

# ISED Reply and follow up to Associate Deputy Minister Schaan's appearance at the Senate Standing Committee on Social Affairs, Science and Technology (SOCI) on February 25, 2026

## Réponse et suivi de l'ISDE à la comparution du sous-ministre délégué Schaan devant le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie le 25 février 2026

### Question 1

**Senator Hay:** My question may be controversial. I want to pick up on social media that was talked about earlier and algorithms that are being built, safety councils big companies invite organizations to be on — I'll call that performative, not authentic — and I'm going to be very cynical here.

Our ability to hold these multi-trillion market cap companies to account as they're building algorithms that drive young people to services like a KHP, how will we hold those multi-trillion-dollar market caps to account? If they can build algorithms to drive what they're driving right now, for sure they can build algorithms for safety. For sure they can, and they're not.

I guess that's my question. How do we hold them to account?

### Answer 1

Response provided by Canadian Heritage:

The Government of Canada is examining options for a future online safety regime that would focus on reducing the risk of harm on large platforms, particularly for children and other vulnerable users. Such regulatory approaches typically rely on expert regulators to set standards, monitor compliance, and use enforcement tools where necessary.

To advise on this proposal, the Government has recently reconvened the Expert Advisory Group on online safety, whose members previously contributed to the development of previous online harms legislation, to engage on new and emerging issues related to online harms. Any future legislative proposal would be subject to parliamentary scrutiny, and details will be made public at the appropriate time.

### Question 1

**Sénatrice Hay:** Ma question pourrait être controversée. Je veux revenir sur les médias sociaux dont il a été question plus tôt et sur les algorithmes qui sont en train d'être construits, les conseils de sécurité que les grandes entreprises invitent les organisations à joindre — je vais appeler ça du performatif pas de l'authentique — et je vais être très cynique ici.

Notre capacité à tenir ces entreprises aux capitalisations boursières de plusieurs trillions responsables alors qu'elles développent des algorithmes qui poussent les jeunes vers des services comme un JJE, comment allons-nous tenir ces entreprises de plusieurs trillions de dollars responsables? S'ils peuvent concevoir les algorithmes qui dirigent actuellement, ils peuvent certainement créer des algorithmes pour la sécurité. Ils le peuvent certainement et ils ne le font pas.

Je suppose que c'est ma question. Comment est-ce qu'on peut les tenir responsables?

## Réponse 1

Réponse fournie par Patrimoine canadien :

Le gouvernement du Canada examine actuellement différentes options en vue de la mise en place d'un régime de sécurité en ligne qui viserait à réduire les risques de préjudice sur les grandes plateformes, en particulier pour les enfants et les autres utilisateurs vulnérables. De telles approches s'appuient généralement sur des régulateurs experts chargés d'établir des normes, de surveiller la conformité et de recourir à des mesures coercitives si nécessaire.

Pour donner des conseils sur cette proposition, le gouvernement a convoqué de nouveau le groupe consultatif d'experts sur la sécurité en ligne dont les membres ont contribué au développement de la précédente proposition législative sur les contenus préjudiciables en ligne pour discuter des enjeux nouveaux émergents reliés aux préjudices en ligne. Toute future proposition législative sera soumise à l'examen du Parlement, et les détails seront rendus publics en temps voulu.

## Question 2

**Senator McPhedran:** My question comes from looking at the European Union Artificial Intelligence Act of 2024, which has a tiered approach and is very definitely geared to the protection of humans. My question is where in the federal department or federal departments is the work being done on legislation to protect Canadians? Not policy, not principles, not guardrails, but legislation.

## Answer 2

Artificial intelligence (AI) is a general-purpose technology being adopted across all sectors of the economy which means that it can be regulated through horizontal, cross-cutting measures, and through targeted sectoral regulations to address risks arising from deployment in certain contexts. At present, a number of departments and agencies are responsible for federal statutes that regulate AI's development, deployment, and use.

The following departments and agencies are non-exhaustive and demonstrate some of the ways existing legal frameworks interact with high-risk AI systems, but their application depends on the circumstances specific to each case.

