Office of the
Saskatchewan Information
and Privacy Commissioner

Update on Children's Privacy and AI Legislation/Privacy Guidelines in Canada

Presentation to the Attorney General of Saskatchewan

April 27, 202600

Grace Hession David
Saskatchewan Information and Privacy Commissioner

Update on Children's Privacy and AI Legislation/Privacy Guidelines in Canada

Grace Hession David
Saskatchewan Information and Privacy Commissioner
(April 27, 2026)

The purpose of this brief is to inform as to the impending federal Artificial Intelligence (AI) legislation and the various statutes and guidelines released by other provinces and the privacy offices across Canada. The concern with online AI involves several issues – especially as they relate to children. Deepfakes, sextortion and the invasion of privacy are now concerns that were not on the radar even five years ago. It is hoped that this research will assist in future discussion within the Ministry of Justice. The Saskatchewan Office of the Information and Privacy Commissioner (OIPC) is pleased to assist since this issue is one of significant importance to our office and to the federal/provincial privacy offices across Canada.

TAB 1: Joint Statement on AI Generated Imagery and the Protection of Privacy (February 26, 2026)

The co-signatories of the world-wide privacy offices have produced a concise listing of the fundamental principles that must guide all organizations developing and using AI content. These principles should form the basics of any proposed legislation:

(1) Safeguards must be implemented to prevent the misuse of personal information and generation of non-consensual intimate imagery and other harmful materials, especially when children are depicted.

(2) Meaningful transparency must be ensured with respect to AI capabilities, safeguards, acceptable uses and the consequences of misuse.

(3) Effective and accessible mechanisms must be provided for individuals to request the removal of harmful content involving personal information which will allow for a rapid response to the request.

(4) The specific risks to children must be addressed through the provision of clear, age-appropriate information easily comprehended by children, parents, guardians, and educators alike.

Federal: *Proposed*: Online Harms Act.

New legislation is pending and it will likely reframe *Bill C-63* (Online Harms Act, 2024) that was tabled in the House of Commons on February 26, 2024. The debate in the House of Commons stalled after a second reading that was preempted and terminated following the prorogation of Parliament on January 6, 2025. The bill was heavily criticized for its definitions of hate-speech.

Bill C-63 was drafted to address seven categories of harm: 1) sexual victimization of children; 2) revictimization online; 3) non-consensual intimate online content; 4) online bullying; 5) content promoting self-harm; 6) hate speech; and 7) incitement of violence.

The bill would have required social media operators to follow four duties of care all outlined in Part 4 of the Act: 1) the duty to act responsibly – section 54; 2) the duty to protect children online – sections 64 to 66; 3) the duty to make certain content inaccessible – sections 67 to 71; 4) the duty to keep records -section 71.

On January 23, 2026, Minister of Artificial Intelligence, Evan Solomon, announced that the federal government is planning to introduce a new online harms bill. The new bill will focus on child online safety. There has been discussion of the introduction of a social media ban for children under 14 but there is great debate on the effectiveness of such a ban. Australia has banned social media for anyone under 16 and a recent survey of the effectiveness of this ban indicated that 70% of children still using restricted sites, easily circumvent the ban. (**TAB 2** – Molly Rose Foundation – Research Briefing, April 2026)

TAB 3: Safe AI and the Public Trust

On January 22, 2026 Minister of AI and Digital Innovation, Evan Solomon, announced the creation of Canada's National AI Task Force. Professor Taylor Owen of McGill University submitted a paper on his theme of Safe AI and the Public Trust. His concerns with ungoverned AI in Canada include the prevalence of mis- and dis-information (deepfakes); non-consensual image generation; impersonation (leading to stalking and sextortion); race and gender-based stereotyping

and manipulation of users through engagement optimization. These factors are of grave concern and all affect children. Professor Owen's statistics show that 89% of Canadians worry about their privacy with AI and 70% are concerned about children and their use of chatbots. 88% of Canadians support stronger governance of AI systems and 85% want government oversight to ensure safe and ethical use. 80% believe that there should be serious penalties for AI-generated deepfakes. Professor Owen's research revealed that AI systems are designed, deployed, and monetized by private actors (most of them in the U.S.), who bear little legal responsibility for the risks their systems create.

TAB 4: March 2026 Report of the Office of the Privacy Commissioners of Canada and the UK.

This report studied 464 websites and 400 mobile applications favoured by children all over the world. The report focused on how these sites/apps collect children's personal information, whether they use age assurance mechanisms, whether they employ privacy control to limit the collection of data and whether they are transparent with respect to their privacy practices. The research showed that online services do not consider the best interests of children. Children can be tracked online, profiled, targeted and exposed to inappropriate/harmful content. Perhaps the most interesting finding of this report was that 62% of the websites surveyed explicitly limited access to users over a certain age – usually 13 years of age. Of these websites 32% employed no technique to determine age and 88% used self-declaration which was very easily circumvented (pages 5 to 6). The most disturbing aspect of this report is the survey of websites/apps that contain inappropriate content and high-risk data capture features. Bullying, abusive or hateful content was found in 15% of the services while sexual content appeared in 11% and content related to self-harm in 7%. This content can appear in user-generated sections of the sites, in chat functions as well as the result of algorithmic feed. (pages 13 to 14).

TAB 5: ***Strengthening Cyber Security and Building Trust in the Public Sector Act****, 2024,* S.O. 2024, c. 24 (Bill 194) (Assented to November 25, 2024)

As of July 1, 2025 this Act enacted several changes to the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) in Ontario. The most important amendment involved a statutory mandated requirement for provincial institutions to report privacy breaches to the Information and Privacy Commissioner of Ontario. The privacy breaches are to be assessed on a threshold of "real risk of significant harm". This threshold considers the sensitivity of the personal information, the probability of misuse, and whether the affected individual can take steps to mitigate the possible harm. Provincial institutions are now required to notify affected individuals if the breach is assessed at a real risk of significant harm. Prior to this legislation, the situation in Ontario was like Saskatchewan where the reporting of a privacy breach was voluntary. We recommend a similar amendment to the Saskatchewan legislation. At the moment, privacy breaches are reported to the Saskatchewan OIPC on a random basis and only on the part of the truly excellent government/municipal/health care citizens. Early reporting allows our organization to assist in the containment of the breach and notification of victims. We would rather assist in this key area than review from afar.

TAB 6: **Bill 194: Ontario's Missed Opportunity to Lead on AI** (Patricia Kosseim)

The Ontario Information and Privacy Commissioner critiqued the new legislation by noting that it failed to enshrine the foundational principles of safe and transparent AI legislation. Instead, the legislation took the easy way out and simply authorized the minister to make rules by way of regulation – which to date have not been enacted. The foundational pillars of AI legislation include:

1) AI systems must be trustworthy and reliable. They should undergo testing and prove their reliability for the purpose for which they are designed.

2) AI systems must be safe and protect the physical/mental health, property and financial security of those who use them.

3) AI must be developed using a "privacy by design" framework. Safety measures must be developed from the beginning to minimize data collection (including personal information), reduce privacy and security risks, and ensure personal information is required only when necessary.

4) Stakeholders must be transparent in their use of AI and explain to their users how AI is incorporated into the system.[1]

5) AI systems require independent oversight.

TAB 7: Principles for the Responsible Use of Artificial Intelligence

January 2026, the Ontario Information and Privacy Commissioner along with the Ontario Human Rights Commission issued *"Principles for the Responsible Use of Artificial Intelligence"*. This report recommended six excellent principles for the use of AI systems that protect system users – especially children:

(1) **Valid and Reliable:** AI systems must exhibit valid, reliable and accurate outputs for the purpose for which they are designed, used or implemented.

(2) **Safe:** AI must be developed, acquired, adopted and governed to prevent harm or unintended harmful outcomes that infringe upon human rights, including the right to privacy and non-discrimination.

(3) **Privacy Protective:** AI should be developed using a privacy by design approach. Developers, providers, or users of AI systems should take proactive measures to protect

---

[1] Hopes had been high that the Ontario legislation would include the mandatory reporting of the use of artificial intelligence if used by a public body to mirror section 65.2 of Québec's "Law 25" (Bill 64, 2021, c. 25 *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information).*

> 65.2. A public body that uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision. It must also inform the person concerned, at the latter's request,
>
> (1) of the personal information used to render the decision;
>
> (2) of the reasons and the principal factors and parameters that led to the decision; and
>
> (3) of the right of the person concerned to have the personal information used to render the decision corrected.
>
> The person concerned must be given the opportunity to submit observations to a member of the personnel of the public body who is in a position to review the decision.

the privacy and security of personal information and support the right of access to information from the very outset.

(4) **Human Rights:** Human rights protections must be built into the design of AI systems.

(5) **Transparent:** Institutions that develop, provide and use AI must ensure that the AI systems are visible, understandable, traceable and explainable to others.

(6) **Accountable:** Institutions should implement a robust internal governance structure with clearly defined roles, responsibilities and oversight procedures, including a human-in-the-loop at all times to ensure accountability.

TAB 8: Comments from the Office of the Information and Privacy Commissioner Regarding Responsible AI Governance in Alberta

The Information and Privacy Commissioner of Alberta has released a report on Responsible AI Governance for that province. This report recommends stand-alone AI specific legislation in Alberta. The privacy rights of children are acknowledged in that privacy-related harms cannot solely be addressed in privacy or AI -specific legislation. The report notes that the sections of the *Criminal Code* that deal with extortion and child luring are important as well as the need to specifically prohibit the distribution of deepfake pornography/child sexual abuse materials and altered images (page 19/23).

Tab 9: Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI

This paper was published in the (2024) 69:4 McGill Law Journal 395 by Professor S. Dunn of the Schulich School of Law, Dalhousie University. Professor Dunn defines non-consensual synthetic intimate images (NSII) as sexual images of a person (or child) that were created using technology such as AI or Photoshop without the subject's consent (p. 399). Professor Dunn also defines "deepfake videos" as: non-consensual, sexual video where an individual's face is superimposed on a previously existing pornographic video that results in a realistic footage that appears as though the individual is engaging in sex acts they did not perform (p. 400).

Professor Dunn noted that *The Privacy Act,* RSS 1978, c. P-24, section 7.1 was amended in 2018 to add the term "altered" to the definition of "intimate image" which would likely include forms of NSII that include deepfakes or nudifying apps and allow for a civil remedy in this province:

> **Definition**
>
> **7.1** In this Part, "intimate image" means a visual recording of a person, whether or not the person is identifiable or whether or not the image has been altered in any way, made by any means, including a photograph, film or video recording:
>
> (a) in which the person in the image is or is depicted as: (i) nude or exposing his or her genital organs or anal region or her breasts; or (ii) engaging in explicit sexual activity;
>
> (b) that was recorded in circumstances that gave rise to a reasonable expectation of privacy with respect to the image; and
>
> (c) if the image has been distributed, in which the person who is or is depicted in the image retained a reasonable expectation of privacy at the time it was distributed

Professor Dunn analyzed the two Criminal Code provisions that could involve artificial intelligence and the altered images of children. Section 163.1(1) defines child sexual abuse and exploitation material sufficiently to include both real and AI altered intimate images of children (p. 408). Subsection 163.1(2) allows for the "making" of child sexual abuse and exploitation material. To date, there are two cases in Canada where the accused has been successfully prosecuted under section 163.1 of the Criminal Code for making non-consensual sexual deepfakes of young persons: (1) *R v Larouche,* 2023 QCCQ 1853, and (2) *R v Legault,* 2024 BCPC 29. Even though section 163.1(2) includes the maximum punishment of 14 years, the offender in *Legault* received a (shocking) conditional sentence of two years less a day followed by three years' probation.[2] The 61 year old offender in *Larouche* was sentenced to 8 years' incarceration. That offender was convicted of possession, distributing and making child pornography by means of deepfake technology. Chief Justice Gagnon of the Cour du Québec provided specific guidance

[2] Justice Patterson of the British Columbia Provincial Court evidenced his displeasure with the joint submission throughout the ruling in *R v Legault.* He ultimately followed the guidance in *R v Anthony-Cook,* 2016 SCC 43, [2016] 2 SCR 204, and reluctantly accepted it.

on the aggravating features in this case with respect to his sentencing on the count for section 163.1(2):

> ***Making child pornography***
>
> 59 This case is unique in the country because the offence of making child pornography using deepfakes has not yet been dealt with by the courts. While deepfakes have recently been analyzed by certain scholars with respect to the connection between this technology and offences related to conjugal violence and the distribution of intimate images, or with respect to the national security risks of this technology (particularly election-meddling), this case appears to be the first involving child pornography offences.
>
> 60 Deepfake (*hypertrucage* in French) technology is an audiovisual technique that uses deep learning algorithms to create extremely realistic fakes. For example, this technology can superimpose one person's face onto another person's body in a video clip. A synthetic voice edited to sound exactly like the individual being impersonated can also be added to this visual fake.
>
> 61 The technology unit investigators were able to seize this type of deepfake file and update the offender's production of this content by chance. Investigating officers assigned to the Sûreté du Québec's technology unit have to be in contact with child pornography as part of their job. Over time, they become familiar with certain series of photographs or videos involving exploited children. Unfortunately, they know some of the victims quite well because their photographs or videos appear in the "collections" of many criminals they deal with.
>
> 62 When the police searched the offender's home, they noted that some files appeared different from a series of photographs they had seen in the past. They noticed some anomalies in the quality of the image. They decided to analyze this series further at the laboratory to verify their theory that these files had been modified or altered.
>
> 63 After analyzing it, the investigators discovered software to create deepfakes and a user manual among the computer equipment seized at the offender's home. The investigators decided to download the software to better understand its features. The everyday person clearly cannot use this software's features. Using it requires computer skills and a significant investment in time.
>
> 64 To create a successful deepfake, a user must have source material and destination material. This can be done using a bank of photographs or video clips. For example, it takes between 3,000 and 8,000 photographs of the same face to create a sufficient source file to export a face onto the body of another person. The software sequences a video excerpt image by image to obtain a bank sufficient to create a minimally realistic deepfake.
>
> 65 Once the database is sufficiently complete, the software tries to teach the artificial intelligence to take into account the different facial features on each photograph: angle of the face, position of the eyes, lips, ears, etc. to mimic the source face's movements. Teaching requires considerable technological means and a number of hours of work that is difficult to quantify other than to say it is particularly long. The longer it takes, the better the result because the artificial intelligence has learned that much more. Note that

> deepfakes can be created using the same medium (video to video) or different media (photograph to video and vice versa).
>
> 66 The offender created several deepfake photographs and videos. While it is clear that there was an evolution in the offender's ability to create deepfake images, some results are of an exceptional visual quality. It is impossible to separate the real from the fake. Had the investigators not been familiar with the known child pornography [TRANSLATION] "media library", it would have been impossible to know whether a photograph was a deepfake. The police have clearly entered a new era of cybercrime.

The mandatory minimum of one year is still alive for the offence of making child pornography and has not yet been challenged.[3] It is my opinion that the reasonable hypotheticals that posed such concern in *R v Senneville,* would not be arguable in a set of facts that involved the making and online distribution of child pornography by means of artificial intelligence. It is highly unlikely that an 18 year old could use artificial intelligence to "make" innocent non-consensual deepfake sexual images of a child in the same way as the possession hypothetical for an 18 year old in *R v Senneville.*

It is Professor Dunn's opinion that section 162.1 (Publication of an intimate image without consent) would not include an altered AI image of a child simply because the definition of "intimate image" in section 162.1(2) only applies to *authentic* images. Of course, when this section was added to the *Criminal Code* in 2014, artificial intelligence was in its infancy. The Nova Scotia Provincial Court adopted Professor Dunn's analysis and acquitted an accused of publishing several intimate images generated by artificial intelligence in *R v MSK,* 2026 NSPC 12 (March 9, 2026).

[3] The mandatory minimum of one year for the offence of possession [s.163.1(4)(a)]/accessing [s.163.1(4.1)(a)] child sexual abuse and exploitation material was struck by the Supreme Court of Canada in *R v Senneville,* 2025 SCC 33 on October 31, 2025. 5:4 decision.

