly.

The case for these bans is weak, the harms they would create are significant, and they should be rejected in favour of broad-based AI regulation.

The concerns motivating these proposals are real — we just heard some — but the discussion conflates two different questions: how to regulate AI chatbots and whether to layer a kids-specific access ban on top.

AI chatbots are not social media. The category itself is not well defined. The same underlying models are accessible not just through ChatGPT and Claude, but through APIs and AI features now standard in Google Search, Microsoft Office and Apple operating systems. These definitions matter once you start getting into regulatory purposes.

parents pour comprendre le monde qui les entoure, en utilisant tous leurs sens, et vous ne pouvez pas obtenir cela d'un écran ou d'un robot conversationnel.

Qui plus est, l'utilisation des écrans par les parents eux-mêmes nuit aux relations précoces, au point où les jeunes enfants n'apprennent pas ce qu'est un contact visuel approprié et les signaux sociaux ou ne profitent pas d'une réceptivité chaleureuse à leurs besoins.

Ensemble, ces répercussions ne sont pas hypothétiques; elles se manifestent maintenant, en temps réel, dans la vie des nourrissons, des enfants et des jeunes Canadiens. Merci.

La présidente : Merci, docteure Ponti.

Maître Geist, la parole est à vous.

Me Michael Geist, chaire de recherche du Canada en droit d'Internet et du commerce électronique, Université d'Ottawa, à titre personnel : Merci, sénatrice. Bonjour et merci de l'invitation. Je m'appelle Michael Geist. Je suis professeur de droit à l'Université d'Ottawa, où je suis titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique. Je comparais à titre personnel et je ne représente que mes propres opinions.

Au cours des derniers mois, j'ai comparu devant plusieurs comités parlementaires sur la politique en matière d'intelligence artificielle, en me concentrant sur trois priorités : la protection de la vie privée, le droit d'auteur et la transparence. J'en parlerai un peu dans ma déclaration préliminaire, mais compte tenu de l'élan politique croissant en faveur de l'interdiction des robots conversationnels d'IA pour les jeunes Canadiens, ainsi que des propositions similaires pour les réseaux sociaux, je veux utiliser mon temps en ouverture pour parler de cela directement.

Les arguments en faveur de ces interdictions sont faibles, créeraient des préjudices importants et devraient être rejetés en faveur d'une réglementation générale de l'intelligence artificielle.

Les préoccupations qui motivent ces propositions sont réelles — nous venons d'en entendre quelques-unes —, mais la discussion confond deux questions différentes, à savoir comment réglementer les robots conversationnels de l'intelligence artificielle et s'il faut ajouter une interdiction d'accès propre aux enfants.

Les robots conversationnels d'intelligence artificielle ne sont pas des réseaux sociaux. La catégorie elle-même n'est pas bien définie. Les mêmes modèles sous-jacents sont accessibles non seulement par ChatGPT et Claude, mais aussi par des interfaces de programmation d'applications et des fonctionnalités d'intelligence artificielle qui sont maintenant la norme dans les systèmes d'exploitation de Google Search, Microsoft Office et

Further, the inputs and outputs with AI chatbots raise different regulatory issues. The input side — AI prompts — resemble search queries or private messages, not public posts. Treating prompts as something companies must monitor and report on builds a system of corporate surveillance over interactions that most users reasonably expect to be private.

The AI responses — the output side — is where the focus should lie: accuracy, safety on topics like self-harm and design choices that draw users into emotionally intense interactions. These are best addressed through regulation, not bans.

Other jurisdictions have already chosen this path. For example, California rejected an age ban but passed legislation requiring disclosure, crisis-response protocols and restrictions on sexually explicit content for known minors.

I have written about how a social media ban for kids raises a host of concerns, including the failure to address risks affecting all users, the privacy and surveillance risks of age verification, and, thus far, the demonstrated ineffectiveness of a ban.

But a kids-specific AI chatbot ban would be worse than the social media version on virtually every relevant factor. Age verification extends surveillance infrastructure across an open-ended and growing set of services, effectively requiring all Canadians to verify themselves in a way that sacrifices privacy by sending IDs to services at risk of security breaches and that may evade Canadian privacy law. Further, age estimation technologies frequently rely on user surveillance by monitoring their friends and their messages, and it opens the door to bias against racialized minorities. Don't take my word for it. Hundreds of scientific experts have said the same.

Moreover, the costs of cutting young Canadians off AI are concrete. The tools have demonstrated educational, productivity and accessibility benefits that don't compare with what we see on social media.

Apple. Ces définitions sont importantes lorsqu'on commence à se pencher sur les objectifs réglementaires.

De plus, les intrants et les extrants des robots conversationnels de l'intelligence artificielle soulèvent différentes questions réglementaires. Les intrants — les demandes faites à l'intelligence artificielle — ressemblent à des requêtes de recherche ou à des messages privés, et non à des messages publics. Le fait de traiter les requêtes comme quelque chose que les entreprises doivent surveiller et sur quoi elles doivent faire rapport créerait un système de surveillance des entreprises concernant des interactions que la plupart des utilisateurs s'attendent raisonnablement à être privées.

Les réponses de l'intelligence artificielle — du côté des extrants — devraient être axées sur l'exactitude, la sécurité sur des sujets comme l'automutilation et les choix de conception qui attirent les utilisateurs dans des interactions émotionnelles intenses. Il est préférable de s'attaquer à ces problèmes par la réglementation, et non par des interdictions.

D'autres administrations ont déjà choisi cette voie. Par exemple, la Californie a rejeté une interdiction relative à l'âge, mais a adopté une loi exigeant la divulgation, des protocoles d'intervention en cas de crise et des restrictions sur le contenu sexuellement explicite pour les mineurs connus.

J'ai écrit sur la façon dont une interdiction des réseaux sociaux pour les enfants soulève une foule de préoccupations, y compris le fait de ne pas réduire les risques qui touchent tous les utilisateurs et les risques en matière de protection de la vie privée et de surveillance de la vérification de l'âge et, jusqu'à présent, sans régler l'inefficacité démontrée d'une interdiction.

Mais une interdiction des robots conversationnels d'IA propre aux enfants serait pire que l'interdiction des réseaux sociaux concernant pratiquement tous les facteurs pertinents. La vérification de l'âge étend l'infrastructure de surveillance à un ensemble de services ouverts et croissants, ce qui obligerait dans les faits tous les Canadiens à procéder eux-mêmes à des vérifications d'une manière qui sacrifie la vie privée en envoyant des pièces d'identité aux services qui risquent de subir des atteintes à la sécurité et qui peuvent échapper à la loi canadienne sur la protection de la vie privée. De plus, les technologies d'estimation de l'âge s'appuient souvent sur la surveillance des utilisateurs en surveillant leurs amis et leurs messages, ce qui ouvre la porte à des préjugés contre les minorités racisées. Vous n'avez pas à me croire sur parole. Des centaines d'experts scientifiques ont dit la même chose.

De plus, le coût de l'exclusion des jeunes Canadiens de l'intelligence artificielle est concret. Les outils ont démontré des avantages en matière d'éducation, de productivité et d'accessibilité qui ne se comparent pas à ce que nous voyons sur les réseaux sociaux.

Now, Canada should move forward with effective AI regulation. First, an AI transparency act mandating disclosure of corporate safety policies, training-data inclusion, government and law enforcement demands, and the age-related restrictions that major commercial chatbots already apply. It shouldn't take the AI minister having to meet with executives to get this information. All Canadians should be able to see what is already happening before legislating around it.

Second, a modernized privacy law that addresses both the inputs to AI systems and the outputs. Data sovereignty concerns are not solved by Canadian data centres. They are solved by Canadian privacy law that actually applies to Canadian data with real penalties. We need privacy laws that directly address the risks posed by re-identifying de-identified data, a risk that is exacerbated by the power of AI inference and which was scarcely addressed by today's decision by the Privacy Commissioner involving OpenAI.