- The Department of Justice Canada is responsible for the *Criminal Code*, which prohibits all aspects of child sexual abuse and exploitation material, including making or distributing it (s. 163.1). Section 163.1 defines "child sexual abuse and exploitation material" to include, among other things, any visual representation that shows a child engaged in an explicit sexual activity, or whose dominant characteristic is the depiction, for a sexual purpose, of a sexual organ or the anal region of the child. This definition applies to AI-generated and AI-altered material if it meets the statutory elements.
- The Office of the Privacy Commissioner (OPC) enforces the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which governs how organizations collect, use, and disclose personal information in the course of commercial activities at the federal level. Similar laws and regulators exist at the provincial and territorial level. Where the OPC is of the opinion that a developer or deployer of an AI system is violating PIPEDA, it may enter into a compliance agreement with the organization to ensure compliance or, on application to the Federal Court, seek an order for the organization to correct its practices (ss. 15 to 16, 17.1 to 17.2).
- The Competition Bureau investigates businesses that, in the course of commercial activities, violate the *Competition Act*, including through the use of algorithmic pricing software in ways that adversely affect competition in Canada. For example, the Bureau recently conducted a civil investigation into whether RealPage Canada, Inc. and Yardi Canada, Ltd. abused a dominant position or entered into anticompetitive collaboration, in contravention of ss. 79 and 90.1 of the Act, through their algorithmic

rental housing pricing software. Civil violations of the Act are brought by the Bureau before the Competition Tribunal and criminal violations are prosecuted by the Public Prosecution Service of Canada.

- The Department of Finance Canada is responsible for legislation regulating how federally-regulated financial institutions (FRFIs) operate. FRFIs are generally required to adhere to investment and lending policies, standards, and procedures to avoid undue risk of loss and obtain a reasonable return (e.g., *Bank Act*, s. 465). They are also required to establish and adhere to policies and procedures to protect themselves against threats to their integrity and security (*Bank Act*, s. 15.1.) The Office of the Superintendent of Financial Institutions (OSFI) is responsible for the supervision of FRFIs, including through issuing guidance, including, where it deems necessary, with respect to the use of AI systems by FRFIs, and has investigatory, order-making, and administrative monetary penalty powers (*Bank Act*, ss. 628, 635, 643, 645, 648; *OSFI Act*, ss. 24 to 37.01). For example, the OSFI may order a bank to cease the deployment or use of an AI system where its use causes the bank to incur an undue risk of loss.

Furthermore, the Government has broad powers to protect the health and safety of Canadians, including against the potential risks of AI. Where a person uses AI as a tool to commit an offence, such as extortion, fraud, identify theft, or intimidation with violence or threats of violence, that person can be held criminally liable in the same way as if they had not used the AI. In addition, the *Criminal Code* provides that anyone else who knowingly facilitates, counsels or incites a person to commit such an offence may also be found guilty of that offence as a participant in it, including, depending on the facts, a corporation that has manufactured and made the AI system available. In cases where an AI system is considered a medical device under the *Food and Drugs Act*, Health Canada may request that the manufacturer conduct a recall if it believes that the system presents a serious or imminent risk of injury to health, and may order a recall if the manufacturer does not take appropriate action. Cybersecurity threats amplified by AI, such as large-scale phishing or ransomware, are crimes under the *Criminal Code*. These types of activities are not only crimes but are also of concern to the Communications Security Establishment and the Canadian Centre for Cyber Security, which provide threat monitoring, incident response, and active cyber operations to disrupt hostile foreign capabilities. Federal, provincial, and territorial governments also have emergency powers that could in principle be applied in extreme circumstances.

## Question 2

**Sénatrice McPhedran:** Ma question vient de l'examen de la Loi sur l'intelligence artificielle de l'Union européenne de 2024, qui adopte une approche par paliers et est très clairement axée sur la protection des humains. Ma question est de savoir dans quel ministère fédéral ou quels ministères fédéraux le travail est en cours sur la législation visant à protéger les canadiens? Pas sur les politiques, pas sur les principes, pas sur les garde-fous, mais sur la législation.

## Réponse 2

L'intelligence artificielle (IA) est une technologie à usage général qui est adoptée dans tous les secteurs de l'économie, ce qui signifie qu'elle peut être encadrée par des mesures horizontales et transversales, ainsi que par des réglementations sectorielles ciblées visant à atténuer les risques découlant de son déploiement dans certains contextes. À l'heure actuelle, plusieurs ministères et organismes sont responsables de lois fédérales qui régissent le développement, le déploiement et l'utilisation de l'IA.

Les ministères et organismes suivants constituent une liste non exhaustive et illustrent certaines des façons dont les cadres juridiques existants s'appliquent aux systèmes d'IA à risque élevé; leur application dépend toutefois des circonstances propres à chaque cas.