Joint Statement on AI-Generated Imagery and the Protection of Privacy

23 February 2026

The co-signatories below are issuing this Joint Statement in response to serious concerns about artificial intelligence (AI) systems that generate realistic images and videos depicting identifiable individuals without their knowledge and consent.

While AI can bring meaningful benefits for individuals and society, recent developments - particularly AI image and video generation integrated into widely accessible social media platforms - have enabled the creation of non-consensual intimate imagery, defamatory depictions, and other harmful content featuring real individuals. We are especially concerned about potential harms to children and other vulnerable groups, such as cyber-bullying and/or exploitation.

Expectations for Organisations

The co-signatories remind all organisations developing and using AI content generation systems that such systems must be developed and used in accordance with applicable legal frameworks, including data protection and privacy rules.

We also highlight that the creation of non-consensual intimate imagery can constitute a criminal offence in many jurisdictions.

Whilst specific legal requirements vary by jurisdiction, fundamental principles should guide all organisations developing and using AI content generation systems, including:

- Implement robust safeguards to prevent the misuse of personal information and generation of non-consensual intimate imagery and other harmful materials, particularly where children are depicted.

- Ensure meaningful transparency about AI system capabilities, safeguards, acceptable uses and the consequences of misuse.

- Provide effective and accessible mechanisms for individuals to request the removal of harmful content involving personal information and respond rapidly to such requests.

- Address specific risks to children through implementing enhanced safeguards and providing clear, age-appropriate information to children, parents, guardians and educators.

Coordinated Response

The harms arising from non-consensual generation of intimate, defamatory, or otherwise harmful content depicting real individuals are significant and call for urgent regulatory attention.

To encourage the development of innovative and privacy-protective AI, the co-signatories of this statement are united in expressing their concern about the potential harms from the misuse of AI content generation systems. The co-signatories aim to share information on their approaches to addressing these concerns that can include enforcement, policy and education, as appropriate and to the extent that such sharing is consistent with applicable laws. This reflects our shared commitment and joint effort in addressing a global risk.

Conclusion

We call on organisations to engage proactively with regulators, implement robust safeguards from the outset, and ensure that technological advancement does not come at the expense of privacy, dignity, safety, and other fundamental rights - particularly for the most vulnerable of our global society.

Signatories

This Joint Statement has been coordinated by the Global Privacy Assembly's (GPA) International Enforcement Cooperation Working Group (IEWG) and is signed by the following co-signatories:

Albania

Information and Data Protection Office of the Republic of Albania
Besnik Dervishi, Information and Data Protection Commissioner

Andorra

Andorran Data Protection Agency
Agència Andorrana de Protecció de Dades
Jèssica Obiols, Head of the Andorran Data Protection Agency

Argentina

Agency of Access to Public Information – DPA Argentina
Agencia de Acceso a la Información Pública
Mg. Beatriz de Anchorena, Commissioner of the Agency to Access to Public Information

Autonomous City of Buenos Aires (Argentina)

Ombudsman's Office of the Autonomous City of Buenos Aires
Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires
María Rosa Muiños, Defensora del Pueblo / Ombudsman

State of Queensland (Australia)

Office of the Information Commissioner, Queensland
Joanne Kummrow, Information Commissioner
Alexander White, Privacy Commissioner

Basque (Spain)

Basque Data Protection Authority
Autoridad Vasca de Protección de Datos
Unai Aberasturi Gorriño, President

Belgium

Data Protection Authority
Autorité de la protection des données – Gegevensbeschermingsautoriteit
Koen Gorissen, Chairman of the Board
Alexandra Jaspar, Member of the Board
Peter Van den Eynde, Member of the Board

Bermuda

Office of the Privacy Commissioner of Bermuda
E. Angie Farquharson, Acting Privacy Commissioner

Brazil

National Data Protection Agency
Agência Nacional de Proteção de Dados

Waldemar Gonçalves Ortunho Junior, Director-President

Bulgaria

Commission for Personal Data Protection of the Republic of Bulgaria
Комисия за защита на личните данни

Borislav Bozhinov, Chairman

Burkina Faso

Commission for Information Technology and Freedoms
Commission de l'Informatique et des Libertés

Kouliga Désiré Yameogo, Director of Legal Affairs and Litigation

Canada

Office of the Privacy Commissioner of Canada

Philippe Dufresne, Commissioner

Province of Alberta (Canada)

Office of the Information and Privacy Commissioner of Alberta

Diane McLeod, Information and Privacy Commissioner

Province of British Columbia (Canada)

Office of the Information and Privacy Commissioner for British Columbia

Michael Harvey, Information and Privacy Commissioner for British Columbia

Province of Newfoundland and Labrador (Canada)

Office of the Information and Privacy Commissioner for Newfoundland and Labrador

Kerry Hatfield, Commissioner

Province of Quebec (Canada)

Commission on Access to Information of Quebec
Commission d'accès à l'information du Québec

Me Lise Girard, President and Member
Me Naomi Ayotte, Vice-President, Supervision Section and Administrative Judge
Me Steeven Plante, Member, Supervision Section and Administrative Judge

Republic of Cabo Verde

National Commission of Data Protection
Comissão Nacional de Proteção de Dados

Faustino Varela Monteiro, President

Catalonia (Spain)

Catalan Data Protection Authority
Autoritat Catalana de Protecció de Dades

Meritxell Borràs i Solé, Director

Colombia

Superintendence of Industry and Commerce of Colombia
Superintendencia de Industria y Comercio

Juan Carlos Upegui, Deputy Superintendent for the Protection of Personal Data

Croatia

Croatian Personal Data Protection Agency
Agencija za zaštitu osobnih podataka

Zdravko Vukić, Director

Cyprus

Commissioner for Personal Data Protection, Cyprus
Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Maria Christofides, Commissioner for Personal Data Protection

Ecuador

Superintendence of Personal Data Protection of Ecuador
Superintendencia de Protección de Datos Personales del Ecuador

Fabrizio Roberto Peralta Díaz, Superintendent of Data Protection

European Data Protection Board

European Data Protection Board

Anu Talus, Chair of the European Data Protection Board

European Data Protection Supervisor

European Data Protection Supervisor

Wojciech Wiewiórowski, European Data Protection Supervisor

France

National Commission for Information Technology and Civil Liberties
Commission Nationale de l'Informatique et des Libertés

Marie-Laure Denis, President

Germany

Federal Commissioner for Data Protection and Freedom of Information
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Andreas Hartl, Deputy Commissioner

Ghana

Data Protection Commission Ghana

Dr Arnold Kavaarpuo, Executive Director / Commissioner
Quintin Akrobotu, Director, Regulatory & Compliance
Abigail Tibuah Yeboah, Head of Administration

Gibraltar

Gibraltar Regulatory Authority

John Paul Rodriguez, Chief Executive Officer

Bailiwick of Guernsey

Office of the Data Protection Authority

Brent Homan, Data Protection Commissioner

Hong Kong, China

Office of the Privacy Commissioner for Personal Data

個人資料私隱專員公署

Ada Chung Lai-Ling, Privacy Commissioner for Personal Data

Iceland

The Icelandic Data Protection Authority

Persónuvernd

Helga Þórisdóttir, Data Protection Commissioner
Helga Sigríður Þórhallsdóttir, Head of International Affairs & Guidance

Ireland

Data Protection Commission

Coimisiún um Chosaint Sonaí

Dr. Des Hogan, Commissioner for Data Protection and Chairperson
Dale Sunderland, Commissioner for Data Protection
Niamh Sweeney, Commissioner for Data Protection

Isle of Man

Isle of Man Information Commissioner

Alexandra Delaney-Bhattacharya, Information Commissioner

Israel

Israeli Privacy Protection Authority

הרשות להגנת הפרטיות

Gilad Semama, Commissioner

Italy

Italian Data Protection Authority
Garante per la Protezione dei dati Personali

Pasquale Stanzione, President
Ginevra Cerrina Feroni, Vice-President
Agostino Ghiglia, Board Member

Bailiwick of Jersey

Jersey Office of the Information Commissioner
Paul Vane, Information Commissioner

Kenya

Office of the Data Protection Commissioner
Oscar Otieno, Deputy Data Commissioner

Kosovo

Information and Privacy Agency
Krenare Sogojeva Dërmaku, Commissioner for Information and Privacy

Malta

Office of the Information and Data Protection Commissioner of Malta
Ian Deguara, Information and Data Protection Commissioner

Mauritius

Mauritius Data Protection Office
Drudeisha Madhub, Data Protection Commissioner

State of Mexico and Municipalities (Mexico)

Institute for Transparency, Access to Public Information and Personal Data Protection of the State of Mexico and Municipalities
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios

Dr. José Martínez Vilchis, President Commissioner
Rosario Mejía Ayala, Commissioner
Sharon Cristina Morales Martínez, Commissioner
Luis Gustavo Parra Noriega, Commissioner
Guadalupe Ramírez Peña, Commissioner

State of Nuevo León (Mexico)

Institute for Transparency, Access to Public Information and Personal Data Protection of Nuevo León
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Nuevo León

Brenda Lizeth González Lara, President Commissioner
Félix Fernando Ramírez Bustillos, Commissioner
María Teresa Treviño Fernández, Commissioner

Mexico

Personal Data Protection Unit of the Anti-Corruption and Good Government Secretariat
Unidad de Protección de Datos Personales de la Secretaría Anticorrupción y del Buen Gobierno

Monaco

Personal Data Protection Authority
Autorité de Protection des Données Personnelles

Agnès Lepaulmier, Secretary General

Netherlands

Dutch Data Protection Authority
Autoriteit Persoonsgegevens

Monique Verdier, Deputy Chair

New Zealand

Office of the Privacy Commissioner, New Zealand

Michael Webster, Privacy Commissioner

Nigeria

Nigeria Data Protection Commission

Dr. Vincent Olatunji, National Commissioner / Chief Executive Officer

Norway

Norwegian Data Protection Authority
Datatilsynet

Tobias Judin, Head of International

Panama

The National Authority for Transparency and Access to Information
Autoridad Nacional de Transparencia y Acceso a la Información

Licda. Sheyla Castillo de Arias, Director

Peru

National Authority for the Protection of Personal Data
Autoridad Nacional de Protección de Datos Personales

Eduardo Luna Cervantes, Director

Philippines

National Privacy Commission, Philippines

Atty. Johann Carlos S. Barcena, CESO III, Privacy Commissioner
Atty. Jose Amelito S. Belarmino, MSc, Deputy Privacy Commissioner
Atty. Juan Paolo F. Fajardo, Deputy Privacy Commissioner

Poland

Personal Data Protection Office
Urząd Ochrony Danych Osobowych

Mirosław Wróblewski, President of the Office

Portugal

Portuguese Data Protection Supervisory Authority
Comissão Nacional de Proteção de Dados

Prof. Dra. Paula Meira Lourenço, President

Singapore

Personal Data Protection Commission of the Republic of Singapore

Denise Wong, Deputy Commissioner

Slovenia

Information Commissioner of the Republic of Slovenia
Informacijski pooblaščenec

dr. Jelena Virant Burnik, Information Commissioner

Republic of Korea

Personal Information Protection Commission
개인정보 보호위원회

Kyung Hee Song, Chairperson

Switzerland

Federal Data Protection and Information Commissioner
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Adrian Lobsiger, Federal Data Protection and Information Commissioner

Emirate of Abu Dhabi (United Arab Emirates)

ADGM Office of Data Protection

Sami Mohammed, Commissioner of Data Protection

Emirate of Dubai (United Arab Emirates)

Dubai International Financial Centre Authority

Lori Baker, Vice President – Data Protection & Regulatory Compliance

United Kingdom

UK Information Commissioner's Office

William Malcolm, Executive Director Regulatory Risk & Innovation

Uruguay

Regulatory and Control Unit for Personal Data
Unidad Reguladora y de Control de Datos Personales

Executive Council

MOLLY ROSE FOUNDATION

Australia's social media ban – is it working?

Research briefing – April 2026

In March 2026, Molly Rose Foundation conducted the first large-scale polling of Australians aged 12–15 on the country's social media ban. Our findings show:

- There are significant questions about the effectiveness of Australia's social media ban. Three fifths (61%) of 12–15 year-olds who previously held accounts on restricted platforms continue to have access to one or more active accounts;
- More than half of 12–15 year-olds who previously used TikTok, YouTube and Instagram remain able to use accounts on these platforms;
- 70% of children still using restricted sites say that it was 'easy' to circumvent the ban. In most cases, social media platforms have failed to detect or seek to remove under 16s accounts;
- Over half (51%) of children who used restricted platforms prior to the ban coming into force say it has made no difference to their online safety. One-in-seven (14%) now feel less safe;
- In the early months of the ban, children report mixed impacts on their wellbeing, with some indications it has reduced their overall time spent online.

Methodology

Molly Rose Foundation has conducted the first large-scale polling of young Australians aged 12–15 on the country's social media ban. Our aim is to inform discussions on whether to follow suit in the UK and Europe.

YouthInsight, Australia's largest online youth panel, surveyed 1,050 Australians aged 12–15. Fieldwork was undertaken between March 12th and 31st and conducted online.

Results

1. A clear majority of Australian 12–15 year-olds are still using social media platforms covered by the ban

Four months after Australia's social media ban took effect, over three-fifths of 12–15 year-olds (61%) who previously had accounts on platforms covered by the ban still have access to at least one active account. This equates to over half (54%) of all children aged 12–15.

More than half of children who previously had TikTok, YouTube and Instagram accounts still remain able to use accounts on these platforms. While a significant proportion of accounts have been deactivated, 53% of previous TikTok users, 53% of YouTube users and 52% of Instagram users are still able to access an account on these platforms.

A small proportion of children have opened accounts on new restricted platforms since the ban came into force. Given the broad questions about the effectiveness of the ban, this churn is unsurprising and suggests that the ban has failed to prevent new account openings.[1]

These findings broadly align with a survey of parents conducted by Australia's eSafety Commissioner, published in March 2026. This survey also found that a majority of under 16s retained access to social media accounts.[2]

Table 1: Proportion of Australian 12–15 year-olds with accounts on restricted platforms before and after the ban came into force.

	Proportion of children with accounts before the ban	Proportion of children with active accounts in March 2026	Proportion of previous user base with active accounts
YouTube	66%	35%	**53%**
TikTok	55%	29%	**53%**
Instagram	49%	25%	**52%**
Snapchat	49%	23%	**47%**
Facebook	43%	23%	**53%**
X	18%	7%	**41%**
Reddit	13%	6%	**49%**
Twitch	12%	6%	**47%**
Threads	10%	4%	**45%**
Kick	3%	1%	**36%**

1 Our figures reflect this churn.
2 eSafety Commissioner (2026) Social Media Minimum Age: Compliance update

2. Most of those still using social media sites covered by the ban had no need to circumvent restrictions

Most children who were still using restricted platforms had not needed to find workarounds – this is because platforms had failed to identify and remove their accounts in the first place.

Among children who remained able to use accounts on restricted platforms, a significant majority (70%) said it had been 'easy' to circumvent the ban. Just under half (46%) had found it 'very easy'.

More than three-fifths of children who continued to use YouTube (64%), Snapchat (61%), Instagram (60%) and TikTok (60%) said that that 'no action' had been taken by the platform to remove or deactivate an account they had before restrictions were introduced.

Around a quarter of children still using each restricted platform had been successfully able to get around an age check on a pre-existing account. This includes 25% of TikTok users, 24% of those still using Snapchat, and 23% of those using YouTube.

Smaller proportions had used proactive measures to circumvent restrictions. For each platform, between 3% and 13% had asked a friend or family member to set up a new account for them.

For each platform, around one in twenty children were using a VPN to access an account.