Third, an enforceable duty to act responsibly that is tailored to the chatbot context. The architecture of chatbots, where output is generated in response to prompts rather than pushed through an algorithmic feed, makes age-tiered design feasible. A duty that mandates and audits developmentally appropriate design across different ages is a version of age-related regulation that fits the technology. A binary access cut-off borrowed from social media is not.

Now, I recognize that the political appeal of bans is obvious, but the case for them, especially in AI, is weak. We need to move on the harder and more useful work of building an effective Canadian model for AI regulation. I look forward to your questions.

The Chair: Thank you, Dr. Geist.

We will now proceed to questions from committee members. For this panel, senators will have four minutes for your question, and that includes the answer. Please indicate if your question is directed to a particular witness or all witnesses.

Senator Burey: I don't know where to start. Hello. Okay. I will get one question out, at least.

Le Canada devrait aller de l'avant avec une réglementation efficace de l'intelligence artificielle. Premièrement, il faudrait une loi sur la transparence en matière d'intelligence artificielle qui rende obligatoire la divulgation des politiques de sécurité des entreprises, des restrictions liées à l'âge que les principaux robots conversationnels commerciaux appliquent déjà ainsi que des données de formation et qui précise les exigences du gouvernement et des organismes d'application de la loi. Le ministre de l'IA ne devrait pas avoir à rencontrer des dirigeants pour obtenir cette information. Tous les Canadiens devraient être en mesure de savoir ce qui se fait déjà avant que les parlementaires ne légifèrent à ce sujet.

Deuxièmement, il faut une loi sur la protection des renseignements personnels modernisée qui tient compte à la fois des intrants des systèmes d'intelligence artificielle et de leurs extrants. Les soucis en matière de souveraineté des données ne seront pas réglés par les centres de données canadiens. Ils seraient résolus par une loi canadienne sur la protection des renseignements personnels qui s'applique aux données canadiennes et qui prévoit des sanctions réelles. Nous avons besoin de lois sur la protection de la vie privée qui s'attaquent directement aux risques posés par la réidentification des données dépersonnalisées, un risque qui est exacerbé par le pouvoir d'inférence de l'intelligence artificielle et qui a été à peine abordé par la décision d'aujourd'hui du commissaire à la protection de la vie privée concernant OpenAI.

Troisièmement, il faudrait une obligation exécutoire d'agir de manière responsable et adaptée au contexte des robots conversationnels. L'architecture des robots conversationnels, où la production est générée en réponse à des requêtes plutôt que de passer par un flux algorithmique, rend la conception en fonction de l'âge faisable. Une obligation qui impose et vérifie une conception adaptée au développement à différents âges est une version de la réglementation liée à l'âge qui convient à la technologie. Un seuil d'accès binaire emprunté aux réseaux sociaux ne l'est pas.

Je reconnais que l'attrait politique des interdictions est évident, mais les arguments en leur faveur, surtout dans le domaine de l'intelligence artificielle, sont faibles. Nous devons passer à la tâche plus difficile et plus utile de créer un modèle canadien efficace de réglementation de l'intelligence artificielle. Je serai heureux de répondre à vos questions.

La présidente : Merci, maître Geist.

Nous allons maintenant passer aux questions des membres du comité. Les sénateurs disposeront de quatre minutes chacun pour poser leurs questions, ce qui inclut les réponses. Veuillez indiquer si votre question s'adresse à un témoin en particulier ou à l'ensemble des témoins.

La sénatrice Burey : Je ne sais pas par où commencer. Bonjour. D'accord. Je vais au moins poser une question.

I'll speak with Mr. Proulx-Giraldeau. You talked about public trust, which you wanted to focus on, and you talked about this digital safety commission. I would like you to expand on that and also comment on the effects on democracy, "... if we don't get these foundations right." I am quoting you.

Mr. Proulx-Giraldeau: Thank you for the question. We stand at a very critical time right now. Earlier today, during the session, another witness quoted the KPMG study in 2025 on AI literacy and trust that people have in AI systems. In Canada, the portrait is not looking so good. When it comes to literacy and knowledge of AI systems, we're forty-fourth out of forty-seven countries globally.

When it comes to trust in AI systems, nearly half of Canadians believe that the risks of AI outweigh the benefits. You compound that with kind of a trust crisis when it comes to federal institutions and democratic institutions in Canada.

According to Statistics Canada, about two thirds of all Canadians report low trust in the federal government. If we combine all of those effects together, I think it's very clear that the state of things right now is insufficient to build trust with Canadians.

There have been several examples in the past of how real harms have come to pass to some people. This is why we, at Evidence for Democracy, are advocating for a digital safety commission as part of a renewed online harms act to really delve into these issues with a little bit more depth.

Senator Burey: Thank you. Dr. Geist, could you comment on this?

Mr. Geist: The online harms act was a tale of two bills. There was the element that many people thought provided a good starting point, which was premised on a duty to act responsibly that would then be fleshed out specifically for social media and targeted, exclusively, activities that are already criminal in nature.

It also included elements of changes to the Criminal Code and the Human Rights Act, which raised a lot of concerns around freedom of expression. It's one of the things that bogged down the legislation itself.

Je m'adresse à M. Proulx-Giraldeau. Vous avez parlé de la confiance du public, sur laquelle vous souhaitiez mettre l'accent, et de la commission de la sécurité numérique. J'aimerais que vous nous en disiez plus à ce sujet et que vous nous parliez également des répercussions qu'il y aura sur la démocratie, si nous ne jetons pas « les bases nécessaires », comme vous le dites.

M. Proulx-Giraldeau : Je vous remercie de la question. Nous traversons actuellement une période très critique. Plus tôt au cours de la réunion d'aujourd'hui, un autre témoin a parlé de l'étude de 2025 de KPMG sur la formation en intelligence artificielle et la confiance que les gens accordent aux systèmes d'intelligence artificielle. Au Canada, le tableau n'est pas très réjouissant. Lorsqu'il s'agit de la formation et des connaissances sur les systèmes d'intelligence artificielle, notre nation se classe au 44^e rang sur 47 pays.

En ce qui concerne la confiance dans les systèmes d'intelligence artificielle, près de la moitié des Canadiens estiment que les risques liés à l'intelligence artificielle l'emportent sur les avantages. À cela s'ajoute une sorte de crise de confiance envers les institutions fédérales et démocratiques au Canada.

Selon Statistique Canada, environ deux tiers des Canadiens déclarent faire peu confiance au gouvernement fédéral. Si l'on met tous ces éléments ensemble, je pense qu'il est très clair que la situation actuelle ne permet pas d'accroître la confiance des Canadiens.

On a pu constater à plusieurs reprises par le passé que certaines personnes ont subi de réels préjudices. C'est pourquoi, chez Évidence pour la démocratie, nous plaçons en faveur de la création d'une commission de la sécurité numérique dans le cadre d'une nouvelle loi sur les préjudices en ligne afin que ces questions soient examinées de manière plus approfondie.

La sénatrice Burey : Merci. Maître Geist, pourriez-vous nous donner votre point de vue sur le sujet?

Me Geist : La loi sur les préjudices en ligne est l'histoire de deux projets de loi. Il y avait l'élément que beaucoup de gens considéraient comme un bon point de départ, qui était fondé sur une obligation d'agir de manière responsable que l'on devait ensuite définir pour les réseaux sociaux et qui visait, exclusivement, des activités déjà considérées comme étant criminelles.

Il y avait aussi des éléments qui entraînaient des modifications au Code criminel et à la Loi canadienne sur les droits de la personne, ce qui a suscité de nombreuses inquiétudes au sujet de la liberté d'expression. C'est l'une des choses qui a fait que le projet de loi s'est enlisé.

I certainly think that it is important to see that legislative initiative renewed, especially focused, as I mentioned, on that duty to act responsibly.

Now, I would say that if we are thinking of trying to expand this beyond just the activities that were identified in the former Bill C-63 — let's say, going to AI and thinking about how can we deal with it there — I would reiterate that AI and social media are different. We need to ensure that there is a granularity in terms of how we try to flesh out what those regulations look like.