- Le ministère de la Justice Canada est responsable de la *Code criminel* interdit tous les aspects liés au matériel d'abus et d'exploitation pédosexuels, y compris sa production ou sa distribution (art. 163.1). L'article 163.1 définit le « matériel d'abus et d'exploitation pédosexuels » comme comprenant, entre autres, toute représentation visuelle montrant un enfant se livrant à une activité sexuelle explicite ou

dont la caractéristique dominante est la représentation, dans un but sexuel, d'un organes sexuels ou de la région anale de l'enfant. Cette définition s'applique au matériel généré ou modifié par l'IA s'il répond aux critères légaux.

- Le Commissariat à la protection de la vie privée veille à l'application de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui règlementent la manière dont les organisations collectent, utilisent et divulguent les renseignements personnels dans le cadre de leurs activités commerciales au niveau fédéral. Des lois et des organismes de réglementation similaires existent au niveau provincial et territorial. Lorsque le Commissariat estime qu'un développeur ou un déployeur d'un système d'IA enfreint la LPRPDE, il peut conclure avec l'organisation intéressée un accord de conformité visant à faire respecter la Loi ou, sur demande à la Cour fédérale, demander une ordonnance pour que l'organisation revoir ses pratiques en vue de se conformer à la Loi (art. 15 à 16, 17.1 à 17.2).
- Le Bureau de la concurrence enquête sur les entreprises qui, dans le cadre de leurs activités commerciales, enfreignent la *Loi sur la concurrence*, notamment en utilisant des logiciels de tarification algorithmique d'une manière qui nuit à la concurrence au Canada. Par exemple, le Bureau a récemment mené une enquête civile afin de déterminer si RealPage Canada, Inc. et Yardi Canada, Ltd. ont abusé d'une position dominante ou conclu une collaboration anticoncurrentielle, en violation des articles 79 et 90.1 de la Loi, par le biais de leur logiciel algorithmique de tarification des logements locatifs. Les infractions civiles à la Loi sont portées devant le Tribunal de la concurrence par le Bureau, tandis que les infractions criminelles sont poursuivies par le Service des poursuites pénales du Canada.
- Le ministère des Finances Canada est responsable des lois qui règlementent le fonctionnement des institutions financières fédérales (IFF). Les IFF sont tenues de se conformer aux principes, normes, et procédures en matière de placements et de prêts afin d'éviter des risques de perte indus et d'assurer un juste rendement (p. ex. *Loi sur les banques*, art. 465). Elles sont également tenues d'établir et de respecter des politiques et des procédures visant à se protéger contre toute menace à leur intégrité et à leur sécurité (*Loi sur les banques*, art. 15.1). Le Bureau du surintendant des institutions financières (BSIF) est chargé de la surveillance des IFF, notamment en publiant des consignes, y compris, lorsqu'il le juge nécessaire, en ce qui concerne l'utilisation des systèmes d'IA par les IFF, et dispose de pouvoirs d'enquête, de prise de décisions et d'imposition de sanctions administratives pécuniaires (*Loi sur les banques*, art. 628, 635, 643, 645, 648 ; *Loi sur le BSIF*, art. 24 à 37.01). Par exemple, le BSIF peut ordonner à une banque de cesser le déploiement ou l'utilisation d'un système d'IA lorsque son utilisation expose la banque à un risque de perte indu.

De plus, le gouvernement dispose de vastes pouvoirs pour protéger la santé et la sécurité des Canadiens, y compris contre les risques potentiels liés à l'IA. Lorsqu'une personne utilise l'IA comme outil pour commettre une infraction, telle que l'extorsion, la fraude, le vol d'identité ou l'intimidation avec violence ou menaces de violence, cette personne peut être tenue pénalement responsable de la même manière que si elle n'avait pas utilisé l'IA. En outre, le *Code criminel* prévoit que toute autre personne qui, sciemment, facilite, conseille ou incite une personne à commettre une telle infraction peut également être reconnue coupable de cette infraction en tant que participante, y compris, selon les faits, une société qui a fabriqué et mis à disposition le système d'IA. Dans les cas où un système d'IA est considéré comme un instrument médical en vertu de la *Loi sur les aliments et drogues*, Santé Canada peut demander au fabricant de procéder à un rappel s'il estime que le système présente un risque grave ou imminent de préjudice à la santé, et peut ordonner un rappel si le fabricant ne prend pas les mesures appropriées. Les menaces à la cybersécurité amplifiées par l'IA, telles que le phishing ou les ransomwares à grande échelle, constituent des infractions au *Code criminel*. Ces types d'activités sont non seulement des infractions, mais elles préoccupent également le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité, qui assurent la surveillance des menaces, la réponse aux incidents et des cyberopérations actives visant à interrompre les capacités hostiles étrangères. Les gouvernements fédéral, provinciaux et territoriaux disposent également de pouvoirs d'urgence qui pourraient en principe être appliqués dans des circonstances extrêmes.