Table 2: How children aged 12–15 had retained access to accounts on social media sites covered by the restrictions

	Children with active accounts on YouTube	Children with active accounts on TikTok	Children with active accounts on Instagram	Children with active accounts on Snapchat
No action taken to remove or deactivate a pre-existing account	**64%**	**60%**	**60%**	**61%**
Got around age checks to keep using a pre-existing account	23%	25%	22%	24%
Used a workaround to set up a new account as an over-16	10%	14%	14%	11%
Had a friend of family member set up a new account as an over-16	10%	8%	7%	7%
Use a VPN to access an account	4%	5%	4%	4%
Something else	4%	1%	1%	2%

Note: As children may have multiple active accounts on a single platform, they were able to select all applicable options. Totals may exceed 100%.

3. Most children do not feel that the ban has improved how safe they feel online

Among 12–15 year-olds who had accounts on restricted platforms prior to the ban coming into force, there is a mixed picture about whether the ban has made them feel any safer.

While three-in-ten of these children (31%) do feel safer, **half (51%) said that the ban had not changed how safe they felt online. One in seven (14%) of these children said they now felt less safe online than before the social media restrictions came into force.**

Among children who had wholly lost access to their accounts on restricted platforms, perceptions of how their safety had changed remained similarly mixed.

Two-fifths (42%) did feel safer, but an identical proportion felt that the restrictions had made no difference to their safety online.

One-in-eight children (12%) felt less safe after having their social media accounts removed. This may reflect a range of factors, including their displacement to smaller or more poorly moderated platforms, their experiences on sites not covered by the ban, or a perception that online platforms have pivoted from safety towards prioritising access restrictions.

4. Children are using gaming, messaging and other social media platforms more, but some are spending less time online

Our data suggests that the social media ban has led to some early changes in children's online behaviour.

Substantial proportions of 12–15 year-olds who used restricted platforms prior to the ban coming into force report that they are using messaging apps (39%) and gaming platforms (43%) more since restrictions were introduced.

Around one in five of these children (21%) have started to more frequently use social media platforms which have not faced restrictions. A smaller proportion of children (16%) have opened accounts on platforms they hadn't previously used.

There are early indications that the social media ban is having some early positive impact on time spent online. Half (50%) of children who used restricted platforms prior to the ban coming into force said they now spent less time online, although 37% felt the time they spent on social media had not changed.

Experience from other countries suggests that these metrics will need to be monitored closely over time. In 2011, South Korea responded to concerns about gaming addiction by introducing a ban on online gaming for children between midnight and 6am. Although the ban initially resulted in a reduction in time spent online, these improvements steadily eroded and within 4 years internet use had increased.[3] South Korea's government subsequently discontinued the policy, with evaluations finding 'practically insignificant effects' on time spent online, academic performance and adolescent sleep time.[4] Studies showed that sleep time increased by an average of only 1.5 minutes per child, with internet addiction declining by only 0.7 percentage points.[5]

3 Lee, C (2017) Ex post valuation of illegalising juvenile online gaming after midnight: a case of shutdown policy in South Korea. Telematics and Informatics, 34(8)
4 Choi, J et al (2018) Effect of the online game shutdown policy on Internet use, Internet addiction, and sleeping hours in Korean adolescents. Journal of Adolescent Health 62(5)
5 Lee, C (2017), see above.

5. The ban is not having a clear positive or negative impact on children's wellbeing

As it stands, children believe that new restrictions are having neither a clear positive or negative impact on their wellbeing.

When asked about the overall impact of the ban on their lives, around two-fifths (42%) of 12–15 year-olds who used restricted platforms prior to the ban coming into force felt it had 'not had any impact'. Around a third felt it had a somewhat or very negative impact (32%). One in five young of these children (22%) felt the ban had a somewhat or very positive impact.

Those who had lost access to all their accounts on restricted platforms also reported a mixed range of experiences. One-third (34%) said the loss had resulted in a negative impact on their life, while similar proportions claimed there was a positive impact (33%), or no impact at all (30%).

When asked about the impact of the ban on their mental health and wellbeing specifically, there was a similarly mixed picture. Of those who used restricted platforms prior to the ban coming into force, 45% felt it had had no impact on their mental health and wellbeing, a fifth reported a negative impact (19%), but around one third (33%) reported a positive impact.

Among those who had wholly lost access to accounts on restricted platforms, around 45% of children reported positive impacts on certain areas of their life, including on their mental health and wellbeing and academic performance. These children also reported a net negative impact on their understanding of news and current events.

Looking forward, negative outcomes on children will need to be studied especially closely, particularly for vulnerable groups - including neurodivergent children, children with mental health difficulties and LGBTQ children.

Table 3: Perspectives on the impact of restrictions by children who used social media before the ban, and among children who have lost access to all their accounts.

	12–15 year-olds who used restricted platforms prior to the ban coming into force			12–15 year-olds who had lost access to all accounts on restricted platforms after the ban		
	Negative impact	No impact	Positive impact	Negative impact	No impact	Positive impact
My mental health and wellbeing	19%	45%	33%	19%	33%	46%
My performance at school or in training	12%	50%	34%	8%	42%	47%
How connected I feel to friends and family	26%	39%	32%	31%	24%	43%
My understanding of what's going on in the world	29%	42%	26%	34%	35%	29%
My sleep	12%	48%	38%	10%	37%	51%

Note: 'Positive' and 'negative' columns include those who reported either a 'somewhat' or 'very' positive or negative impact. The table does not include those who chose 'not sure' or 'prefer not to say'.

Analysis and implications

Last month, Australia's e-safety Commissioner told the UK Parliament that Australia's social media ban had been 'very successful in its early days.'[6] This research, the first large-scale survey of Australian 12–15 year-olds, suggests a very different picture.

Proponents of a ban in the UK have argued that a ban is necessary to deliver immediate and swift improvements to children's safety. Early data from Australia suggests that it will deliver neither:

- a majority of children who previously used social media platforms covered by the ban remain able to do so;
- two-thirds of children who used restricted platforms prior to the ban coming into force report it has had no impact on their safety (or has actively made it worse), and;
- despite this being a signature policy of the Australian Government, malign compliance from the tech firms means that social media platforms have largely failed to detect and remove accounts in the first place.

This data suggests that, at least in the medium term, an Australia-style ban is unlikely to deliver the improvements in safety that parents and children deserve and demand. At worst, the Australian ban risks giving parents a false sense of safety, with children still freely able to use social media platforms, but with tech firms let off the hook in terms of their safety-by-design and safeguarding responsibilities.

Given the substantial questions raised by this research, it would be deeply imprudent for the UK or other countries to follow suit with social media bans at this point. The question marks about the efficacy and implementation of Australia's ban are significant and unresolved.

Instead, we recommend that the Prime Minister makes **a commitment to a new Online Safety Act in the Kings Speech, building on the Government's ongoing consultation to end addictive and harmful design features.** This must make provisions for a systemic Duty of Care, reset regulatory incentives in favour of harm reduction, and significantly strengthen the regulatory regime so that it is better targeted to the size and cash-rich position of the largest companies in the world.

There is palpably no basis to rush into a social media ban at this early stage. The UK and other countries should instead continue to closely follow the lessons from Australia – including the outcomes from long-term, systematic evaluations and academic reviews.

This will enable the efficacy of regulatory measures to be determined, and where early data suggests that a ban may produce positive effects if it is capable of being scaled effectively, for the harm-benefit ratio to be properly assessed against other interventions, including compared to strengthened regulation.

Regulation remains the most powerful tool available to tackle the underlying business models and commercial incentives that are the root causes of preventable harm. Got right, it can protect children on social media, gaming services and on AI.

With the right political will, fixing and strengthening the Online Safety Act can deliver the quickest, most effective and decisive route to protect children from preventable harm.

6 Evidence to the Commons Science, Innovation and Technology Select Committee, 11th March 2026

For further briefing and a conversation about how Molly Rose Foundation can support your work please contact Rowan Ferguson at **r.ferguson@mollyrosefoundation.org**

Registered Charity No: 1179482 https://mollyrosefoundation.org

Final Report to the AI Strategy Task Force
Submitted by: Taylor Owen[1]

As part of the Federal Government's AI Strategy Task Force I was asked to provide input on the theme of Safe AI & Public Trust. Given the broad nature of this topic, I have chosen to focus this report on what I believe are core imperatives of democratic governance: ensuring that AI systems and other digital technologies used by Canadians are safe, contribute to the health of our democratic society, and are governed in ways that sustain public confidence. In what follows, I recommend a series of policies to achieve these goals organized into three priority areas (Citizen Safety, Information Ecosystem Integrity, and Democratic Legitimacy), most of which could be implemented through two existing federal governance frameworks:

- An amended version of the *Online Harms Act* that includes AI platforms within its scope;
- An amended version of the *Consumer Privacy Protection Act*.

By leveraging these frameworks, the Canadian government could ground its approach to AI governance in best international practices, move swiftly to ensure that Canadians are protected from immediate harms that AI systems pose,[2] and facilitate safe AI innovation and adoption.[3] Given low levels of trust in AI amongst Canadians,[4] legitimate concerns about its safety, and genuine uncertainty over how it will affect our economy and society, effective governance is imperative to solidifying Canadians' collective confidence in a future of Canada that is increasingly reliant on and intertwined with AI development, research, and implementation. Without this confidence, a sovereign AI innovation and adoption agenda is fraught with risk that undermines the government's investments in AI and the public's trust that it will do so responsibly.

The research centre I founded at McGill University seeks to better understand these complex systems, and to help citizens and their democratic governments maximize the benefits and minimize the harms posed by digital technologies, including AI. Through academic and policy research, years of public consultation, and close relationships with expert partners, we have built a deep empirical understanding of the impacts of the digital ecosystem on Canadians, and the policy mechanisms that advance a uniquely Canadian mix of public priorities for digital governance. This memo's perspectives grow out of that work, while also drawing from other

---

[1] Beaverbrook Chair in Media, Ethics and Communication in the Max Bell School of Public Policy, and Founding Director of the Centre for Media, Technology and Democracy, McGill University. This memo was written in collaboration with Helen A. Hayes, Associate Director, Policy, Centre for Media, Technology and Democracy.
[2] These harms, outlined below, include individual harms like race and gender-based stereotyping and collective harms, including the amplification of mis- and dis-information.
[3] Canada's G7 presidency in 2025 presents a unique opportunity to translate international commitments—such as the G7 Leaders' Statement on AI for Prosperity—into concrete domestic policies that meet the highest standards for safety and democratic values.
[4] According to KPMG's Trust, attitudes and use of artificial intelligence: A global study 2025, Canada ranks among the lowest globally in perceived trustworthiness of AI systems, with only 46% of respondents expressing trust. Similarly, Telus' Human-centric AI, perspectives on trust and the future of AI report finds that 70% of Canadians believe AI poses serious risks that society is not adequately prepared to address, and, notably, that only 1% of Canadians trust AI to operate independently.

expert scholars and civil society organizations; investigations into AI systems by international regulators; and statements and policy commitments made by governments around the world.

In summary, my opinion is that:

1. AI systems are increasingly embedded in Canadians' daily lives, shaping what we see,[5] the work we do,[6] the decisions we make,[7] and the services we access.[8] These systems mediate how citizens access information,[9] engage with public institutions,[10] and make decisions that shape their social and economic lives. This adoption is moving at a historically unprecedented rate.
2. For some, AI tools, particularly generative, conversational, and agentic systems, can enhance creativity,[11] facilitate learning,[12] and provide accessible forms of interaction or self-expression.[13]
3. For many others, AI systems pose significant risks and harms. Empirical studies have documented instances where AI chatbots, for example, fail to respond appropriately to users experiencing mental health crises,[14] reinforce cognitive distortions through mirroring language,[15] and cultivate a false sense of emotional reciprocity.[16] Beyond individual wellbeing, AI systems have also been shown to amplify mis- and dis-information,[17] enable non-consensual image generation[18] and impersonation,[19] perpetuate race- and gender-based stereotyping and inequalities,[20] and manipulate users through data-driven optimization for engagement.[21]
4. Public concern about AI in Canada is widespread and deeply held: only 32% of Canadians believe that the benefits of AI outweigh the risks,[22] 89% worry about their privacy,[23] 78% fear that AI will spread false information during elections,[24] and 70% are concerned about their children accessing AI chatbots.[25] In the 2025 election, polling we conducted at the

[5] Guess et al. 2023; Cinelli et al. 2021
[6] KPMG 2025.
[7] Levy et al. 2021; Lang 2021; Sumer 2024
[8] Pham et al. 2024; Ashraf et al. 2024; Sollapur et al. 2024
[9] Brown et al. 2024; Edelson et al. 2025
[10] Frangoudes et al. 2021; Senadheera et al. 2024
[11] Agboola and Yassin 2025; Chandrasekara et al. 2024
[12] Chiu and Rospigliosi 2025; Aluko et al. 2025
[13] Chemnad and Othman 2024; Penuela et al. 2024
[14] De Freitas et al. 2023; Dergaa et al. 2024
[15] Alabad et al. 2024 ; Yankouskaya et al. 2025
[16] Zhang et al. 2025; Laestadius et al. 2022; Li and Zhang 2024
[17] Canadian Digital Media Research Network 2025; Wack et al. 2025
[18] Hawkins et al. 2025; Umbach et al. 2024
[19] Tariq et al. 2022; Jasserand 2024
[20] Scheuerman et al. 2020; Omiye, J. A. et al. 2023
[21] Du and Sen 2023; Roberts and David 2025
[22] KPMG 2025.
[23] Office of the Privacy Commissioner of Canada, 2025.
[24] Leger 2025.
[25] Leger 2025.

Centre found that one in four Canadians encountered fake news sites, and that 80% of Canadians were concerned about AI-generated, misleading content.[26]

5. These harms originate from the structural dynamics of AI systems, which are shaped by corporate and economic incentives that govern their design, deployment, and diffusion. These conditions are largely insulated from democratic oversight.
6. Without this oversight, Canadians' trust in AI systems will remain low. 88% of Canadians support stronger governance of AI systems,[27] 85% want government oversight to ensure ethical and safe use,[28] and 80% believe that there should be penalties for AI-generated dis-information.[29]
7. If technical solutions do not make AI more trustworthy or the public does not perceive AI to be trustworthy despite those technical solutions, then trust must instead be built in the democratic infrastructure that governs AI. So, Canada's democratic institutions need to be capable of holding AI companies to account if and when they are irresponsible.
8. Canada is not alone in this: governments around the world[30] are beginning to enact legislation that addresses the structures, design, and incentives of AI and other digital technologies. They recognise that digital sovereignty[31] demands not just infrastructure, but also governance. Canada can learn from these and other best practices.
9. International precedent has demonstrated that effective AI governance does not necessarily require generalized AI legislation (such as the previous government's *Artificial Intelligence and Data Act*), but can at least initially be achieved through a range of existing and targeted policy mechanisms.
10. In Canada, there are two existing governance frameworks that could be quickly implemented by Canada's federal government to address the root causes of AI harm and promote safer systems: 1) an amended and re-introduced version of the *Online Harms Act* that includes AI platforms within its scope; and, 2) an amended and re-introduced version of the *Consumer Privacy Protection Act.*
11. While these governance frameworks will require policy iteration and innovation over time and may at some point fall short and demand stand-alone AI regulation, it is imperative that the Canadian government build a foundation of AI policy capacity. Doing so will ensure the baseline democratic accountability that Canadians rightly demand, and provide the time for a next phase of public consultation and policy iteration and design.

---

[26] The Canadian Digital Media Research Network 2025.
[27] Telus 2025.
[28] Leger 2025.
[29] The Canadian Digital Media Research Network 2025.
[30] Across Europe, the democratic global south, and at the US state-level.
[31] Canada's digital ecosystem and infrastructures are largely determined by foreign platforms, rules, and shareholder value. This leaves Canadian institutions and citizens vulnerable to the incentives of powerful, unpredictable, and uncontrollable foreign forces, and threatens Canada's digital sovereignty.