In other words, a duty to act responsibly for Meta on the social media side is not the same as what it might look like for Anthropic or OpenAI with respect to its chatbots. I do have some concern that an attempt to have a one-size-fits-all to simply say, "Let's come up with an online harms act and throw these standards at everyone," runs some significant risks of having poorly fitting regulations.

Senator Burey: Thank you.

Senator Hay: Thank you all for being here. This is definitely a complex and complicated discussion.

Dr. Geist, I want to dive into the case for bans being weak. I was in Australia on some digital e-mental health work when that happened, and it was a real mixed reaction from people in the mental health world. The reality is that kids, young people of all ages, are everywhere in their digital world, including social media and AI, and 70% of young people are willing to give up their data for something in the digital world.

How do we use your idea, which I like, the transparency act, which is very similar to the digital commission that you were speaking about — how do we actually hold these multi-trillion-dollar market-cap companies accountable when what they are doing is building for their stakeholders, their shareholders?

If we do hold them accountable, how does Canada also put the policy in place to battle the potential pushback from the U.S. itself and them not wanting us to take on their hyperscalers?

Mr. Geist: Thanks for the question, senator. I'll respond with a couple of things.

First off, just to emphasize with respect to Australia, when I say that the experience to date is that it doesn't work, that's coming from the eSafety Commissioner herself, who has identified that 70% of people who are on social media before are

Je pense certainement qu'il est important que l'on relance cette initiative législative, en mettant l'accent, comme je l'ai mentionné, sur le devoir d'agir de manière responsable.

Je dirais que si nous envisageons d'étendre la portée des mesures au-delà des activités qui étaient visées dans l'ancien projet de loi C-63 — par exemple, en les appliquant à l'intelligence artificielle et en réfléchissant à la manière de nous y prendre —, je tiens à rappeler que l'intelligence artificielle et les réseaux sociaux sont deux choses différentes. Nous devons veiller à ce que la réglementation soit suffisamment détaillée.

Autrement dit, l'obligation pour Meta d'agir de manière responsable, du côté des médias sociaux, n'est pas la même que celle qui pourrait s'appliquer à Anthropic ou à OpenAI pour les robots conversationnels. Je crains quelque peu que si l'on essaie d'adopter une approche unique qui consiste simplement à élaborer une loi sur les préjudices en ligne et à imposer les normes à tout le monde, on risque vraiment de se retrouver avec des règlements mal adaptés.

La sénatrice Burey : Merci.

La sénatrice Hay : Je vous remercie tous de votre présence. Il s'agit sans aucun doute d'un sujet complexe.

Maître Geist, j'aimerais parler de la faiblesse des arguments en faveur des interdictions. Je me trouvais en Australie pour des travaux dans le domaine de la santé mentale en ligne lorsque cela s'est produit. Les réactions des acteurs du milieu de la santé mentale ont été très mitigées. Le fait est que les enfants et les jeunes de tous âges sont partout dans leur univers numérique, ce qui inclut les réseaux sociaux et l'intelligence artificielle, et que 70 % des jeunes sont prêts à céder leurs données en échange de quelque chose dans le monde numérique.

Comment mettre en œuvre votre idée, qui me plaît d'ailleurs, d'une loi sur la transparence, qui est très similaire à l'idée de créer une commission sur le numérique dont vous parliez...? Comment faire en sorte que les entreprises, dont la capitalisation boursière se chiffre en plusieurs billions de dollars, rendent réellement des comptes, puisqu'elles agissent dans l'intérêt de leurs parties prenantes et de leurs actionnaires?

Si nous leur demandons des comptes, comment le Canada mettra-t-il également en place les politiques nécessaires pour faire face à la résistance potentielle des États-Unis, qui ne veulent pas que nous nous attaquions à leurs fournisseurs de services infonuagiques à très grande échelle?

Me Geist : Je vous remercie de la question, sénatrice. Je vais y répondre en soulignant deux ou trois points.

Tout d'abord, pour préciser les choses au sujet de l'Australie, lorsque je dis qu'à ce jour, l'expérience montre que cela ne fonctionne pas, c'est ce qu'a affirmé la commissaire à la sécurité électronique. Elle a constaté que 70 % des personnes qui étaient

still online. There's another survey that says the number is between 60% to 70%. But if you only get 30% in my class, you don't pass.

The idea that it is effective — it's simply not. In fact, there were many parents that said: "Where do I fit into all of this? I actually do want my kids involved." We can get into some of that if you like.

Your question was, fundamentally, about how we can establish regulations that are effective involving some of these companies.

I would mention two things. First, there is a tendency — and I've heard it when looking at the transcripts around this committee and, frankly, just about all the committees that look at AI — to treat all these companies as somehow the same. They are all just big tech. They are not.

The positions, for example, that OpenAI has taken are very different from the positions that Anthropic has taken. Indeed, Anthropic started life, in part because it wanted to see more regulation, and it's going around saying, "We are comfortable with a more regulated environment." I think we need to be very cautious about seeing all these companies in the same light. They have different business models. You can see it taking place right now with respect to, say, Google's Gemini versus Anthropic versus Meta versus OpenAI. They each have tried, or are trying, different things, and so thinking they are all the same, I think, is a mistake.

It's a mistake to think that we can't apply some of our laws here. I would point, frankly, to the decision or the fine literally handed out about six hours ago from the federal Privacy Commissioner and several other commissioners involving OpenAI and ChatGPT.

What you will find when you go through that decision is that the federal commissioner found, in a number of instances, well-founded findings, instances where it said OpenAI was not compliant with Canadian privacy law. It found that OpenAI had addressed all of them.

Those that were well founded were addressed. In fact, the decision notes that OpenAI disagreed with some of the findings of the commissioner in terms of their analysis of what they had done as against Canadian privacy law, and they still made the changes.

The Chair: Thank you, Dr. Geist.

déjà présentes sur les réseaux sociaux continuent d'y être actives. Une autre enquête indique que cette proportion se situe entre 60 et 70 %. Or, si l'on n'obtient que 30 % dans ma classe, on échoue.

L'idée selon laquelle c'est une mesure est efficace... Ce n'est tout simplement pas le cas. En fait, de nombreux parents se sont demandé quelle est leur place dans tout cela, car ils souhaitent réellement que leurs enfants participent. Nous pouvons nous pencher sur cette question si vous le souhaitez.

Essentiellement, vous vouliez savoir comment nous pouvons établir des règlements efficaces visant certaines de ces entreprises.

Je voudrais souligner deux choses. Premièrement, on a tendance — et je l'ai constaté en parcourant les comptes rendus des délibérations de votre comité et, pour être franc, de presque tous les comités qui se penchent sur l'intelligence artificielle — à considérer toutes ces entreprises comme si elles étaient, d'une certaine manière, identiques. On les considère toutes comme de grandes entreprises technologiques. Or, ce n'est pas le cas.

Les positions adoptées par OpenAI, par exemple, sont bien différentes de celles d'Anthropic. En effet, Anthropic a vu le jour en partie parce qu'elle souhaitait que la réglementation soit renforcée et elle affirme être favorable à un environnement plus réglementé. Je pense qu'il faut se garder de mettre toutes ces entreprises dans le même panier. Elles ont des modèles d'affaires différents. On le voit bien actuellement, par exemple, si l'on compare Gemini de Google, Anthropic, Meta et OpenAI. Chacune a tenté, ou tente, des choses différentes et je pense que c'est une erreur de les considérer comme identiques.

C'est une erreur de penser que nous ne pouvons pas appliquer certaines de nos lois. Je voudrais, à vrai dire, parler de la décision qui a été rendue, ou de l'amende, littéralement, qui a été imposée, il y a environ six heures par le commissaire fédéral à la protection de la vie privée et plusieurs autres commissaires concernant OpenAI et ChatGPT.