### Question 3

**Senator Senior:** I really appreciate your openness and the sharing of information. Thank you for that. Related to the last two questions, I'm more relating it to the strategy. I don't know if you can speak to this because I know it's supposed to be out the first quarter of this year. Will the strategy be inclusive of accountability? Possibly legislation? I would like to get a sense of what the strategy will cover and then, more specifically, was the strategy inclusive of equity-seeking groups and organizations as well as gender?

### Answer 3

The Government launched a 30-day national sprint in October 2025 to inform the renewal of Canada's AI strategy. This included an open public consultation, direct engagements with dozens of key stakeholders, and the creation of the AI Strategy Task Force, made up of 28 Canadian AI experts from civil society, industry, academia and research, who each submitted reports at the conclusion of the Sprint.

Safe AI systems and public trust were key themes explored by the Task Force. Task Force reports emphasized the need for transparent accountability, governance and public engagement, and the establishment of oversight mechanisms to monitor AI deployments. There was also widespread support for streamlined regulatory frameworks that include tiered risk assessments, secure data-sharing protocols, and clear standards for privacy and cybersecurity to ensure that both public- and private-sector AI initiatives are deployed safely and responsibly.

In addition to the expert advice of the Task Force, the Government received over 11,300 submissions from the public during the Sprint, including several from key equity-seeking organizations and associations in Canada, including Indigenous groups, Black Canadian associations, and disability advocacy organizations. Further details on the inputs received during the consultation period can be found in [Engagements on Canada's next AI Strategy: Summary of Inputs](#), published last month on Canada.ca. Raw data from the online consultation is also available on the [Open Government Portal](#).

The Government will present the AI Strategy shortly and it will contemplate key measures to respond to the concerns raised by Canadians.

### Question 3

**Sénatrice Senior :** J'apprécie vraiment votre ouverture et le partage d'informations. Merci pour cela. En lien avec les deux dernières questions, je les relie davantage à la stratégie. Je ne sais pas si vous pouvez en parler parce que je sais qu'elle devrait être publiée au cours du premier trimestre de cette année. La stratégie inclura-t-elle des mesures de responsabilité? Possiblement une législation? J'aimerais avoir une idée de ce que couvrira la stratégie et, plus précisément, si la stratégie prend en compte les groupes et organisations recherchant l'équité ainsi que les questions de genre.

### Réponse 3

Le gouvernement a lancé un sprint national de 30 jours en octobre 2025 afin d'informer le renouvellement de la stratégie canadienne en matière d'IA. Cette initiative comprenait une consultation publique ouverte, des échanges directs avec des dizaines de parties prenantes clés, ainsi que la création du Groupe de travail sur la stratégie en matière d'IA, composé de 28 experts canadiens en IA issus de la société civile, de l'industrie, du milieu académique et de la recherche, qui ont chacun soumis un rapport à la conclusion du sprint.

La sécurité des systèmes d'IA et la confiance du public ont été des thèmes centraux explorés par le Groupe de travail. Les rapports du Groupe de travail ont mis en évidence la nécessité d'une reddition de comptes transparente, d'une gouvernance et d'un engagement public accrus, ainsi que de la mise en place de mécanismes de surveillance pour suivre les déploiements d'IA. Un large soutien s'est également manifesté en

faveur de cadres réglementaires simplifiés comprenant des évaluations de risques à plusieurs niveaux, des protocoles sécurisés de partage de données, ainsi que des normes claires en matière de protection de la vie privée et de cybersécurité, afin de garantir que les initiatives d'IA des secteurs public et privé soient déployées de manière sûre et responsable.

En plus des conseils d'experts du Groupe de travail, le gouvernement a reçu plus de 11 300 soumissions du public durant le sprint, dont plusieurs émanant d'organisations et d'associations représentant des groupes en quête d'équité au Canada, notamment des groupes autochtones, des associations de Canadiens noirs et des organisations de défense des droits des personnes handicapées. De plus amples détails sur les contributions reçues durant la période de consultation sont disponibles dans le document [Mobilisation au sujet de la prochaine stratégie: Résumé des contributions](#), publié le mois dernier sur Canada.ca. Les données brutes de la consultation en ligne sont également disponibles sur le [Portail du gouvernement ouvert](#).

Le gouvernement présentera la stratégie en matière d'IA sous peu, laquelle envisagera des mesures clés pour répondre aux préoccupations soulevées par les Canadiens et Canadiennes.