Summary of Policy Recommendations and Implementation Tactics

	Citizen Safety	Info Ecosystem Integrity	Democratic Legitimacy
Amended and Re-introduced *Online Harms Act*	Digital Safety Commission (1.1)[32] Systemic Risk Governance (1.2)[33] Age-Appropriate Design (1.3)[34]	Monitoring and Data Sharing (2.2)[35]	Recourse Mechanisms (3.2)[36]
Amended and Re-introduced *Consumer Privacy Protection Act*		AI Identification and Provenance Disclosure (2.1)[37]	Data Portability, Interoperability, and Right to Deletion (3.1)[38] User Empowerment Support (3.2)[39]
Other Measures		Reliable Information Production (2.3)[40]	Mandated Consultation Mechanisms (3.3)[41]

[32] The Digital Safety Commission would have authority to: 1.1.1) regulate data access; 1.1.2) conduct algorithmic audits; and, 1.13) enforce compliance by issuing orders, penalties, and corrective action plans.
[33] This would include three duties to: 1.2.1) act responsibly; 1.2.2) protect children; and, 1.2.3) make certain content inaccessible. It should also minimize users' exposure to other forms of harmful content, including fraud and scam content.
[34] This requires heightened safety and design standards, overseen by the Digital Safety Commission, including: 1.3.1) child-impact assessments; 1.3.2) default high-privacy settings; and 1.3.3) crisis-response protocols for conversational systems.
[35] At a minimum, this includes: 2.2.1) mandated data inventories of AI system inputs and outputs; 2.2.2) secure researcher access frameworks for data on social media and consumer chatbot use and algorithmic design, facilitated by an independent monitoring or observatory body; and, 2.2.3) confidentiality-safe data enclaves for public-interest research.
[36] This would involve 3.2.1) establishing a statutory AI and Digital Safety Ombudsperson within the Digital Safety Commission.
[37] This should include: 2.2.1) visible labelling; 2.2.2) provenance metadata and digital watermarking; and, 2.2.3) source transparency requirements.
[38] This should include: 3.1.1) interoperable data standards; 3.1.2) user-initiated data mobility rights; 3.1.3) public disclosure of interoperability specifications, and, 3.1.4) mandated right to deletion for users.
[39] This include: 3.2.2) mandatory human review of consequential automated decisions; and, 3.2.3) public reporting obligations.
[40] The government could: 2.3.1) consider adapting existing journalistic support mechanism to, and develop new programs for, a broader range of journalistic content creators and reliable content generations forms; 2.3.2) support new sovereign, decentralized infrastructure for public interest media; and, 2.3.3) actively engage in domestic and international efforts to transition the journalism sector to a new AI-driven mediated information ecosystem.
[41] This could include: 3.3.1) standing citizens' assemblies or deliberative panels; 3.3.2) structured partnerships between civil society organizations and academic researchers; and 3.3.3) mandated and regularly held advisory councils.

Democratic Priority 1: Citizen Safety

One of the most fundamental obligations of a democratic government is to ensure the safety and security of its citizens.[42] As new AI technologies enter the Canadian market,[43] this responsibility extends to ensuring that they do not expose individuals or communities to preventable harms. On this measure, Canada has fallen short. While the decision to delay comprehensive AI legislation may reflect a desire for measured policy development, the absence of enforceable safety obligations has left Canadians under protected in a rapidly evolving digital marketplace.[44] The core challenge is not merely technological, but structural: AI systems are being designed, deployed, and monetized by private actors who bear little legal responsibility for the risks their systems create. Addressing this requires moving beyond voluntary ethics frameworks and industry self-regulation toward binding legal mechanisms that assign clear accountability and remedies. In order to protect Canadians from AI harms, the government should consider:

1.1 Independent Regulatory Authority. The asymmetry between global technology firms and national governments (both in technical capacity and access to information) makes independent regulatory authority not a procedural detail but a democratic necessity. Canada should create a single, empowered institution responsible for coordinating national digital governance (i.e., social media and consumer-facing AI) through new online harms legislation. This Digital Safety Commission[45] would have authority to: 1.1.1) mandate data access;[46] 1.1.2) conduct algorithmic audits;[47] and 1.1.3) enforce compliance by issuing orders, penalties, and corrective action plans.[48]

1.2 Systemic Risk Governance. The Digital Safety Commission, as proposed in Part 1 of the *Online Harms Act*, should adopt a systems-level duty of care for AI systems (once scoped in), which 1.2.1) obliges providers to assess and mitigate systemic risks before and after deployment (*duty to act responsibly)*;[49] 1.2.2) requires heightened protections for minors (*duty to protect*

[42] Anderljung et al. 2023; Coeckelbergh 2024
[43] Benchetrit 2025; Steven 2025
[44] Competition Bureau 2025; Du and Sen 2023
[45] In addition to the establishment of a Digital Safety Commission, it is also important for the Government of Canada to have a central digital governance coordinating capacity in order to overcome the soloing of digital polices between departments. In addition, it is critical that the Digital Safety Commission, the Office of the Privacy Commissioner of Canada and the Competition Bureau be empowered to share data and collaborate.
[46] This can be accomplished by applying sections 73-77 of Bill C-63, which provides mechanisms for a Commission to grant access to inventories and electronic data of the operators of social media services.
[47] The EU's Digital Services Act Article 37 requires very large online platforms to contract an independent auditor to assess compliance. In Canada, this function could be filled by a designated Commission, rather than left to independent auditors, such as the proposed Digital Safety Commission in Bill C-63.
[48] These powers are assigned to the Digital Safety Commission in Bill C-63.
[49] This can be accomplished by adapting Bill C-63, Section 54: operators "must implement measures that are adequate to mitigate the risk that users of the regulated service will be exposed to harmful content on the service." The EU's AI Act Article 51 further provides definitions and obligations for operators of general-purpose AI models that entail systemic risk.

children);[50] and, 1.2.3) mandates categorical removal of certain categories of content and updating of models,[51] including child sexual abuse material and non-consensual intimate images (*duty to make certain content inaccessible).*[52] Beyond this, systemic risk governance should also minimize users' exposure to other forms of harmful content, including fraud and scam content.[53]

1.3 Age-Appropriate Design. Democratic societies have distinct obligations to protect children and youth in digital environments.[54] Beyond content-based governance mechanisms, this requires heightened safety and design standards, overseen by the Digital Safety Commission, including: 1.3.1) child-impact assessments;[55] 1.3.2) default high-privacy settings;[56] and, 1.3.3) crisis-response protocols for conversational systems.[57]

Democratic Priority 2: Information Ecosystem Integrity

Democratic societies demand access to reliable information. AI is reshaping our information ecosystem in two ways: it is used to determine our personalised feeds of content,[58] and is increasingly creating content itself.[59] In the near future, the majority of what we see online may

[50] This can be accomplished by adapting Bill C-63, Section 65: "an operator must integrate into a regulated service that it operates any design features respecting the protection of children, such as age-appropriate design, that are provided by regulations." The EU's AI Act also obligates operators to identify and address unique vulnerabilities of minors on digital platforms. California Senate Bill 243 additionally requires special protections for minors using chatbot platforms. The UK's Online Safety Act includes specific provisions for child safety, such as requiring platforms to use effective age assurance to prevent children from accessing harmful content.

[51] Examples of this include: the EU's Digital Services Act requirement for platforms to remove or disable access to illegal content and easily enable users to flag such content; the UK's Online Safety Act requirement that platforms remove illegal content, including fraud, incitement of violence, and content that promotes suicide. Luccioni et al., 2022.

[52] This can be accomplished by adapting Bill C-63, Sections 67-71, which obligates operators of regulated service to remove content that "sexually victimizes a child or revictimizes a survivor or intimate content communicated without consent" within 24 hours of identification.

[53] This can be accomplished by adapting Bill C-63, Section 54: operators "must implement measures that are adequate to mitigate the risk that users of the regulated service will be exposed to harmful content on the service" and by adding online scams and fraud as a category of harm.

[54] The UN Committee on the Rights of the Child's General Comment No. 25 clarifies that Canada's obligation to protect children's rights applies in the digital world, which explicitly encompasses AI technologies; This further contributes to the global consensus that children's rights must be protected in the age of AI, as reflected in the UN High-Level Advisory Body on AI's 'Governing AI for Humanity', UN General Assembly resolution 78/187 on the Rights of the child in the digital environment, and UNICEF's Policy guidance on AI for children.

[55] These assessments should be designed around the "best interests of the child". See UNCRC General comment No. 25, paras. 23 and 38, the Canadian Department of Justice, Child Rights Impact Assessment tool and e-learning course, and UNICEF, Assessing child rights impacts in relation to the digital environment.

[56] This aligns with the Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight "Putting best interests of young people at the forefront of privacy and access to personal information"; the Roundtable of G7 Data Protection and Privacy Authorities Statement on AI and Children; and the Sweep Report 2024: Deceptive Design Patterns.

[57] Examples of this includes California Senate Bill 243, which obligates conversational AI platforms to maintain "a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to the user" and issue crisis service provider referral notifications when needed.

[58] Brown et al. 2024; Edelson et al. 2025

[59] Wei and Tyson 2024; DiResta and Goldstein 2024

be both selected and created by AI.[60] This raises acute challenges for democratic societies, particularly regarding electoral integrity. AI systems can now produce and circulate synthetic political content,[61] impersonations,[62] and deepfakes at unprecedented speed. Ensuring the transparency of these systems and the reliability of content they prioritize and generate must be a priority for democratic societies. In order to ensure information ecosystem integrity, the government should consider:

2.1. AI Identification and Provenance Disclosure. Citizens should have the right to know when they are interacting with or consuming content produced by an AI system. This requires a multi-layered identification regime that mandates clear disclosure in both human and machine-readable formats. At a minimum, a re-introduced and amended *Consumer Privacy Protection Act* should include: 2.1.1) visible labelling;[63] 2.1.2) provenance metadata and digital watermarking;[64] and, 2.1.3) source transparency requirements, including training data.[65]

2.2 Monitoring and Data Sharing with Researchers and Civil Society. Addressing the power asymmetry between private platforms and the public, and ensuring that researchers, journalists, and civil society organizations can study the effects of AI systems, requires statutory mechanisms given to the Digital Safety Commission for data access, transparency, and independent oversight. At a minimum, this includes: 2.2.1) mandated data inventories of AI system inputs and outputs;[66] 2.2.2) secure researcher access frameworks for data on social media and consumer chatbot use and algorithmic design, facilitated by an independent monitoring or observatory body;[67] and 2.2.3) confidentiality-safe data enclaves for public-interest research.[68]

---

[60] Kreps and Kriner 2023; Birrer 2024

[61] Examples in Canada include the Kirkland Lake Bot Incident and the emergence of AI-generated ads masquerading as legitimate news sources during the 2025 Federal Election.

[62] Leong et al. 2024; Lyngaas 2025

[63] California's Senate Bill 243 requires that conversational AI systems issue periodic, in-context notifications to remind users that they are interacting with an automated agent, with heightened requirements for mental health and companion chatbots; South Korea's Artificial Intelligence (AI) Basic Act requires labelling or generative AI content.

[64] The EU's AI Act (article 50) establishes mandatory disclosure when users interact with an AI system and requires providers of generative AI to implement technical measures such as watermarking or metadata tagging that signal synthetic content.

[65] This can be achieved through the Consumer Privacy Protection Act or through the transparency provision of the Online Harms Act should AI systems be brought into scope. Other examples of legislation with AI transparency provisions include Australia's Data Availability and Transparency Act, the EU's AI Act, and Japan's Act on Improving and Fairness of Digital Platforms.

[66] The EU's AI Act (article 10) mandates developers of high-risk systems must maintain detailed records and evaluations of training and testing datasets.

[67] This can be achieved through Sections 73-74 of Bill C-63, which outlines access to electronic data by accredited researchers.

[68] This can be achieved by amending Part 1, Sections 73-74 of Bill C-63 or introducing a stand-alone Act to allow persons engaged in public interest research to request access to inventories of electronic data that are included in digital safety plans. Other examples of legislation with similar provisions include that EU AI Act's Article 57, which establishes "AI regulatory sandboxes" for controlled testing of AI and the EU's Digital Services Act Article 40 which obligates very large online platforms to provide vetted researchers with access to platform data for systemic-risk research under secure conditions.

2.3 Support for Reliable Information Production. As AI-generated content saturates digital spaces,[69] supply-side measures are essential to preserve and promote the production of reliable, evidence-based information in an increasingly AI mediated and created information ecosystem. Policies in this domain are less developed, however, the government could: 2.3.1) consider adapting existing journalistic support mechanism to, and develop new programs for, a broader range of journalistic content creators and reliable content generations forms;[70] 2.3.2) support new sovereign, decentralized infrastructure for public interest media; and, 2.3.3) actively engage in domestic and international efforts to transition the journalism sector to a new AI-driven mediated information ecosystem.[71]

Democratic Priority 3: Democratic Legitimacy

In a democratic society, citizens must have meaningful agency in determining the development and governance of the AI infrastructure that shapes their lives. Rebuilding democratic legitimacy in the age of AI therefore requires more than public consultation; it demands institutional pathways that are built for meaningful participation, agency and autonomy, and accountability. This includes mechanisms through which citizens can contest automated decisions,[72] assert control over their data,[73] and contribute to the governance of AI itself.[74] In order to ensure the democratic legitimacy of AI systems, the government should consider:

3.1 Data Portability, Interoperability, and Right to Deletion. Empowering citizens also means restoring their control over their personal data. In our current information economy, data mobility is not simply a matter of convenience, but is a structural determinant of citizens' autonomy.[75] Together, portability and interoperability provide the technical and legal architecture through which citizens can reclaim agency over their data[76] and reduce the concentration of informational power.[77] To do so, amendments to the *Consumer Privacy*

[69] Birrer 2024; Chen et al. 2025
[70] Such as the Local Journalism Initiative, the Online News Act and the Media Fund.
[71] Examples include: International Fund for Public Interest Media, Media Forward Fund, Public Media Bridge Fund.
[72] The EU's General Data Protection Regulation Article 22 grants individuals the right "not to be subject to a decision based solely on automated processing", and allows them to request human review and contest decisions. The EU's AI Act Article 86 further allows individuals affected by AI systems to lodge complaints with national authorities and receive information about how decisions were made.
[73] This can be accomplished by applying sections 62, 63, and 72 of Bill C-27, which requires organizations to disclose the use of individual data in automated decision systems, provide explanations of decisions with "significant impact" on individuals, and "disclose the personal information that it has collected from the individual to an organization designated by the individual" upon request.
[74] Examples of this include regular citizen assemblies on AI policy and the creation of public transparency registers to allow civil society to monitor incidents and risks.
[75] The EU's Digital Markets Act Article 6(64) explains that a "lack of interoperability allows gatekeepers that provide number-independent interpersonal communications services to benefit from strong network effects, which contributes to the weakening of contestability."
[76] Walker and Milne 2024; Crabtree and Mortier 2016
[77] Mantelero 2012; Rahman 2018; Zuboff 2015

Protection Act should include: 3.1.1) interoperable data standards;[78] 3.1.2) user-initiated data mobility rights including social graph data;[79] 3.1.3) public disclosure of interoperability specifications,[80] and, 1.1.4) a mandated right to deletion for users.[81]

3.2 Recourse Mechanisms and User Empowerment Support. Citizens must have clear and accessible avenues for redress when AI systems cause or exacerbate individual and collective harms. Establishing recourse mechanisms ensures procedural fairness by enabling users to challenge automated decisions, demand explanation, and seek remedies. The amended and re-introduced *Online Harms Act* should include: 3.2.1) a statutory AI and Digital Safety Ombudsperson[82] within the Digital Safety Commission, who is empowered to receive complaints, investigate harms, and provide users with informational resources, including literacy materials. The amended Consumer Privacy Protection Act should include: 3.2.2) mandatory human review of consequential automated decisions;[83] and, 3.2.3) public reporting obligations.[84]

3.3 Mandated Consultation Mechanisms. This will institutionalize democratic input into the design and oversight of AI policy. This could include: 3.3.1) standing citizens' assemblies or deliberative panels, composed of demographically representative participants;[85] 3.3.2) structured partnerships between civil society organizations and academic researchers to promote co-governance and value-chain governance;[86] and 3.3.3) mandated and regularly held advisory councils, such as with youth and Indigenous stakeholders.[87]

---

[78] The EU Digital Markets Act Article 6 mandates that gatekeeper operating systems provide "effective interoperability for third party services," and in all cases, "the gatekeeper and the requesting provider should ensure that interoperability does not undermine a high level of security and data protection in line with their obligations."
[79] This can be accomplished by applying and expanding section 72 of the CPPA in Bill C-27, which grants individuals the right to request an organization to disclose their data to another organization.
[80] An example of this includes the EU's Digital Markets Act Article 7, which requires companies to allow "reasonable requests for interoperability" by providing technical interfaces and relevant information required to interoperate.
[81] The "right to erasure" originates in the EU's General Data Protection Regulation Article 17. This grants data subjects the right to request the prompt deletion of personal data held about them by a business organization.
[82] This can be accomplished by applying and expanding the rights and duties afforded to the Digital Safety Ombudsperson proposed in Bill C-63, Sections 10-12.
[83] An example of this includes the EU's AI Act Article 14, which requires that high-risk AI systems be designed and developed in such a way that "they can be effectively overseen by natural persons,"
[84] This can be accomplished by applying and expanding section 62 of Bill C-27, which requires organizations to publicly disclose their data collection policies and account how automated decision systems are used for significant impact decisions, and section 62 of the Online Harms Act in Bill C-63, which requires operators to publish a digital safety plan online.
[85] Examples of these assemblies include Taiwan's standing Alignment Assemblies, The Centre for Media, Technology and Democracy's Youth Assembly on Digital Rights and Safety, and Germany's Artificial Intelligence and Citizens Councils.
[86] The United States has relied primarily on soft law and voluntary frameworks for AI governance, including NIST's AI Risk Management Framework (2023) and the White House's Blueprint for an AI Bill of Rights (2022), both which promote co-governance through extensive multi-stakeholder consultation.
[87] Examples of these councils include the IPC's Youth Advisory Council, The Digital Youth Advisory Committee, the OECD's Youthwise, and the Global Indigenous Data Alliance.