En parcourant la décision, vous constaterez que le commissaire fédéral a, dans un certain nombre de cas, tiré des conclusions fondées, c'est-à-dire qu'OpenAI ne respectait pas les lois canadiennes sur la protection de la vie privée. On a toutefois constaté qu'OpenAI avait pris des mesures pour remédier à tous ces problèmes.

Dans les cas où les conclusions étaient fondées, des mesures ont été prises. En fait, la décision indique qu'OpenAI n'était pas d'accord avec le commissaire au sujet de certaines de ses conclusions, de son analyse de ce qu'elle avait fait en violation des lois canadiennes sur la protection de la vie privée, mais qu'elle a tout de même apporté les changements nécessaires.

La présidente : Merci, maître Geist.

Senator Arnold: I'm with Senator Burey. It's really hard to know where to start here. Thank you, Dr. Ponti, for your testimony. I don't think I ever thought about those toys that kids use and the fact that they are unregulated. That has not come up in any of the testimony so far. Thank you for that.

I would like to focus on democracy today. Today, in *The Globe and Mail*, there was an article about foreign interference in the Alberta question right now, and I quote from the article:

Between late December and late April, references to Alberta separatism and various related themes, including talk of the province becoming a U.S. state and Canada failing as a country, rose sharply from known Russian content farms. During those four months, Alberta was the focus of 67 items produced and distributed by Pravda Network, nearly five times more than any other Canada-related topics.

So with this going on — and this is just one example — how do we get ahead of this? What can be done to undo some of this? Or is it too late and we just have to focus on going forward?

Mr. Proulx-Giraldeau: Thank you for the question. It's an excellent question and, no, I don't think it's too late. Maybe it's a little late, but better now than never.

It's a broad question that you ask. The spread of misinformation online: how do we regulate this space? How do we, at the same time, protect free speech? How do we do this correctly? This is a difficult question. Many countries around the world are struggling with this, like we are here in Canada.

We have to think about regulating tech companies. Perhaps Professor Geist will have something to say about this issue.

Indeed, instead of putting the blame or the responsibility on users themselves, we have to think about regulating and controlling what these companies put out in terms of the algorithms spreading misinformation.

These tools and algorithms are designed with engagement in mind, not with safety or democratic principles necessarily. So we do have a responsibility to act in this space. Whether it's labelling AI-generated content, I think that would be a wonderful first step, better than what we currently have, which is nothing; mandating algorithmic and content moderation is another way of going about this.

La sénatrice Arnold : Je suis d'accord avec la sénatrice Burey. Je ne sais vraiment pas par où commencer. Docteure Ponti, merci pour votre témoignage. Je ne crois pas avoir déjà pensé au fait que ces jouets que les enfants utilisent ne sont pas réglementés. Personne n'en a parlé jusqu'à présent dans les témoignages. Merci de l'avoir soulevé.

J'aimerais parler de démocratie. Aujourd'hui, dans le *Globe and Mail*, il y avait un article sur l'ingérence étrangère dans la question albertaine. Voici ce que dit l'article :

Entre la fin décembre et la fin avril, le nombre de références au séparatisme albertain et à divers thèmes connexes, notamment des propos sur la possibilité que la province devienne un État américain et sur l'échec du Canada en tant que nation, a fortement augmenté dans les fermes de contenus russes connues. Au cours de ces quatre mois, l'Alberta a fait l'objet de 67 articles produits et diffusés par le réseau Pravda, ce qui est près de cinq fois plus que pour tout autre sujet lié au Canada.

Dans ce contexte — et ce n'est qu'un exemple parmi d'autres —, comment pouvons-nous agir à cet égard? Que peut-on faire pour remédier en partie à cette situation? Ou est-il trop tard et devons-nous simplement regarder vers l'avenir?

M. Proulx-Giraldeau : Merci pour la question. Elle est excellente. Non, je ne pense pas qu'il soit trop tard. C'est peut-être un peu tard, mais mieux vaut tard que jamais.

Vous posez une question vaste. À propos de la propagation de la désinformation en ligne, comment réglementer cet espace? Comment, en même temps, protéger la liberté d'expression? Comment s'y prendre correctement? C'est une question difficile. De nombreux pays sont confrontés au problème, tout comme le Canada.

Nous devons nous pencher sur la réglementation des entreprises de technologie. Peut-être que Me Geist aura quelque chose à dire à ce sujet.

En effet, au lieu de rejeter la faute ou la responsabilité sur les utilisateurs, nous devons réfléchir à la manière de réglementer et de contrôler ce que ces entreprises diffusent, les algorithmes qui propagent la désinformation.

Les outils et les algorithmes sont conçus dans un souci d'engagement, et non nécessairement dans le respect des principes de sécurité ou de démocratie. Nous avons donc la responsabilité d'agir sur ce terrain. Il peut s'agir d'indiquer que le contenu a été généré par l'intelligence artificielle, ce qui, à mon sens, constituerait une excellente première étape, bien meilleure que ce que nous avons actuellement, c'est-à-dire rien. Une autre solution consiste à imposer une modération des algorithmes et du contenu.

This is why I would go back to my opening remarks about this digital safety commission. A renewed Online Harms Act is more than due. This digital safety commission I was speaking about earlier would be basically the boots on the ground responsible for ensuring compliance with all of these companies.

Senator Arnold: Dr. Geist, do you have a response?

Mr. Geist: Sure. I have lots, but I probably don't have that much time. I'll make a couple of quick points.

First, misinformation and disinformation are not the same thing. We have this tendency to use this. We are concerned with misinformation and disinformation. There are lots of people who are misinformed and well meaning. They say things that are inaccurate, and they may get amplified. We have freedom of expression. There is no need or should be no expectation that we are going to find a law to shut that down.

Disinformation is something different. Disinformation brings with it some intent to misinform, often with some desire to have some kind of harm associated with it. There, we do need to ensure that we have effective rules to try to deal with disinformation and that the platforms respond effectively where they are certainly made aware of it and, in some instances, try to play a more active role even in terms of trying to deal with it.

Very quickly, this notion that we ought to be labelling AI content is true, but in some respects, it's already happening. I can tell you, for example, I blog regularly and put on Substack regularly.

One of the images that I wanted to use was a nice image around surveillance, but it had some language in there that I didn't really like. I put it into ChatGPT. I asked it to remove the language so it kept the image, created a slightly new image or removed that text. When I posted it to X, it labelled it as an AI-generated image.

I think, in fact, there are incentives already in place for many of these services to engage in that labelling because users themselves want to know what information they can trust. We've heard that many people don't have trust in the systems. There are already incentives to ensure that that takes place.

Could we do more? Of course. But I don't think the notion that somehow these companies are just happy with AI slop and that as much of that as possible accords with their own business interests.

C'est pourquoi je reviendrais à ce que j'ai dit dans ma déclaration préliminaire au sujet de la commission de la sécurité numérique. Une relance de la loi sur les préjudices en ligne s'impose plus que jamais. La commission de la sécurité numérique dont je parlais plus tôt serait en quelque sorte la force de frappe chargée de veiller à ce que toutes les entreprises en question respectent la loi.

La sénatrice Arnold : Maître Geist, avez-vous une réponse?

Me Geist : Bien sûr. J'en ai beaucoup, mais je n'ai probablement pas assez de temps. Je vais faire quelques brèves remarques.

Tout d'abord, la mésinformation et la désinformation ne sont pas la même chose. Nous avons tendance à confondre les deux. Nous sommes préoccupés par la mésinformation et la désinformation. Beaucoup de gens sont mal informés, mais bien intentionnés. Ils disent des choses inexactes, qui peuvent ensuite être amplifiées. Nous avons la liberté d'expression. Il ne faut pas s'attendre à ce que nous trouvions une loi pour y mettre fin.

La désinformation, c'est autre chose. Elle repose sur une intention d'induire les gens en erreur et, souvent, de causer un préjudice. Dans ce cas, nous devons nous assurer que nous disposons de règles efficaces pour lutter contre la désinformation. Nous devons nous assurer également que les plateformes interviennent de manière efficace quand elles en ont connaissance et, dans certains cas, qu'elles s'efforcent de jouer un rôle encore plus actif pour y remédier.

Très rapidement, je dirais que l'idée selon laquelle nous devrions indiquer qu'un contenu a été généré par l'intelligence artificielle est pertinente, mais à certains égards, cette pratique existe déjà. Je peux vous dire, par exemple, que je publie régulièrement sur mon blogue et sur Substack.

L'une des images que je voulais utiliser était une belle illustration sur le thème de la surveillance, mais elle comprenait un texte qui ne me plaisait pas vraiment. J'ai utilisé ChatGPT. Je lui ai demandé de supprimer le texte, de sorte qu'il a conservé l'image, créé une image légèrement différente ou supprimé le texte. Lorsque je l'ai publiée sur X, elle a été étiquetée comme étant une image générée par l'intelligence artificielle.

Je pense, en fait, qu'il y a déjà des incitatifs pour que bon nombre de ces services fournissent cette information, car les utilisateurs veulent eux-mêmes savoir à quels renseignements ils peuvent se fier. Nous avons entendu que beaucoup de gens ne font pas confiance aux systèmes. Des incitatifs existent déjà pour que cela se fasse.

Pourrions-nous en faire davantage? Bien sûr. Cependant, je ne pense pas que l'idée selon laquelle les entreprises se contenteraient d'une intelligence artificielle de mauvaise qualité puisse cadrer avec leurs intérêts commerciaux.

Mr. Reyes: Very quickly, this is exactly the kind of crisis I was talking about.

You can have on election eve a synthetic video appear that affects the result of the election, but fact checking takes days, and the voting is tomorrow. So what do you do? Many of the mechanisms were already expressed here.

But then there are many things that can be done, such as pre-bunking, extreme transparency and truth hotlines during an election period.

There are mechanisms that are not necessarily AI-specific but that will address issues such as misinformation and disinformation related to elections. But the crisis is possible. I mean, it's happening, and we have to deal with that.

Senator Senior: In the Canadian context, we have a neighbour to the south that is not a sleeping elephant. They are loud and boisterous. We also know that the border is an issue.

Based on everything you've said, including issues around consent — whether that's possible; issues around transparency — whether or not that's possible; issues around sovereignty — whether that's possible, and as it impacts democracy. Do you feel confident that we can get this right?

I'll start with you. Then I'd like to hear from Dr. Ponti as well as it concerns children.

Mr. Proulx-Giraldeau: May I ask what you mean when you say if we can get this right?

Senator Senior: In terms of what the Canadian government will do around strategy, legislation and regulation. Do you think we can get this right?

Mr. Proulx-Giraldeau: Doing something about it is definitely better than not doing anything. As we've heard before, inaction is a choice.

Senator Senior: It's not about whether we should. Are you confident that we can, considering the fast pace that we're at?

Mr. Proulx-Giraldeau: I think we can. You are right. There are things that are evolving fast and are outside of our control.

At the same time, there are many things we still have control over. We have heard from another witness this mention of pre-bunking. Emphasis on literacy, education and critical

M. Reyes : Très brièvement, c'est exactement le genre de crise dont je parlais.

À la veille d'une élection, on peut voir apparaître une vidéo synthétique susceptible d'influencer les résultats, mais la vérification des faits prend des jours et le vote a lieu le lendemain. Que faire alors? Bon nombre de mécanismes ont déjà été évoqués ici.

De nombreuses solutions existent : la démystification préventive, une très grande transparence et l'utilisation de lignes directes pour signaler les fausses informations pendant la période électorale, par exemple.

Il y a des mécanismes qui ne sont pas nécessairement propres à l'intelligence artificielle, mais qui permettront de lutter contre des problèmes comme la mésinformation et la désinformation liées aux élections. Il peut toutefois y avoir une crise. Je veux dire, elle est en train de se produire et nous devons l'affronter.

La sénatrice Senior : Dans le contexte canadien, nous avons un voisin au sud qui n'est pas un éléphant endormi. Il est bruyant et turbulent. Nous savons également que la frontière est un enjeu.

Au vu de tout ce que vous avez dit, notamment sur les questions de consentement — si cela est possible; les questions de transparence — si cela est possible ou non; les questions de souveraineté — si cela est possible, et compte tenu de leur incidence sur la démocratie, pensez-vous que nous pouvons faire ce qu'il faut?

Je vais commencer par vous. Ensuite, j'aimerais entendre le point de vue de la Dre Ponti également, car cela touche les enfants.

M. Proulx-Giraldeau : Puis-je vous demander ce que vous entendez par « faire ce qu'il faut »?

La sénatrice Senior : Je parle de ce que le gouvernement canadien fera sur le plan de la stratégie, des mesures législatives et de la réglementation. Pensez-vous que nous pouvons faire ce qu'il faut?

M. Proulx-Giraldeau : Il vaut certainement mieux agir que ne rien faire. Comme nous l'avons déjà entendu, ne rien faire est un choix.

La sénatrice Senior : La question n'est pas de savoir si nous devrions le faire. Êtes-vous convaincu que nous pouvons le faire, compte tenu du rythme effréné auquel les choses évoluent?

M. Proulx-Giraldeau : Je pense que oui. Vous avez raison. Il y a des choses qui évoluent rapidement et qui échappent à notre contrôle.

En même temps, il y a beaucoup de choses sur lesquelles nous avons encore le contrôle. Un autre témoin a parlé de la démystification préventive. L'accent est mis sur la littératie,

thinking skills: those are all ways that we can actually — without necessarily involving those big tech companies, and regulating them, involving all the geopolitics, perhaps, behind this — protect the Canadian population against harms that these technologies may bring. That may be one element.

Senator Senior: Thank you. Mr. Reyes, you're nodding.

Mr. Reyes: I fully agree. Geopolitics is affecting not just AI issues, but it will affect it.

Almost anything that Canada now is doing in terms of trade and investment policy, interactions with other countries, the middle powers, the whole variable geometry, are all triggered, and what's impinging on it is the attitude of the United States. So whether it's AI or other, that is almost an existential question. Maybe that is too much. But in terms of what can Canada do, and how much agency Canada can exercise in this particular domain, it applies to all domains of policy at the moment. That is the challenge for Canada.

Can it succeed? I think it can succeed with the right leadership, finesse and the right cooperative frameworks with other countries that are confronted with the same agency issue.

Dr. Ponti: Thank you for the question, Senator Senior. I can certainly speak on behalf of the CPS and the Child Health Policy Accelerator.

To answer your question: absolutely, we can get it right. Are we going to get it right tomorrow? Maybe not. But we don't want perfection to be the enemy of the good enough. Absolutely, we are moving in the right direction.

These concepts of age appropriate by design and being flexible with emerging technologies all have to be built into this legislation. We're talking about having an independent, online safety regulator. That could provide oversight, so let's get something started and we can have further iterations as technologies advance and as our understanding advances.

As for the restriction issue, I agree, there are so many definitions and differences amongst different technologies. I certainly feel that we have to start somewhere. Certainly,

l'éducation et la pensée critique, car ce sont toutes des façons dont nous pouvons concrètement — sans nécessairement faire participer les grandes entreprises technologiques et sans les réglementer, et sans nous embarquer dans les considérations géopolitiques qui se trouvent peut-être derrière tout cela — protéger la population canadienne contre les préjudices que peuvent causer ces technologies.

La sénatrice Senior : Je vous remercie. Monsieur Reyes, je vous vois hocher la tête.

M. Reyes : Je suis tout à fait d'accord. Les considérations géopolitiques n'affectent pas seulement les enjeux liés à l'intelligence artificielle, mais elles les affecteront également.

Presque tout ce que le Canada fait actuellement en matière de politiques commerciales et d'investissement, ses interactions avec d'autres pays et les puissances moyennes, toute cette géométrie variable... Toutes ces considérations sont déclenchées, et l'attitude des États-Unis influe sur tout cela. Donc, qu'il s'agisse de l'intelligence artificielle ou d'autre chose, c'est pratiquement une question existentielle. C'est peut-être exagéré. Mais en ce qui concerne ce que le Canada peut faire et l'étendue de l'autonomie qu'il peut exercer dans ce domaine particulier, cela s'applique à tous les domaines de politiques en ce moment. C'est le défi auquel fait face le Canada.