Global Privacy Enforcement Network

GPEN Sweep Report: Children's Privacy

March 2026

Authored by the Central Sweep Coordinators:

Office of the Privacy Commissioner of Canada

Information Commissioner's Office, the United Kingdom

Office of the Data Protection Authority of the Bailiwick of Guernsey

Table of contents

Background

The 2025 Global Privacy Enforcement Network (GPEN) Sweep ("the Sweep") took place during the week of November 3-7, 2025.

The Sweep examined how websites and mobile applications ("apps") used by children collect children's personal information, are transparent about their privacy practices, use age assurance mechanisms, and employ privacy protective controls to limit data collection. Some of the reviewed apps and websites are specifically designed for children, while others are used by the general population but are particularly popular among children and young people.

Today's digital space is a significant part of children's lives, offering opportunities for self-expression, learning, socialising, and connecting with their community. Online services that do not consider the best interests of children can leave young people vulnerable to risks such as online tracking, profiling, targeting, and exposure to inappropriate or harmful content.

The 2025 Sweep marked the 10-year anniversary of a similar children's privacy Sweep conducted by GPEN in 2015. This enabled a comparison of how online services protected children and used their data back then, and how they do so a decade later.

The Sweep was coordinated by the Office of the Privacy Commissioner of Canada, the United Kingdom Information Commissioner's Office, and the Office of the Data Protection Authority of the Bailiwick of Guernsey ("Central Sweep Coordinators").

Twenty-seven privacy enforcement authorities from around the world (see Appendix 1) participated in the 2025 Sweep, examining 876 websites and apps.[1]

This report is authored by the Central Sweep Coordinators. It sets out the findings and analysis of those that participated in the Sweep. It is not intended to represent the views of the wider GPEN membership or any specific authority.

The GPEN Sweep is not in itself an investigation, nor is it intended to conclusively identify compliance issues or legal contraventions. The concerns identified via this exercise may help inform targeted guidance, future engagement with organizations, and potential enforcement actions.

Methodology

The goal of the Sweep was for participants, or "Sweepers," to replicate the user experience by engaging with websites and apps used by children and gather insight

[1] Participating privacy enforcement authorities reviewed 464 websites and 400 apps (12 platforms were not categorized by the Sweepers). Note that Sweepers may have independently examined different versions of websites and/or apps. Therefore, the total number of distinct platforms swept may be lower.

into the current state of their data collection and online privacy practices. This enabled us to compare findings with those of the 2015 Sweep, where relevant. While these observations and comparisons are informative, the Sweep is not a scientific study.

The Central Sweep Coordinators developed a set of instructions and associated questions to guide Sweepers' engagement with each website and app, based on the approach used in 2015. This helped ensure that Sweepers assessed websites and apps according to similar standards.

The questions focused on five indicators, which largely mirrored those from the 2015 Sweep. However, it is important to note that the questions Sweepers answered in 2025 were more comprehensive than the questions used a decade ago, which limited our ability to draw certain comparisons with previous findings. The indicators, which will be further explained in the relevant sections below, were:

1. Age assurance;
2. Collection of children's data;
3. Protective controls;
4. Account deletion; and
5. Other overall concerns.

Sweepers were asked to document their interactions with the content and features of the websites and apps – including privacy settings, privacy policies, and account creation and deletion processes – using the provided Sweep form.[2] Throughout the report, some figures exclude blank responses to specific questions in the Sweep Form, which accounts for the slight discrepancy with the total number of websites and apps examined.

Within the topic of children's privacy, each participating authority selected the focus of their Sweep – for instance, they selected websites and/or apps to sweep within specific sectors that aligned with their strategic priorities. The following chart (Figure 1) is a sectoral breakdown of the websites and apps examined in the Sweep:[3]

[2] Because the Sweep was based on the observations and interactions of Sweepers with websites and apps within a relatively short period of time (around 30 minutes), Sweepers may not have experienced and documented the full extent of content, features, and data collection of each website or app.

[3] Examples of websites and apps belonging to the "Other" sector include but are not limited to AI products, communications and instant messaging, arts and culture, entertainment, leisure, online dating, and sports news.

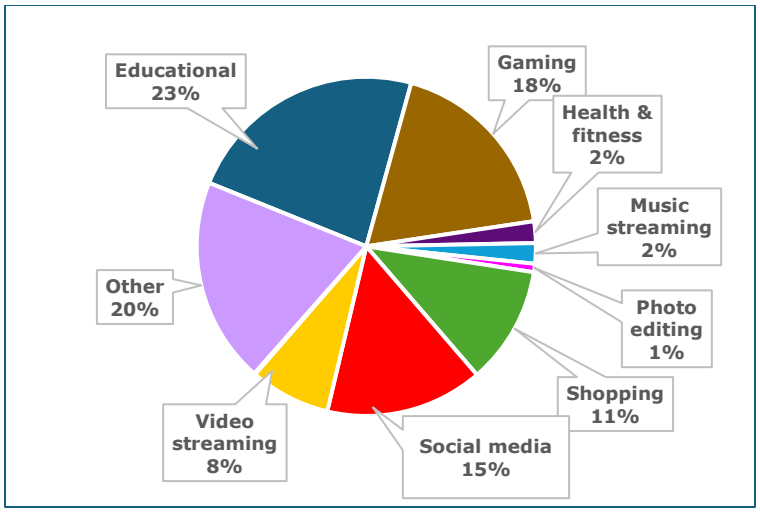


Figure 1. Sectoral breakdown of websites and mobile applications

Age assurance (Indicator 1)

Approaches to age assurance

Age assurance involves mechanisms for assessing a child's age so their access to or interactions with an online service can be tailored or restricted accordingly. There are different approaches to age assurance. Amongst others, mechanisms include:

- self-declaration (a user states their age but is not required to provide evidence);
- age verification (a user is asked to verify their age, e.g. by providing a form of ID); and
- age estimation (a user's age is estimated, often by algorithmic means, e.g. facial age estimation).

Age assurance mechanisms observed in the Sweep

Sweepers reported that the terms of service for 62% of all websites and apps reviewed (517 out of 832)[4] explicitly limited access to users over a certain age, most often 13 years of age. Of these websites and apps, 32% (164 out of 517) did not use any age assurance mechanisms at all. For the remaining 68% of websites and apps (353 out of 517) with age restrictions:

- the majority used self-declaration (88%, or 311 out of 353);
- a smaller number used age verification (11%, or 38 out of 353); and

[4] These figures exclude blank responses.

- fewer still used age estimation (5%, or 19 out of 353).[5]

Not all Sweepers reported the type of age estimation used but, where they did, this was always facial age estimation, which requires provision of a photo or video selfie.

Circumvention of age assurance

Findings from the Sweep demonstrated that self-declaration, a trust-based approach to age assurance, can easily be circumvented.[6] Sweepers reported that they were able to circumvent age assurance measures used in 72% (460 out of 641)[7] of cases; most often where self-declaration was used.

In some cases, websites and apps that used self-declaration implemented additional mechanisms to prevent access by underage users, such as simple math questions, prompts for parental consent, and preventing changes to the initial self-declared age. However, Sweepers reported that such measures were also easily bypassed, for instance by re-installing an app or clearing cookies.

Inappropriate content and high-risk processing

Given ease of circumvention, relying solely on self-declaration is unlikely to prevent children from being exposed to inappropriate content or high-risk data processing and design features where these are present in websites and apps used by children. (See pages 13 to 16 for the types of content and data processing and design features Sweepers looked for.)

Of the 34% of websites and apps (288 out of 826)[8] that Sweepers identified as having inappropriate content for children, 24% (68 out of 288) did not have age assurance mechanisms in place. However, where age assurance was implemented, 90% (161 out of 179) used self-declaration. Similarly, of the 38% of websites and apps (317 out of 824)[9] that Sweepers identified as having high-risk data processing and design features for children, 24% (76 out of 317) did not have age assurance mechanisms in place. However, where age assurance was implemented, 89% (169 out of 190) used self-declaration.

This means that children would be able to access (amongst other things) sexual images and violent content, and freely engage with other users on some websites and apps. See page 13 for further findings on inappropriate content and high-risk

[5] These figures show the percentage of websites and apps with age restrictions that deployed each type of age assurance mechanism. Some websites and apps deployed more than one type of age assurance mechanism.
[6] Circumvention in this context refers to either easily deceiving the age assurance system or entirely bypassing it.
[7] These figures exclude blank responses.
[8] These figures exclude blank responses.
[9] These figures exclude blank responses.

data processing and design features identified in some websites and apps by Sweepers.

What has changed over the last decade?

Participants in the GPEN 2015 Sweep reported that only 15% of swept websites and apps used a form of age assurance. A decade later, Sweepers reported that 45% of all websites and apps (397 out of 876) deployed a form of age assurance, which represents an increase of 30%.

Summary observations

Age assurance can be a valuable part of an overall approach to protecting children and their privacy rights online. While the Sweep findings indicate an increase in the use of age assurance mechanisms over the last decade, the sole use of self-declaration (or lack of age assurance altogether) is concerning for websites and apps identified as having inappropriate content or high-risk data processing and design features for children. Where platforms are designed for or popular with children, the participating authorities encourage online services deploying age assurance to ensure that the mechanisms they use are appropriate to the risks posed to children by their platforms and that they collect the minimum amount of personal information required.

Collection of personal information and protective controls (Indicators 2 and 3)

Privacy policies

Privacy policies play an important role in enabling users to make informed and meaningful privacy decisions. A well-crafted privacy policy builds trust by setting clear expectations about how individuals' personal information will be collected, used and disclosed by an organization.

As expected, Sweepers found that most websites and apps (96%, or 825 out of 862)[10] included privacy policies. However, they identified opportunities for improvement. For example, some of the policies contained minimal information, while others were long and difficult to understand.

Sweepers also observed that 85% of the websites and apps (705 out of 825) indicated in their privacy policies that they may share personal information with third parties. This represents a substantial increase compared to 51% found in the 2015 Sweep. This may suggest that reliance on third parties may have increased, likely due to evolving revenue models, business practices and ecosystems.

[10] These figures exclude blank responses.

Collection of personal information

Sweepers found that certain categories of personal information were collected more often than others. To access the full functionality of the platforms, 50% of the websites and apps examined (437 out of 876) required the collection of usernames, 59% (519 out of 876) required an email address, and 46% (399 out of 876) required geolocation.

Other categories of personal information were collected less frequently. For example, personal interests (253 out of 876) and characteristics (257 out of 876) were collected by fewer than 30% of the websites and apps swept.

Overall, Sweepers noted an increase in the collection of certain types of personal information compared to what was observed in 2015. For example:

	2015	**2025**
Name	29% mandatory/12% optional	41% mandatory/23% optional
Phone number	12% mandatory/10% optional	18% mandatory/28% optional
Address	11% mandatory/8% optional	12% mandatory/18% optional
Photos or videos	9% mandatory/14% optional	5% mandatory/40% optional

Table 1: Comparison of personal information collection by all websites and apps swept, between 2015 and 2025

Moreover, Sweepers observed that 41% (341 out of 825) of privacy policies explicitly stated that the websites or apps did not knowingly collect children's personal information. Twenty five percent (86 out of 341) of these websites and apps were specifically targeted at children. However, Sweepers observed that some types of personal information were still collected on a mandatory basis such as the name (30%, 26 out of 86), email address (56%, 48 out of 86), username (56%, 48 out of 86) and photos or videos (5%, or 4 out of 86). Furthermore, while 54% of the websites and apps (184 out of 341)[11] making this statement in their privacy policy were not specifically targeted at children, Sweepers noted that they were still popular with, and commonly used by, children. This raises concerns about the resulting collection of children's personal information, with Sweepers reporting that many of these websites and apps mandated the collection of personal information, as shown in the chart below.

[11] Fifteen percent of Sweepers (51 out of 341) answered that they were unsure whether the website or app was targeted at children, or popular with children. Six percent of Sweepers (20 out of 341) left the response blank.

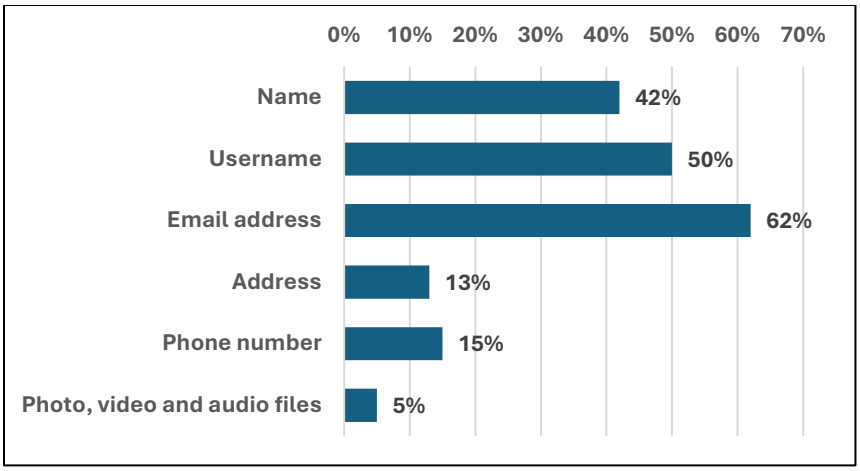


Figure 2. Mandatory collection of personal information on websites and apps, stating that they do not knowingly collect children's personal information

Protective controls

Protective controls are mechanisms implemented by organizations operating websites and apps to limit the collection of personal information to what is necessary and reduce the risk of harm to users. For example, this can be in the form of prompts for parental involvement, warnings when leaving the site, pre-made avatars/usernames, or moderated chats/message boards to prevent inadvertent sharing of personal information.