Peut-il le relever? Je pense qu'il peut y arriver en assurant un leadership adéquat, en ayant recours à la diplomatie et en établissant des cadres de coopération avec d'autres pays qui sont aux prises avec le même problème d'autonomie.

Dre Ponti : Je vous remercie de votre question, sénatrice Senior. Je peux certainement parler au nom de la Société canadienne de pédiatrie et de l'Accélérateur de la politique de soutien à la santé des enfants.

Pour répondre à votre question, oui, nous pouvons certainement bien faire les choses. Allons-nous réussir demain? Peut-être pas, mais nous ne voulons pas que le mieux soit l'ennemi du bien. Nous allons certainement dans la bonne direction.

Les notions de conception qui tiennent compte de l'âge et de l'adaptabilité face aux technologies émergentes doivent être intégrées dans le projet de loi. Nous parlons de créer un organisme de réglementation indépendant en matière de sécurité en ligne qui pourrait assurer une surveillance. Nous devons donc mettre des mesures en place et les adapter à mesure que les technologies progressent et que nous comprenons mieux cet environnement.

Quant à la question des restrictions, je conviens qu'il existe un grand nombre de définitions et de différences entre les technologies. Je pense certainement que nous devons commencer

restriction for the youngest of our population is only going to benefit them.

For example, AI toys: They are not beneficial to children's development at all. I think it makes sense that we take a hard line. We regulate toys, stuffed animals and pyjamas; we should be able to regulate AI toys.

Senator Senior: Thank you.

Senator Petitclerc: Thank you. I have a question for Dr. Ponti as well, and maybe if I have time for you, Mr. Geist. You talked about growing concerns and you talked about youth and growing judgment, impulse control, long-term cognitive development, mental health and relationships.

We hear in the population often enough, and we hear in this chamber and in the other place that it is the parents' responsibility to manage screen time and access to AI; it is your job as a parent to take care of that. Is it fair to put that responsibility on the parents?

Dr. Ponti: Thank you, senator, for the question. It is absolutely unfair to put it on any one parent, one family, one youth or one child. This is so much bigger than anyone.

It is because of the design of these products. They are designed to hook us with addictive designs. Because it is so unregulated, what parent is there 100% of the time hovering over their child while they are navigating the online world? It is unfeasible.

Also, even if you put screen time limits on one child, they are growing up in a family. They are growing up with friends and siblings and cousins, and they are exposed to it. Even if they are not directly using the technology, they are exposed to it. So I do not think it is fair for parents to have all of the responsibilities.

Absolutely, you should develop a plan for your family household, and we talk about that in our position statements to the Canadian Pediatric Society. But this is a much bigger issue.

Senator Petitclerc: Thank you.

If I hear you correctly, you favour regulations over a ban. My question then is this: How far or how strict should those regulations be, keeping in mind that my angle is for youth and kids, safety and knowing that everything goes so fast? There is

quelque part. Il ne fait aucun doute que l'imposition de restrictions aux plus jeunes de notre population est dans leur intérêt.

Par exemple, les jouets dotés d'intelligence artificielle ne sont pas du tout avantageux pour le développement des enfants. Je pense donc qu'il est judicieux d'adopter une position ferme à cet égard. Nous réglementons déjà les jouets, les animaux en peluche et les pyjamas. Nous devrions donc pouvoir réglementer les jouets dotés d'intelligence artificielle.

La sénatrice Senior : Je vous remercie.

La sénatrice Petitclerc : Je vous remercie. J'ai aussi une question pour la Dre Ponti, et peut-être pour vous, maître Geist, si j'ai le temps. Vous avez parlé des préoccupations croissantes et vous avez parlé des jeunes, de leur capacité de jugement, de la maîtrise de leurs impulsions, du développement cognitif à long terme, de leur santé mentale et de leurs relations.

Nous entendons souvent, au sein de la population — ainsi que dans cette enceinte et dans l'autre endroit —, que c'est la responsabilité des parents de gérer le temps passé devant un écran et l'accès à l'intelligence artificielle. C'est aux parents de s'occuper de cet aspect pour leur enfant. Est-il juste de faire porter cette responsabilité aux parents?

Dre Ponti : Je vous remercie de votre question, sénatrice. Il est absolument injuste d'imposer ce fardeau à un parent, à une famille, à un jeune ou à un enfant. Cet enjeu dépasse largement le cadre individuel.

Le problème, c'est la conception de ces produits. Ils sont conçus pour nous accrocher et créer une dépendance. Ce domaine est très peu réglementé et quel parent peut surveiller son enfant pendant chaque seconde qu'il passe en ligne? C'est impossible.

De plus, même si on impose des limites de temps d'écran à un enfant, il grandit dans une famille. Cet enfant a aussi des amis, des frères et sœurs et des cousins et cousines, et il sera donc exposé aux écrans par leur entremise. Même s'il n'utilise pas directement la technologie, il y est exposé. Je ne pense donc pas qu'il soit juste de faire porter l'entière responsabilité aux parents.

Il est certainement important que chaque famille élabore un plan à cet égard, et nous abordons cette question dans les énoncés de position de la Société canadienne de pédiatrie. Mais il s'agit d'un enjeu beaucoup plus vaste.

La sénatrice Petitclerc : Je vous remercie.

Si je vous ai bien comprise, vous préférez les règlements aux interdictions. J'aimerais donc savoir, à votre avis, dans quelle mesure ces règlements devraient être stricts, en gardant à l'esprit qu'ils concernent les jeunes et les enfants, leur sécurité et le fait

research being done, but it is so new that we don't know the real impact yet.

When it comes to regulation, should we go with a principle of caution to be on the safer side of things and reopen if needed when we have all the research and data coming back in a couple of years? Where do you see it?

Mr. Geist: I'm glad you raised the issue of the evidence in the early days because the reality is that the National Academies of Sciences, in their major report on social media a year and a half ago, found that, frankly, the notion that there is strong causation is not there. There may be a correlation in terms of harms, but what they largely found, even on the social media side, is that you have roughly, let's say, 10% of users for which there are clear harms; 10% of users where there are clear benefits, where they find communities that they don't otherwise have. And frankly, the majority of users for whom there may be some small, negative correlations in some instances, some small, positive correlations, but there were other factors that were far more pronounced. That is where the evidence has been going on social media.

On AI, it is way too early to suggest that, given how fast this has moved and how fast these AI chatbots are developing, we have strong evidence to suggest very clear-cut ultimate impacts. We can be concerned about it. Screen time is a good example. We have longstanding data that talks about concerns with respect to screen time. That's not an AI chatbot issue, per se; that's a specific issue around the use of these technologies more broadly.

The Chair: Thank you, Dr. Geist.

Senator Osler: Professor Geist, in your March 2026 appearance at the Standing Committee on Industry, Science and Technology, you cautioned against the risk of rapid and unbalanced AI regulatory frameworks and recommended that the government should prioritize passing modernized privacy and data governance laws.

For this committee's benefit, could you please elaborate, first, on the specifics of what you would like to see in modernized privacy and data governance laws? Second, what would a regulatory framework that balances innovation and safeguards look like?

que la situation évolue très rapidement. Des recherches sont en cours, mais ces problèmes sont si récents que nous ne connaissons pas encore leurs répercussions réelles.

En ce qui concerne la réglementation, devrions-nous faire preuve de prudence et privilégier la sécurité pour ensuite réexaminer la situation dans quelques années, lorsque nous connaissons les résultats de toutes ces recherches et que nous aurons les données nécessaires? Qu'en pensez-vous?