Similar to 2015, Sweepers saw good practices in the use of protective controls in 2025. For example:

- The possibility for parents to approve new people's invitations (or alternatively activate a "friend mode" where the child is free to accept new people's invitations);
- Warnings not to use real names or upload images on the website or app, such as pop-ups advising to not include personal information when choosing a username, or generation of random usernames during the sign-up process;
- The location sharing and contact access being disabled by default;
- The possibility to decline the use of location or choose to only share general location;
- The display of 'Privacy protective tips' advising users not to share personal information when interacting with a chatbot;
- Filtering posts and chats from users aged 12 and younger to prevent personal information from being posted; and
- Specifically for educational websites for children, restricting child account creation to teachers, and parental approval of content.

However, Sweepers also noted several concerning practices across many of the websites and apps. For example:

- Only 56% of the websites and apps examined (442 out of 794)[12] had the personal information collected set to private by default;
- On 47% of the websites and apps examined (393 out of the 828)[13], Sweepers were redirected to another website or app where they could be asked to disclose personal information. We note that this figure was higher in 2015 (58%);
- Seventy-one percent of the swept websites and apps (589 out of the 827)[14] did not have communications about protective controls and privacy practices tailored to children (e.g., simple language, child-friendly animations);
- Of the 38% of the websites and apps (317 out of 824)[15] for which Sweepers identified high-risk data processing and design features for children (e.g., behavioural profiling, geolocation by default, or nudging to share personal information with others), only 25% (80 out of 317) had parental dashboards and 35% (112 out of 317) had privacy communications prompting for parental involvement;
- Similarly, of the 35% of swept websites and apps (288 out of 826)[16] that featured content that could be deemed inappropriate for children (e.g., depiction of violence, hateful content, sexuality), only 35% (100 out of 288) had privacy communications prompting for parental involvement and 27% (79 out of 288) had parental dashboards; and
- As part of an overall assessment of each website and app swept, Sweepers were asked for their opinion, based on their experience using the service, on whether they would feel comfortable with a child using a website or app. The Sweepers noted that they would not be comfortable with children using 41% (343 out of 833)[17] of the websites and apps. Only 19% (64 out of 343) of these platforms were reported to have protective controls that effectively limit the collection of personal information.

Summary observations

While Sweepers identified some good examples of privacy communications and controls, they also observed concerning practices which could lead to a lack of understanding and excessive collection of children's personal information.

The participating authorities encourage organizations to ensure that their privacy policies accurately reflect and clearly explain their data handling practices, taking into consideration the potential diversity and age of their user bases. Privacy policies should be comprehensive in content and easy to understand. Platforms should also find creative and accessible ways to explain their privacy practices. Organizations can

[12] These figures exclude blank responses.
[13] These figures exclude blank responses.
[14] These figures exclude blank responses.
[15] These figures exclude blank responses.
[16] These figures exclude blank responses.
[17] These figures exclude blank responses.

empower young users and their parents by tailoring privacy communications to the intended users and making privacy controls easy to find and to use.

Organizations should carefully consider whether their collection of personal information from children is necessary and proportionate for the delivery of their services, and ensure that the privacy of young users is protected by design and by default.

Where appropriate, platforms should also encourage and facilitate parental involvement to ensure that parents can guide or support their children in making meaningful decisions about their privacy.

Account deletion (Indicator 4)

Why account deletion matters for children

Being able to delete an account easily helps children control their personal information and leave services they no longer want to use. If deletion is difficult to find or complete, children may remain on a service longer than intended, increasing exposure to unwanted content. In addition, their personal information may be retained for a prolonged period, which increases the risks of unwanted data processing in the future.

Sweepers were asked to assess whether account deletion was easy to find and easy to complete, using their judgment based on the number of steps required and the clarity of information provided.

What Sweepers observed

Consistent with the results from the 2024 GPEN Report on Deceptive Design Patterns[18], Sweepers reported that 64% of websites and apps (481 out of 755)[19] had an accessible process for account deletion (easy to find and understand), while 36% (274 out of 755) did not. In services where deletion was assessed as inaccessible (not easy to find and understand), Sweepers commonly reported that deletion options were hidden within multiple menus, users were redirected to long help pages or external support processes, or deletion required contacting customer support rather than being completed directly by the user. Sweepers described such processes as "laborious" and "practically impossible for children" in some cases.

[18] See GPEN Sweep Report 2024: Deceptive Design Patterns, July 9, 2024
[19] These figures exclude blank responses.

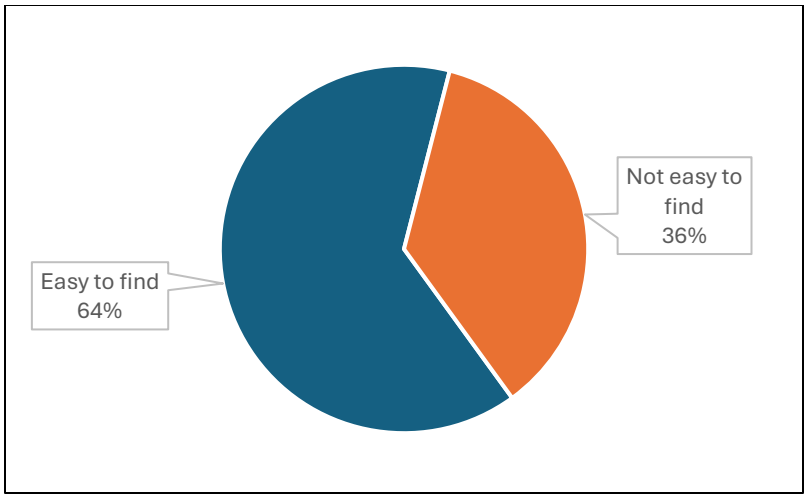


Figure 3. Ease of access to account deletion options

What has changed over the last decade?

Participants in GPEN's 2015 Sweep reported that only 29% of swept websites and apps provided an accessible means for account deletion. Ten years later, 35% more websites and apps now offer accessible deletion, increasing from 29% to 64%.

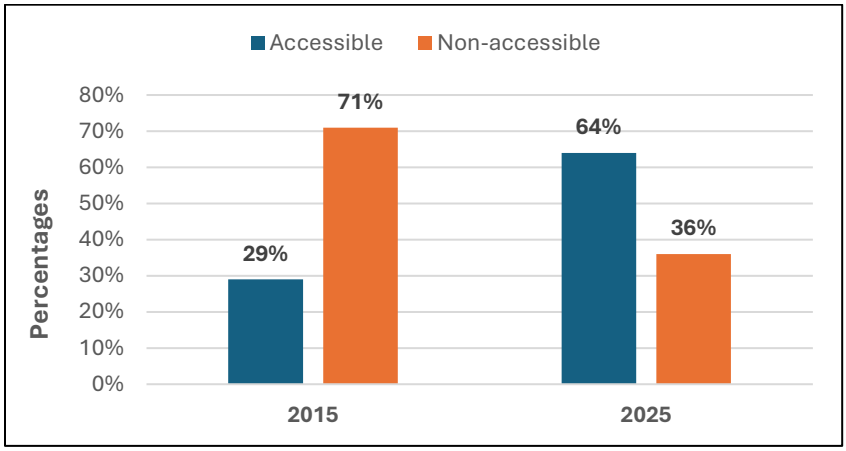


Figure 4. Ten-year progress regarding accessible account deletion options

Summary observations

The ease with which accounts can be deleted is an important measure of how well an individual can maintain control over their personal information. The Sweep findings show significant progress over the last decade in making account deletion options easier to find. However, over one-third of swept websites and apps still do not provide an accessible way to delete accounts. Making account deletion simple and user-

controlled remains an important part of child safety, particularly as children's relationships with online services change over time.

Inappropriate content and high-risk data processing and design features (Indicator 5)

Sweepers assessed whether websites and apps featured content that might be inappropriate for children[20], and data processing and design features that could represent a high risk to them.[21]

Exposure to harmful content

Sweepers identified concerning content across a significant proportion of websites and apps (see chart below).[22] Bullying, abusive, or hateful content was found in 15% of services (127 out of 876), while sexual content appeared in 11% of services (94 out of 876). Content related to self-harm was present in 7% of services (65 out of 876), and content related to eating disorders in a similar proportion (7%, or 64 out of 876).

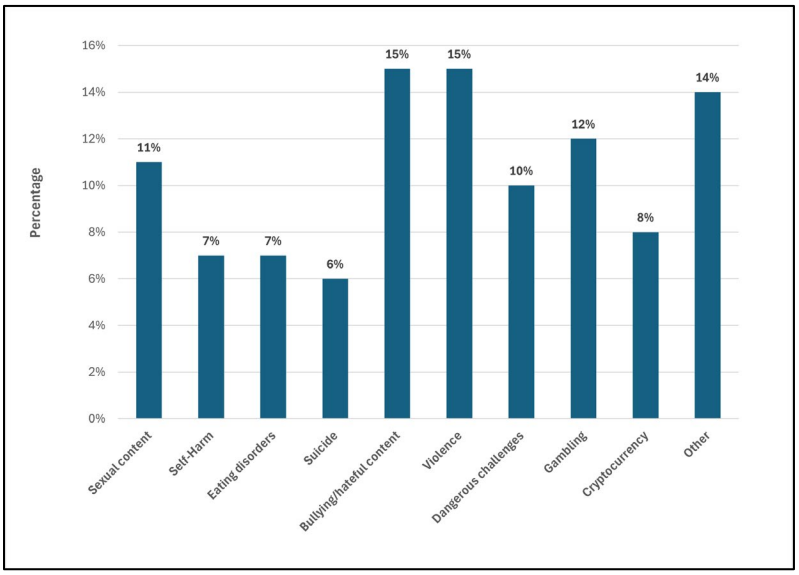


Figure 5. Proportion of websites and apps with inappropriate content, by type

[20] Sweepers were asked to record if they encountered the following types of content: sexual content; self-harm; eating disorders; suicide; bullying; abusive or hateful content; depiction or encouragement of violence; encouragement of dangerous challenges; gambling; cryptocurrencies.

[21] Sweepers were asked to record if they encountered the following data processing and design features: complex language for children; public by default privacy settings; nudging/nagging to share personal information with others; discouraging use of privacy protective options; processing of biometric data; use of behavioural profiling; geolocation on by default; ability to freely engage with other users.

[22] The chart shows the percentage of websites and apps containing inappropriate content. Some websites and apps contained more than one type of inappropriate content.

These findings demonstrate that children using some popular websites and apps risk exposure to harmful content. Sweepers noted that such content appeared in user-generated sections, chat functions, and algorithmic feeds.

When harmful content meets risky features

The combination of inappropriate content with high-risk design features may further amplify risk. For instance, when using the websites and apps and reviewing their privacy communications, Sweepers reported that behavioural profiling (i.e., tracking and analysis of user behaviour to predict interests and serve content) was present alongside self-harm content in 60% of cases (39 out of 65), and eating disorder content in 58% of cases (37 out of 64). This combination is particularly troubling, as it suggests that some platforms may not have implemented suitable measures to prevent profiling of children and delivery of content that is detrimental to their health and well-being.

Risks in child-targeted services

Sweepers noted that, in some cases, even services that are targeted at children incorporated high-risk data processing and design features. For example, Sweepers reported that 6% (18 out of 284) of such platforms employed behavioural profiling. Of these, 39% (7 out of 18) also hosted bullying or abusive content, while 28% (5 out of 18) featured depictions of violence.

Sweepers expressed concern about these findings. For instance, one Sweeper observed that a service "clearly designed for young children" included "extensive tracking of in-app behaviour with no parental visibility or control," while another noted "user-generated content with violent themes appearing in feeds alongside educational material."

Overall suitability for child use

As mentioned above, Sweepers were asked whether they would feel comfortable with a child using a website or app, taking into account both its privacy practices and any inappropriate content and high-risk data processing and design features. While it was a subjective assessment, Sweepers reported that they were not comfortable with children using 41% (343 out of 833)[23] of swept websites and apps.

[23] These figures exclude blank responses.

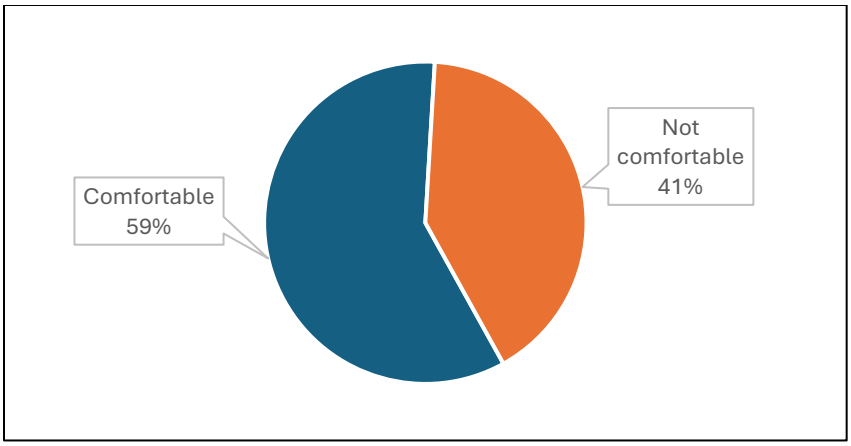


Figure 6. Overall suitability for child use

Sweepers identified a range of factors contributing to discomfort with child use. These included exposure to violent or sexual content, with Sweepers noting in some cases that services contained "content rated for ages 18 and up, with extreme violence, sex, and other themes." Sweepers also identified unrestricted interaction with other users, particularly through chat functions and community features where children could freely engage with strangers.

Design features encouraging prolonged or repeated engagement were noted, alongside monetisation practices that may place pressure on children, including advertising banners that "may direct the child to inappropriate places." Sweepers further identified profiling, tracking, and other high-risk data processing, with some reporting that tracking technologies appeared to collect information "without measures to halt collection" for child users. In many cases, more than one of these factors was present (see chart below).[24]

[24] The chart shows the percentage of websites and apps with unsuitable design features. Some websites and apps did not contain unsuitable design features.

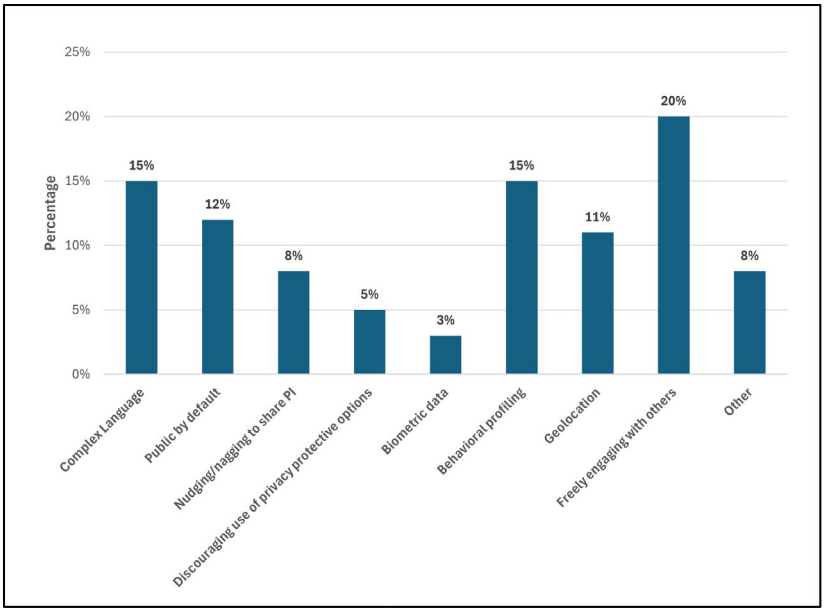


Figure 7. Proportion of websites and apps with unsuitable design features, by type

Websites versus apps

The Sweep findings show slight differences between platform types. Sweepers were generally more comfortable with children using websites rather than apps: 59% of websites (275 out of 464) were considered suitable, compared to 53% of apps (212 out of 400).

This gap suggests that mobile applications may present particular challenges for child safety, potentially due to differences in functionality, data collection practices, or interaction features.

Free services and child safety

Analysis of the data also reveals differences based on how services generate revenue. Paid services were assessed as suitable for child use in 61% of cases (117 out of 193), compared to 53% for free services (345 out of 648).

This pattern may reflect differences in business models and the incentives they create. Services that generate revenue through subscriptions may be less reliant on data-driven monetisation or engagement-maximising features that can raise concerns for children. Free services, by contrast, may be more likely to employ such practices.

Summary observations

The Sweep findings reveal that a significant proportion of services expose children to harmful content, and subject them to high-risk data processing and design features. Sweepers often reported the presence of both harmful content and high-risk design

features within the same service, potentially amplifying risks to children. Where websites and apps are used by children, the participating authorities encourage online services to design these platforms in a way that is appropriate for their use, including ensuring that the content children encounter and the features made available are age appropriate.

Conclusion

The purpose behind the GPEN Sweep is to encourage organizations to comply with privacy and data protection legislation, while promoting co-operation between privacy enforcement authorities across the globe. Though the Sweep is not in itself an investigation, nor is it intended to conclusively identify compliance issues or legal contraventions, the concerns identified via this initiative may help support targeted advice, engagement with organizations and/or enforcement actions in the future.

The outcome of this year's Sweep shows mixed results. Across many websites and apps, Sweepers observed good practices to protect children and their personal information. However, Sweepers also noted practices that raise concerns about children's privacy, and that suggest some risks may have increased over the last ten years.

For instance, compared to 2015, more online services designed for or used by children now require users to provide their personal information to access the full functionality of the platform or share their personal information with third parties. Additionally, while the use of age assurance mechanisms to restrict children's access or interaction with online services has increased, Sweepers found that such measures were often easily circumvented. This is concerning in instances where websites and apps had inappropriate content and/or high-risk data processing and design features for children.

All individuals should have their personal information protected, particularly children who navigate the digital space and use online services. By adopting child-friendly practices, such as limiting the collection of personal information, designing the services to be privacy-protective by design and by default, and using age assurance mechanisms appropriate to the level of risk on their platforms, organizations can contribute to children's well-being online.

Appendix A

The following privacy enforcement authorities provided their results:

1. Office of the Australian Information Commissioner
2. Office of the Privacy Commissioner for Bermuda
3. Agência Nacional de Proteção de Dados, Brazil
4. Office of the Information and Privacy Commissioner of Alberta, Canada
5. Office of the Information and Privacy Commissioner for British Columbia, Canada
6. Office of the Privacy Commissioner of Canada
7. Information and Privacy Commissioner of Ontario, Canada
8. Commission d'accès à l'information du Québec, Canada
9. Office of the Privacy Commissioner for Personal Data, Hong Kong, China
10. Personal Data Protection Bureau, Macao, China
11. Estonian Data Protection Inspectorate
12. Commission Nationale de l'Informatique et des Libertés, France
13. Gibraltar Regulatory Authority
14. Office of the Data Protection Authority of the Bailiwick of Guernsey
15. Isle of Man Information Commissioner
16. The Privacy Protection Authority, Israel
17. Garante per la Protezione dei dati personali, Italy
18. Personal Information Protection Commission, Japan
19. Jersey Office of the Information Commissioner
20. Office of the Information and Data Protection Commissioner, Malta
21. Autoriteit Persoonsgegevens, Netherlands
22. Office of the Privacy Commissioner of New Zealand
23. Datatilsynet, Norway
24. National Privacy Commission, Philippines
25. Information Commissioner of the Republic of Slovenia
26. Information Commissioner's Office, the United Kingdom
27. California Privacy Protection Agency, the United States of America

Français

CHAPTER 24

An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures

Assented to November 25, 2024

CONTENTS

Preamble

The Government of Ontario:

Recognizes the importance of cyber security in establishing trust in digital services delivered by the public sector.

Believes that cyber security in the public sector should be strengthened.

Believes that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario while protecting privacy.

Recognizes that digital information and technology related to children warrants special protection.

Recognizes the importance of protecting the privacy of the people of Ontario and the value of enhancing Ontario's privacy safeguards through increased transparency and independent oversight.

Therefore, His Majesty, by and with the advice and consent of the Legislative Assembly of the Province of Ontario, enacts as follows:

Contents of this Act

1 This Act consists of this section, sections 2 and 3 and the Schedules to this Act.

Commencement

2 (1) Except as otherwise provided in this section, this Act comes into force on the day it receives Royal Assent.

(2) The Schedules to this Act come into force as provided in each Schedule.

(3) If a Schedule to this Act provides that any of its provisions are to come into force on a day to be named by proclamation of the Lieutenant Governor, a proclamation may apply to one or more of those provisions, and proclamations may be issued at different times with respect to any of those provisions.

Short title

3 The short title of this Act is the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.

SCHEDULE 1
ENHANCING DIGITAL SECURITY AND TRUST ACT, 2024

CONTENTS

INTERPRETATION

Definitions

1 (1) In this Act,

"artificial intelligence system" means,

(a) a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments, and

(b) such other systems as may be prescribed; ("système d'intelligence artificielle")

"children's aid society" means a society within the meaning of the *Child, Youth and Family Services Act, 2017*; ("société d'aide à l'enfance")

"cyber security" means the security, continuity, confidentiality, integrity and availability of digital information and the infrastructure housing and transmitting digital information, and includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and information from attack, damage or unauthorized access; ("cybersécurité")

"Minister" means the Minister of Public and Business Service Delivery and Procurement or such other member of the Executive Council as may be designated under the *Executive Council Act* to administer this Act; ("ministre")

"prescribed" means prescribed by the regulations made under this Act; ("prescrit")

"public sector entity" means,

(a) an institution within the meaning of subsection 2 (1) of the *Freedom of Information and Protection of Privacy Act*, other than the Assembly,

(b) an institution within the meaning of subsection 2 (1) of the *Municipal Freedom of Information and Protection of Privacy Act*,

(c) a children's aid society, and

(d) a school board; ("entité du secteur public")

"school board" means a board as defined in subsection 1 (1) of the *Education Act*. ("conseil scolaire")

Artificial intelligence system

(2) For greater certainty, for the purposes of this Act, use of an artificial intelligence system by a public sector entity includes use of a system that is,

(a) publicly available;

(b) developed or procured by the public sector entity; or

(c) developed by a third party on behalf of the public sector entity.

Digital information

(3) For greater certainty, for the purposes of this Act, the collection, use, retention or disclosure of digital information by a public sector entity includes collection, use, retention or disclosure of digital information by a third party on behalf of the public sector entity.

CYBER SECURITY

Regulations made by Lieutenant Governor in Council

2 (1) The Lieutenant Governor in Council may make regulations governing cyber security at such public sector entities as may be prescribed, including,

(a) requiring public sector entities to develop and implement programs for ensuring cyber security;

(b) governing programs mentioned in clause (a), which may include prescribing elements to be included in the programs;

(c) requiring public sector entities to submit reports to the Minister or a specified individual in respect of incidents relating to cyber security, which may include different requirements in respect of different types of incidents;

(d) prescribing the form and frequency of reports.

Regulations re programs

(2) Without limiting the generality of clause (1) (b), a regulation made under that clause may require that a public sector entity's program include,

(a) roles and responsibilities of specified individuals within the public sector entity relating to ensuring cyber security;

(b) reporting on the public sector entity's progress with respect to ensuring cyber security;

(c) education and awareness measures respecting cyber security;

(d) response and recovery measures for incidents relating to cyber security; and

(e) oversight measures for implementation of the program.

Minister's regulations re standards

3 The Minister may make regulations setting technical standards that such public sector entities as may be prescribed by the Minister must conform to respecting cyber security.

Minister's directives

4 (1) The Minister may issue directives to public sector entities respecting cyber security.

Same

(2) A directive may be general or particular in its application, and may provide for different classes or categories.

Status

(3) Part III (Regulations) of the *Legislation Act, 2006* does not apply with respect to a directive.

Compliance

(4) A public sector entity to whom a directive is issued shall comply with the directive.

USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

Use, intended use

Application

5 (1) This section applies to such public sector entities as may be prescribed for the purposes of this section if they use or intend to use an artificial intelligence system in prescribed circumstances.

Information to public

(2) A public sector entity to which this section applies shall, in accordance with the regulations, provide information to the public about their use of the artificial intelligence system.

Accountability framework

(3) A public sector entity to which this section applies shall, in accordance with the regulations, develop and implement an accountability framework respecting their use of the artificial intelligence system.

Risk management

(4) A public sector entity to which this section applies shall take such steps as may be prescribed to manage risks associated with the use of the artificial intelligence system.

Requirements

(5) A public sector entity to which this section applies shall use the artificial intelligence system in accordance with any prescribed requirements.

Prohibited use

(6) A public sector entity to which this section applies shall not use an artificial intelligence system if the use is prohibited by the regulations.

Specific uses

Application

6 (1) This section applies in respect of such public sector entities as may be prescribed for the purposes of this section.

Obligations

(2) A public sector entity to which this section applies shall, when using an artificial intelligence system in prescribed circumstances,

(a) disclose information, in accordance with the regulations, respecting the use of the artificial intelligence system; and

(b) ensure that an individual,

(i) exercises oversight of the use of the artificial intelligence system, in accordance with the regulations, and

(ii) provides additional information, in accordance with the regulations, respecting the use of the artificial intelligence system.

Regulations made by Lieutenant Governor in Council

7 The Lieutenant Governor in Council may make regulations governing the use of artificial intelligence systems by public sector entities, including,

(a) prescribing public sector entities to whom section 5 or 6 applies;

(b) prescribing circumstances for the purposes of subsection 5 (1);

(c) governing the provision of information under subsection 5 (2), which may include,

(i) prescribing the manner in which information must be provided,

(ii) prescribing information that must be provided,

(iii) prescribing information that is not required to be provided,

(iv) specifying when information must be provided and updated,

(v) exempting public sector entities from the requirement to provide information in specified circumstances;

(d) governing the development of accountability frameworks under subsection 5 (3), which may include,

(i) prescribing the form and content of the accountability frameworks,

(ii) specifying when the accountability frameworks must be developed and updated,

(iii) prescribing roles and responsibilities of specified individuals under the accountability frameworks,

(iv) requiring documentation respecting the use of the artificial intelligence system, including documentation respecting different phases of its use, performance and monitoring;

(e) prescribing steps to be taken for the purposes of subsection 5 (4), including reporting and record-keeping;

(f) prescribing requirements for the purposes of subsection 5 (5), which may include requiring that an artificial intelligence system be used only for specified purposes;

(g) prohibiting, for the purposes of subsection 5 (6), the use of an artificial intelligence system;

(h) prescribing circumstances for the purposes of subsection 6 (2);

(i) governing the disclosure of information under clause 6 (2) (a), which may include,

(i) prescribing the manner in which information must be disclosed,

(ii) prescribing information that must be disclosed,

(iii) prescribing information that is not required to be disclosed,

(iv) specifying when information must be disclosed and updated,

(v) exempting entities from the requirement to disclose information in specified circumstances;

(j) governing the exercise of oversight for the purposes of subclause 6 (2) (b) (i);

(k) governing the provision of additional information for the purposes of subclause 6 (2) (b) (ii), which may include requiring the provision of information about how to make inquiries about the use of the artificial intelligence system.

Minister's regulations re standards

8 The Minister may make regulations setting technical standards that such public sector entities as may be prescribed by the Minister must conform to in their use of artificial intelligence systems.

DIGITAL TECHNOLOGY AFFECTING INDIVIDUALS UNDER AGE 18

Regulations made by Lieutenant Governor in Council

9 The Lieutenant Governor in Council may make regulations respecting such children's aid societies and school boards as may be prescribed,

(a) requiring prescribed digital information relating to individuals under age 18 that is collected, used, retained or disclosed to be collected, used, retained and disclosed in a prescribed manner;

(b) requiring reports to be submitted to the Minister or a specified individual in respect of the collection, use, retention and disclosure of information mentioned in clause (a);

(c) prohibiting the collection, use, retention or disclosure of prescribed digital information relating to individuals under age 18, which may include prohibiting such activities in prescribed circumstances, for prescribed purposes or subject to prescribed conditions.

Minister's regulations re standards

10 The Minister may make regulations setting technical standards that such children's aid societies and school boards as may be prescribed by the Minister must conform to respecting,

(a) the collection, use, retention and disclosure of digital information relating to individuals under age 18; and

(b) digital technology made available for use by individuals under age 18.

Minister's directives

11 (1) The Minister may issue directives to children's aid societies and school boards respecting digital technology made available for use by individuals under age 18.

Same

(2) A directive may be general or particular in its application, and may provide for different classes or categories.

Status

(3) Part III (Regulations) of the *Legislation Act, 2006* does not apply with respect to a directive.

Compliance

(4) A children's aid society or school board to whom a directive is issued shall comply with the directive.

GENERAL

No establishment of private law duty of care

12 Nothing in the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, this Act or any regulation made or directive issued under this Act establishes a private law duty of care owing to any person.

Effect of failure to comply

13 Failure to comply with this Act or any regulation made or directive issued under this Act does not affect the validity of any policy, Act, regulation, directive, instrument or decision.

Conflict, general

14 If a provision of this Act or the regulations made or directives issued under this Act conflicts with a provision of any other Act or regulation, the provision in the other Act or regulation prevails.

Directives, conflict

15 In the event of a conflict between a requirement set out in a directive issued under this Act and a directive made by the Management Board of Cabinet, the requirement in the directive made by the Management Board of Cabinet prevails.

Regulations, general

16 The Lieutenant Governor in Council may make regulations prescribing anything in this Act that is referred to as prescribed or otherwise dealt with in the regulations, other than anything in respect of which the Minister is given authority to make regulations or which is referred to as prescribed by the Minister.

COMMENCEMENT AND SHORT TITLE

Commencement

17 The Act set out in this Schedule comes into force on a day to be named by proclamation of the Lieutenant Governor.

Short title

18 The short title of the Act set out in this Schedule is the *Enhancing Digital Security and Trust Act, 2024*.

SCHEDULE 2
FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

1 Subsection 2 (1) of the *Freedom of Information and Protection of Privacy Act* is amended by adding the following definition:

"information practices" means the practices and procedures of an institution for actions in relation to personal information, including,

(a) when, how and the purposes for which the institution collects, uses, modifies, discloses, retains or disposes of personal information, and

(b) the administrative, technical and physical safeguards and practices that the institution maintains with respect to protecting the information; ("pratiques relatives aux renseignements")

2 (1) The French version of clause 15 (b) of the Act is amended by striking out "des renseignements confidentiels confiés à une institution par un autre gouvernement ou par l'un de ses organismes" at the end and substituting "des renseignements qu'une institution a reçus à titre confidentiel d'un autre gouvernement ou de l'un de ses organismes".

(2) The French version of clause 15 (c) of the Act is amended by striking out "des renseignements confidentiels confiés à une institution par une organisation internationale d'États ou l'une de leurs entités" at the end and substituting " des renseignements qu'une institution a reçus à titre confidentiel d'une organisation internationale d'États ou de l'une de ses entités".

3 (1) Subsection 34 (1) of the Act is repealed and the following substituted:

Annual report of head

(1) A head shall provide to the Commissioner an annual report with respect to the previous calendar year in accordance with this section.

(2) Subsection 34 (2) of the Act is amended by adding the following clause:

(c.1) the number of thefts, losses or unauthorized uses or disclosures of personal information recorded under subsection 40.1 (8);

(3) Section 34 of the Act is amended by adding the following subsection:

Form of report etc.

(5) The annual report shall be provided no later than the date specified by the Commissioner, if any, and shall be in the form and manner as may be specified by the Commissioner.

4 (1) Subsection 38 (1) of the Act is amended by striking out "section 39" and substituting "section 39 and subsection 40 (5)".

(2) Section 38 of the Act is amended by adding the following subsections:

Privacy impact assessment

(3) Unless the regulations provide otherwise, before collecting personal information, the head of an institution shall ensure that a written assessment is prepared that contains the following information respecting any personal information that the institution intends to collect:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.

3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended be collected.
5. The position titles of the officers, employees, consultants or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40 (1).
8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 40 (5) and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,
    i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    ii. to mitigate the risks to individuals in the event of such an occurrence.
10. Such other information as may be prescribed.