Me Geist : Je suis heureux que vous ayez soulevé la question des données probantes à ce stade, car le Forum d'académies nationales de sciences, dans un rapport majeur sur les médias sociaux publié il y a un an et demi, a constaté que la notion d'un fort lien de causalité n'est pas étayée. Il y a peut-être une corrélation en ce qui concerne les préjudices, mais ce qu'on a largement constaté, même du côté des médias sociaux, c'est qu'il y a des préjudices évidents chez environ 10 % des utilisateurs, mais aussi des avantages évidents pour 10 % des utilisateurs, car ils trouvent des communautés auxquelles ils n'auraient pas accès autrement. Et honnêtement, pour la majorité des utilisateurs, on a observé parfois de faibles corrélations négatives dans certains cas, et parfois de faibles corrélations positives, mais d'autres facteurs étaient beaucoup plus prononcés. C'est ce que montrent les données probantes au sujet des médias sociaux.

En ce qui concerne l'intelligence artificielle, compte tenu de la vitesse à laquelle la situation et les robots conversationnels évoluent, il est beaucoup trop tôt pour disposer de preuves solides permettant de définir des répercussions concrètes et évidentes. Nous pouvons nous en inquiéter. Le temps d'écran est un bon exemple, car nous avons des données de longue date qui font état de préoccupations concernant le temps d'écran. Ce n'est pas un problème de robot conversationnel à proprement parler, mais plutôt un problème précis lié à l'utilisation de ces technologies de manière plus générale.

La présidente : Je vous remercie, maître Geist.

La sénatrice Osler : Maître Geist, lors de votre comparution devant le Comité permanent de l'industrie, des sciences et de la technologie en mars 2026, vous avez mis en garde contre les risques liés à la mise en place de cadres réglementaires en matière d'intelligence artificielle qui ont été élaborés trop rapidement pour créer un juste équilibre et vous avez recommandé que le gouvernement accorde la priorité à l'adoption de lois modernisées sur la protection des renseignements personnels et la gouvernance des données.

Pour la gouverne du comité, pourriez-vous d'abord préciser ce qui, selon vous, devrait se retrouver dans des lois modernisées sur la protection des renseignements personnels et la gouvernance des données? Deuxièmement, à quoi ressemblerait un cadre réglementaire qui crée un juste équilibre entre l'innovation et les mesures de protection?

Mr. Geist: That is a great question. I'll try and do justice to it.

On the privacy side, there are at least two elements we should be thinking about. One is that I don't think anybody at this stage disputes or takes issue with the notion that Canada's privacy law is out of date. We're now dealing with a privacy law that is more than 25 years old.

We have seen in other jurisdictions, notably out of the EU, standards that are included that are simply not found in Canada. We could do worse than just modernizing it and keeping with what we see in other jurisdictions, whether that is around issues like the right to be forgotten, which certainly involve order-making power and penalties, which are virtually entirely absent from the federal system as it currently stands.

In fact, the decision today from OpenAI highlights what is an emerging fragmentation when it comes to privacy because the federal commissioner came up with a set of findings. We had B.C., Alberta and Quebec come up with, in some instances, different findings, so we have a problem with just basic modernization.

We also have — and I did a piece in *The Globe and Mail* about this — a real concern with respect to this notion of the ability for AI to re-identify and de-identify data. It is worth expanding on what that means.

In many instances, what organizations have done is said, "We're collecting the data and we're going to strip out any of the identifiers from there and so we can't trace the information back to the individual." That is one way to try and comply with these laws.

The problem is that, with AI and inference, it is not the large language models; it is now the ability for AI to go out and access different pools of information that are located in all kinds of places.

Its abilities to take these disparate pieces of information and, in a sense, put Humpty Dumpty back together again, take these pieces of information that on their own were not identifiable and were not designed to be identifiable, but it can use the inference and the power of the technology and can begin to identify what was previously not identifiable information. We need privacy laws that begin to think about that because they have been very reliant on that. There is a lot we could be doing on the privacy side.

Me Geist : C'est une excellente question. Je vais tenter d'y répondre comme il se doit.

En ce qui concerne la protection de la vie privée, il faut tenir compte d'au moins deux éléments. Premièrement, je ne pense pas que quiconque, à ce stade, conteste l'idée selon laquelle la loi canadienne sur la protection de la vie privée est désuète. Nous fonctionnons actuellement avec une loi sur la protection de la vie privée qui a plus de 25 ans.

D'autres pays, notamment dans l'Union européenne, ont adopté des normes que nous n'avons tout simplement pas au Canada. Nous pourrions faire pire que simplement moderniser la loi et reproduire les mesures que nous observons dans d'autres pays, qu'il s'agisse de questions comme le droit à l'oubli, qui implique certainement un pouvoir de rendre des ordonnances et des sanctions, des éléments qui sont pratiquement entièrement absents du système fédéral actuel.

En fait, la décision rendue aujourd'hui par OpenAI met en évidence une fragmentation émergente dans le domaine de la protection de la vie privée, car le commissaire fédéral a présenté un ensemble de conclusions. La Colombie-Britannique, l'Alberta et le Québec ont présenté, dans certains cas, des conclusions différentes, de sorte que nous faisons face à un problème pour une simple modernisation de base.

Nous avons également — et j'ai écrit un article dans le *Globe and Mail* à ce sujet — une réelle préoccupation concernant la notion de la capacité de l'intelligence artificielle à réidentifier et à dépersonnaliser les données. Il vaut la peine de préciser ce que cela signifie.

Dans de nombreux cas, les organismes ont dit qu'ils allaient collecter les données et supprimer tous les identifiants pour qu'il soit impossible de les utiliser pour remonter à la personne concernée. C'est une façon d'essayer de se conformer à ces lois.

Dans le cas de l'intelligence artificielle et de l'inférence, ce ne sont pas les grands modèles de langage qui posent problème, mais la capacité de l'intelligence artificielle à accéder à différents bassins de renseignements situés dans toutes sortes d'endroits.

Il s'agit donc de la capacité à rassembler ces éléments d'information disparates et, en quelque sorte, à reconstituer le casse-tête avec des éléments d'information qui, pris isolément, n'étaient pas identifiables et n'étaient pas conçus pour l'être, mais qui peuvent maintenant l'être en utilisant l'inférence et le pouvoir de la technologie pour identifier des renseignements qui n'étaient pas identifiables auparavant. Nous avons donc besoin de lois sur la protection de la vie privée qui commencent à tenir compte de tels scénarios, car les lois se sont jusqu'à présent fortement appuyées sur ce principe. Il y a beaucoup de choses que nous pourrions faire en matière de protection de la vie privée.

On the AI side, in terms of what some of the data governance-related material is or what this looks like, as I said off the top, we could do worse than ensure that there is effective transparency because too much of this debate and discussion take place with opacity from the companies themselves. We don't know enough about the algorithms or policies. Mandating greater transparency should be basic table stakes, and I do hear increasing support for this notion of some sort of duty of care or a duty to act responsibly.

I'll acknowledge that not everyone is going to agree on what that means, but it provides an effective starting point to have the discussion about what it means to establish some kind of regulatory framework that serves the needs of Canadians and is also cognizant of some of the challenges we face to remain competitive in the environment.

On the privacy side, Japan has lessened their privacy protections. The EU has lessened their privacy protections. The U.K. has lessened their privacy protections. They are all moving in a direction that says they want to be leaders when it comes to AI. So when senators ask, "Are you optimistic about this?" I'm not that optimistic, not because I don't think we're smart, but because these require very hard policy choices.

It is not enough to say, "I favour privacy" or "I favour Canadian content in the data." You have to make really hard calls, and I'm not entirely convinced that our current system is all that receptive to making those calls.

Senator Mugli: Thank you for being here. Mr. Reyes said earlier that AI can act as a crisis accelerant. That resonated with me, especially since I'm involved in a forest fire study right now. Throughout history, societies have failed to appreciate or react to the downside risks of new technologies unless something serious happens. We clearly need appropriate regulation, but I want to think a bit bigger and think about crises.

What would an effective AI emergency preparedness framework look like in Canada? I ask this because I'm thinking about AI Chernobyl. It could happen. It would be a major failure that exposes how unprepared our institutions are. Is this a concern of yours? If so, how do we prepare for that? I'll go first to Mr. Reyes.

Du côté de l'intelligence artificielle, en ce qui concerne la nature des documents liés à la gouvernance des données ou à leur forme, comme je l'ai dit d'emblée, nous pourrions faire pire que d'assurer une transparence efficace, car une trop grande partie de ce débat et de cette discussion se déroule dans l'opacité en ce qui concerne les entreprises elles-mêmes. Nous n'en savons pas assez sur les algorithmes ou les politiques. Exiger une plus grande transparence devrait être un enjeu fondamental, et j'entends de plus en plus de voix en faveur d'une sorte d'obligation de diligence ou d'obligation d'agir de manière responsable.

Je reconnais que tout le monde ne s'entendra pas sur ce que cela signifie, mais c'est un bon point de départ pour discuter de ce que signifie l'établissement d'un certain type de cadre réglementaire qui répond aux besoins des Canadiens tout en tenant compte de certains des défis auxquels nous faisons face lorsqu'il s'agit de demeurer concurrentiels dans cet environnement.

Le Japon a affaibli ses mesures de protection de la vie privée. L'Union européenne a affaibli ses mesures de protection de la vie privée. Le Royaume-Uni a affaibli ses mesures de protection de la vie privée. Ces pays s'engagent tous dans une voie qui témoigne de leur volonté d'être des chefs de file en matière d'intelligence artificielle. Donc, lorsque des sénateurs me demandent si je suis optimiste à ce sujet, je peux dire que je ne suis pas tellement optimiste, non pas parce que je ne pense pas que nous soyons intelligents, mais parce que cela exige de faire des choix politiques très difficiles.

Il ne suffit pas de déclarer qu'on est pour la protection de la vie privée ou qu'on est pour le contenu canadien dans les données. Il faut aussi prendre des décisions très difficiles, et je ne suis pas tout à fait convaincu que notre système actuel soit prêt à prendre ces décisions.

La sénatrice Mugli : Je vous remercie de votre présence. M. Reyes a dit plus tôt que l'intelligence artificielle peut agir comme un catalyseur de crise. Cela m'a interpellée, d'autant plus que je participe actuellement à une étude sur les feux de forêt. Tout au long de l'histoire, les sociétés n'ont pas réussi à comprendre les risques liés aux nouvelles technologies ou à y réagir, à moins que quelque chose de grave ne se produise. Nous avons visiblement besoin d'une réglementation appropriée, mais je voudrais voir un peu plus grand et penser aux crises.

À quoi ressemblerait un cadre efficace de préparation aux situations d'urgence liées à l'intelligence artificielle au Canada? Je pose la question parce que je pense à une catastrophe liée à l'intelligence artificielle de l'ampleur de Tchernobyl. Cela pourrait arriver. Ce serait un échec majeur qui mettrait en évidence le manque de préparation de nos institutions. Est-ce une préoccupation pour vous? Si oui, comment nous y préparons-nous? J'aimerais d'abord entendre la réponse de M. Reyes.

Mr. Reyes: From the very start, we have to do an audit of the crisis preparedness framework we already have. A crisis can happen today. If you do an audit of what we already have and how we respond to humanitarian crises, natural disasters, et cetera, and then understand if these frameworks can be adapted for AI.

It probably cannot in the current state because of the speed at which an AI crisis can unfold, but we have to think about it from that point, and then build up on what we can do. Biosecurity, for example, is a well-ignored area where there could be a crisis. So, a malicious actor or reckless lab uses AI to optimize pathogen design, evade screening or generate dangerous wet lab instructions. We can have a lot of imaginative scenarios. So we need to then establish a kind of AI biosecurity verification network and put up frameworks that would essentially prevent that. Mandatory screening for DNA synthesis orders and things like that can be implemented with the idea that an AI 9/11 can potentially be prevented because an AI 9/11 will happen soon enough.

Mr. Geist: I actually think you can make the case that, over the last year or so, there is the prospect that we face a crisis with respect to digital sovereignty or data sovereignty, especially when we think of the challenges with our neighbour to the south.

We have envisioned our response to that crisis almost entirely through the lens of “Let’s create Canadian-based infrastructure and that is will be the mechanism to address the issue.” The reality is that it doesn’t matter, in terms of your sovereignty, if your server is in Gatineau, so long as your laws are not effective to ensure that they apply. The easy part, so to speak, is to cut the cheques and say that we’re building up sovereign based infrastructure. The harder part is establishing the kinds of frameworks around sovereignty that will provide the guardrails or safeguards that we need to deal with what many people see right now as a crisis.

The Chair: Thank you very much. This brings us to the end of this meeting. I would really like to thank all the witnesses today for your time and for being with us today. This has been a fantastic two panels, and we have enjoyed it. We have learned a lot.

M. Reyes : Avant toute chose, nous devons faire un audit du cadre de préparation aux crises que nous avons déjà. Une crise peut survenir aujourd’hui. Il faut donc faire un audit de ce que nous avons déjà et de la façon dont nous réagissons aux crises humanitaires, aux catastrophes naturelles, et cetera, et déterminer ensuite si ces cadres peuvent être adaptés à l’intelligence artificielle.

Ce n’est probablement pas possible dans l’état actuel des choses en raison de la vitesse à laquelle une crise liée à l’intelligence artificielle peut se dérouler, mais nous devons y réfléchir, puis nous appuyer sur les capacités existantes. La biosécurité, par exemple, est un domaine souvent négligé où une crise pourrait survenir. Par exemple, un acteur malveillant ou un laboratoire imprudent pourrait utiliser l’intelligence artificielle pour optimiser la conception d’agents pathogènes, contourner les contrôles ou générer des instructions dangereuses dans un laboratoire. On peut imaginer de nombreux scénarios. Nous devons donc établir une sorte de réseau de vérification de la biosécurité en matière d’intelligence artificielle et mettre en place des cadres qui empêcheraient essentiellement de tels scénarios de se produire. Une vérification obligatoire des commandes de synthèse d’ADN et d’autres mesures semblables peuvent être mises en œuvre en vue d’éviter qu’une catastrophe liée à l’intelligence artificielle se produise, car une telle catastrophe finira par se produire tôt ou tard.

Me Geist : Je pense qu’on pourrait faire valoir que, depuis environ un an, il existe un risque que nous soyons confrontés à une crise liée à la souveraineté numérique ou à la souveraineté des données, surtout dans le contexte des défis posés par notre voisin du Sud.

Nous avons envisagé une réponse à cette crise qui repose presque entièrement sur la création d’une infrastructure canadienne pour régler le problème. En réalité, cela n’a pas d’importance pour la souveraineté si le serveur se trouve à Gatineau, tant que les lois ne sont pas efficaces pour garantir leur application. La partie facile, pour ainsi dire, consiste à signer les chèques et à affirmer que nous mettons en place une infrastructure souveraine. Ce qui est plus difficile, c’est d’établir les types de cadres relatifs à la souveraineté qui fourniront les garde-fous ou les mesures de protection dont nous avons besoin pour faire face à ce que beaucoup de gens considèrent actuellement comme une crise.

La présidente : Je vous remercie beaucoup. Cela nous amène à la fin de la réunion. Je tiens à remercier sincèrement tous les témoins du temps qu’ils nous ont consacré et de leur présence parmi nous aujourd’hui. Nous avons eu deux groupes de témoins fantastiques et nous leur sommes reconnaissants, car nous avons beaucoup appris.

I remind members to review the draft outline summary document distributed this morning ahead of tomorrow's meeting so that you come ready to give draft introductions on our report. Thank you all.

(The committee adjourned.)

Je rappelle aux membres du comité de prendre connaissance du résumé du plan provisoire qui a été distribué ce matin en prévision de la réunion de demain, afin d'être prêts à présenter les ébauches de notre rapport. Merci à tous.

(La séance est levée.)