Risk mitigation

(4) The head of an institution shall ensure that the steps mentioned in paragraph 9 of subsection (3) are implemented,

(a) before collecting the personal information mentioned in that subsection; or

(b) if it is not possible to implement the steps before collecting the personal information, within a reasonable time after collecting the information.

Requirement to update

(5) Unless the regulations provide otherwise, before making any significant change to the purpose for which personal information mentioned in subsection (3) is used or disclosed, the head of an institution shall,

(a) update the assessment prepared under subsection (3) to reflect the proposed change and to set out the proposed intended use or disclosure; and

(b) implement any additional steps identified under paragraph 9 of subsection (3).

Copy to Commissioner

(6) The head of an institution shall, on request, provide the Commissioner with access to, or a copy of, an assessment prepared under subsection (3) or updated under subsection (5).

5 Section 40 of the Act is amended by adding the following subsection:

Privacy safeguards

(5) The head of an institution shall take steps that are reasonable in the circumstances to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the personal information are protected against unauthorized copying, modification or disposal.

6 The Act is amended by adding the following section:

Breach of privacy safeguards

40.1 (1) The head of an institution shall report to the Commissioner any theft, loss or unauthorized use or disclosure of personal information in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is real risk that a significant harm to an individual would result or if any other prescribed circumstances exist.

Report requirements

(2) The report mentioned in subsection (1) must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the head determines that the theft, loss or unauthorized use or disclosure has occurred.

Notification to individual

(3) Unless otherwise prohibited by law, the head of an institution shall notify an individual of any theft, loss or unauthorized use or disclosure of the individual's personal information that is in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is a real risk of significant harm to the individual or if any other prescribed circumstances exist.

Contents of notification

(4) The notification mentioned in subsection (3) must contain a statement that the individual is entitled to make a complaint to the Commissioner and any other prescribed information and must be made in the prescribed form and manner as soon as feasible after the head determines that the theft, loss or unauthorized use or disclosure of personal information has occurred.

Complaints — time limit

(5) A complaint mentioned in subsection (4) must be made in writing and filed with the Commissioner within one year after the subject-matter of the complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant, whichever is the shorter.

Extension of time limit

(6) Despite subsection (5), a complaint may be filed with the Commissioner after the time limit set out in that subsection if,

(a) the Commissioner is satisfied that the significance of the matter warrants a time extension and that the time extension would not result in any prejudice to any person; or

(b) the time limit set out in subsection (5) presents a barrier, as defined in the *Accessibility for Ontarians with Disabilities Act, 2005*, to the complainant and the Commissioner is satisfied that the time extension is reasonably required in the circumstances to accommodate the complainant for the purpose of making the complaint.

Real risk of significant harm — factors

(7) The factors that are relevant to determining whether a theft, loss or unauthorized use or disclosure of personal information creates a real risk of significant harm to an individual include,

(a) the sensitivity of the personal information;

(b) the probability that the personal information has been, is being or will be misused;

(c) the availability of steps that the individual could take to,

(i) reduce the risk of the harm occurring, or

(ii) mitigate the harm should it occur;

(d) any direction, recommendation or guidance provided by the Commissioner pertaining to what constitutes a real risk of significant harm; and

(e) any other prescribed factor.

Records

(8) The head of an institution shall, in accordance with any prescribed requirements, keep and maintain a record of every theft, loss or unauthorized use or disclosure of personal information reported under subsection (1).

Provision to Commissioner

(9) The head of an institution shall, on request, provide the Commissioner with access to, or a copy of, the record.

Definition

(10) In this section,

"significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Regulations

(11) The Lieutenant Governor in Council may make regulations respecting anything in this section that is referred to as being prescribed.

7 The Act is amended by adding the following section:

Commissioner's review of information practices

49.0.1 (1) The Commissioner may conduct a review of the information practices of an institution if the Commissioner has received a complaint under subsection 40.1 (4) or has other reason to believe that the requirements of this Part are not being complied with.

Informal dispute resolution

(2) Before conducting a review, the Commissioner may try to resolve the matter through mediation, conciliation or any other informal means of dispute resolution that the Commissioner considers appropriate.

No review

(3) The Commissioner may decide not to conduct a review for whatever reason the Commissioner considers proper, including if satisfied that,

(a) the institution has responded adequately to the complaint;

(b) the complaint has been or could be more appropriately dealt with, initially or completely, by means of a procedure, other than a complaint under this Act;

(c) there is insufficient evidence to warrant a review;

(d) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(e) the subject matter of the complaint is already the object of an ongoing review under this section; or

(f) the subject matter of the complaint has already been the subject of a review by the Commissioner.

Conduct of review

(4) In conducting a review referred to in subsection (1), the Commissioner shall review the institution's information practices to determine whether,

(a) there has been unauthorized collection, use, modification, disclosure, access to or retention of personal information collected under this Part; and

(b) the requirements under this Part, including requirements with respect to notice, retention, security and secure disposal, have been met.

Duty to assist

(5) The head and all officers, employees, consultants and agents of an institution shall co-operate with and assist the Commissioner in the conduct of a review, including using any data storage processing or retrieval device or system to produce a record required by the Commissioner in readable form.

Powers of Commissioner

(6) The Commissioner may require the production of such information and records that are relevant to the subject matter of the review and that are in the custody or under the control of an institution.

Orders

(7) If, after giving an opportunity to be heard to the head of the institution, the Commissioner determines that an information practice contravenes this Part, the Commissioner may order the head to do any of the following:

1. Discontinue the information practice.
2. Change the information practice as specified by the Commissioner.
3. Return, transfer or destroy personal information collected or retained under the information practice.
4. Implement a different information practice as specified by the Commissioner.
5. Make a recommendation in respect of how the information practice could be improved.

Limit on certain orders

(8) The Commissioner may order under subsection (5) no more than what is reasonably necessary to achieve compliance with this Part.

Procedure

(9) The *Statutory Powers Procedure Act* does not apply to a review conducted under this section.

8 Subsection 50 (4) of the Act is amended by striking out "under section 49.12 or an order made by the Commissioner under that section" and substituting "under section 49.0.1 or 49.12 or an order made by the Commissioner under either of those sections".

9 Subsection 55 (1) of the Act is amended by striking out "any other Act" at the end and substituting "any other Act, unless the disclosure is permitted for a prescribed purpose".

10 The Act is amended by adding the following section:

Whistleblowing

57.1 (1) Any person who has reasonable grounds to believe that an institution, a ministry data integration unit under Part III.1 or a multi-sector data integration unit under Part III.1 has contravened or is about to contravene this Act or the regulations may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality

(2) The Commissioner must keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

11 Subsection 58 (2) of the Act is amended by adding the following clause:

(0.a) the number of complaints received by the Commissioner in respect to the information practices of institutions and the number of reviews conducted under section 49.0.1;

12 (1) Clause 59 (b) of the Act is repealed.

(2) Section 59 of the Act is amended by adding the following subsections:

Consultations with other privacy commissioners

(2) The Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with a law enforcement officer or any person who, under an Act of Canada or of another province or territory of Canada, has powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information.

Agreements or arrangements

(3) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (2) in order to,

(a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(b) undertake and publish research or develop and publish guidelines or other documents related to the protection of personal information;

(c) develop model contracts or other documents related to the protection of personal information that is collected, used or disclosed interprovincially or internationally; and

(d) develop procedures for collecting and disclosing information referred to in subsection (4).

Collection or disclosure of information

(4) The Commissioner may, in accordance with any procedure established under clause (3) (d), disclose information, other than information described in section 12, 14 or 19 of the Act, to any person referred to in subsection (2) of this section or may collect information from any such person, if the information,

(a) could be relevant to an ongoing or potential investigation of a complaint, inquiry or audit under this Act or under an Act of Canada or of another province or territory of Canada that has objectives that are similar to this Act; or

(b) could assist the Commissioner or that person in the exercise of their powers or the performance of their duties or functions with respect to the protection of personal information.

Purpose and confidentiality

(5) The procedures referred to in clause (3) (d) must,

(a) restrict the use of the information to the purpose for which it was originally disclosed; and

(b) stipulate that the information be treated in a confidential manner and not be further disclosed for other purposes without the express consent of the Commissioner.

13 Subsection 60 (1) of the Act is amended by adding the following clauses:

(c.1) governing assessments under section 38, including prescribing information to be included in an assessment and providing for circumstances in which an assessment or an update is not required to be prepared;

. . . . .

(g.2) prescribing purposes for which disclosure is permitted under subsection 55 (1);

14 Clause 61 (1) (a) of the Act is amended by striking out "disclose" and substituting "collect, use or disclose".

15 (1) The definition of "customer service information" in subsection 65.1 (2) of the Act is repealed and the following substituted:

"customer service information" means, in relation to a service,

(a) the name, sex, gender identity, preferred language and date of birth of the individual to whom the service is to be provided,

(b) the address, email address and telephone number or other contact information of the individual to whom the service is to be provided and, if applicable, the person acting on behalf of that individual, and an indication of any accessibility or communication preferences,

(c) the transaction or receipt number, the order status, the shipping status, the product identification number and the product expiry date provided by the service provider organization in relation to the request for the service, as applicable,

(d) information relating to the payment of any fee,

(e) information relating to communications between the service provider organization in relation to the request for the service and the individual to whom the service is to be provided, and, if applicable, the person acting on behalf of that individual, and

(f) such other information as may be prescribed; ("renseignements liés au service à la clientèle")

(2) Section 65.1 of the Act is amended by adding the following subsection:

Additional uses of customer service information

(4.1) A service provider organization that collects customer service information under subsection (4) is authorized to retain and use the information, with the consent of the individual to whom the information relates, for the purposes of providing any designated service to the individual.

(3) Clause 65.1 (9) (a) of the Act is amended by striking out "clause (d)" and substituting "clause (f)".

Commencement

16 (1) Except as otherwise provided in this section, this Schedule comes into force on the day the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* receives Royal Assent.

(2) Sections 1 to 14 come into force on a day to be named by proclamation of the Lieutenant Governor.

Français

Back to top

Bill 194: Ontario's missed opportunity to lead on AI

December 2, 2024

What if the most transformative technology of our time — artificial intelligence — was already impacting Ontarians' lives without the protections we deserve?

Ontario's *Strengthening Cyber Security and Building Trust in the Public Sector Act*, arguably the most consequential bill of the current legislative session, was adopted last Monday.

Bill 194 regulates some of the most significant digital issues of our time: cybersecurity, artificial intelligence, and children's digital information. Yet it leaves all the critical rulemaking for future regulations to be set by government overseeing its own public institutions. The lack of transparency, explicit independent oversight and democratic process around this bill should be a concern for all Ontarians.

AI is already transforming public services in Ontario, shaping decisions in health care, education, and social services. Done right, AI can enhance efficiency and improve outcomes. Done wrong, it can cause serious harms and have discriminatory impacts. Bill 194 was Ontario's chance to set clear statutory guardrails for public sector use of AI. Unfortunately, that chance has come and gone, leaving Ontarians without the certainty and protections they deserve.

When AI systems influence decisions that touch people's lives, we must demand that they respect the fundamental principles we all value as a society.

To be trustworthy, AI systems must be valid and reliable. They must undergo meticulous testing, with human review, to verify that they're functioning reliably for the purpose for which they were designed, used, or implemented, under real-world conditions.

AI must be safe and designed to protect our lives, physical and mental health, property and economic security, and the environment. This requires robust monitoring and cybersecurity measures.

AI must be developed using a privacy-by-design approach, with safeguards built in right from the start to minimize data collection, reduce privacy and security risks, and ensure personal information is used only when necessary.

Institutions must be transparent about their use of AI by adopting accessible policies and practices that clearly explain to Ontarians how they are using AI and supporting their access to information rights.

They must also set clear rules and processes to manage every stage of AI development — from its creation and use to any changes or retirement of AI systems.

AI-enabled decisions by must be traceable — institutions must clearly explain how automated decisions are made and take responsibility for the outcomes. People must be provided with ways to challenge AI decisions, and there must be independent oversight to hold institutions accountable.

Most importantly, AI must affirm the human rights of individuals and communities and actively address historical biases to ensure that decisions made or assisted by AI are fair, non-discriminatory, and respectful of human dignity.

These are foundational principles. Yet Bill 194 mentions none of them. Instead, it authorizes the minister to set out eventual rules by way of regulation. Regulations are easier to make and change as the technology evolves. This need for flexibility may make sense at the level of technical detail, but not at the level of principle.

Can you imagine a world where we would *not* want AI to be valid and reliable, safe, privacy-protective, transparent, accountable and human rights-affirming?

These globally recognized principles should have been codified in Bill 194 to signal a clear government commitment to stand and live by them. Public institutions seeking to use Ontarians' data in AI systems or other applications should be bound by these principles as a *non-negotiable* part of the social contract. Principles as fundamental as these should not be left to the whim of a murky regulation-making process.

Moreover, these principles cannot exist in a vacuum — they require independent oversight to ensure compliance and hold public institutions accountable for potential misuse or harm. Bill 194 provides no clear or direct avenue for individuals to file privacy complaints to my office if they are legitimately concerned about the over collection, misuse or inaccuracy of their personal information and consequential decisions made about them, including through AI.

Without statutory guardrails and explicit independent oversight, Bill 194 missed the opportunity to secure Ontarians' trust in AI's promise to deliver a prosperous digital future for them and their children.

But continue forward we must. For my part, I will continue to advocate for stronger protections, clearer accountability, and independent oversight throughout the regulation-making process to ensure AI is used to serve Ontarians, not the other way around.

JANUARY 2026

Principles for the Responsible Use of Artificial Intelligence

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Ontario

Ontario Human Rights Commission
Commission ontarienne des droits de la personne

Contents

Preface

Artificial intelligence (AI) has the potential to significantly enhance the lives of all Ontarians. To realize this potential, it is imperative that AI systems are developed, acquired, used, and decommissioned in a manner that upholds safeguards for human rights, including the right to privacy. Accordingly, the Office of the Information and Privacy Commissioner of Ontario (IPC) and the Ontario Human Rights Commission (OHRC) continue to emphasize the importance of responsible and trustworthy AI adoption by the Ontario public sector and the broader public sector. The principles outlined herein, jointly developed by the IPC and OHRC, identify key concepts that will ground our assessment of organizations' adoption of AI systems consistent with privacy and human rights obligations.

The IPC–OHRC Principles represent a versatile and scalable foundation for responsible AI governance. These principles assist institutions in responsibly implementing AI innovations while ensuring the protection of privacy, human rights, human dignity, and public trust for Ontarians.

Institutions are strongly encouraged to adopt the IPC–OHRC AI Principles to ensure that their use of AI systems is responsible, transparent, and compliant with Ontario's human rights and privacy laws. These principles offer a clear, credible, and robust framework for assessing risk, guiding system design and deployment, and embedding accountability throughout the AI life cycle. By adhering to the IPC-OHRC principles, institutions can effectively safeguard individuals and communities from potential harms, show their commitment to fairness and substantive equality, and improve public trust. Ultimately, implementing the IPC–OHRC AI Principles helps ensure that AI systems uphold the rights and dignity of people affected, while fostering responsible innovation throughout the development, provision, and use of AI systems.

Organizations in Canada and internationally are increasingly implementing AI principles to address the challenges associated with adopting AI systems. Notable initiatives include the European Union (EU) Ethics Guidelines for Trustworthy AI,[1] the Group of Seven (G7) Hiroshima Process establishing International Guiding Principles for Organizations Developing Advanced AI Systems,[2] and the Organization for Economic Cooperation and Development (OECD) AI Principles.[3] In Canada, the federal government has introduced an AI strategy for the federal public service,[4] and Ontario has established a directive for all provincial ministries and agencies regarding the responsible use of AI.[5] The IPC–OHRC principles presented in this document are designed to complement these provincial, national, and international principles, while emphasizing the protection of human rights, including privacy laws.

1 Ethics guidelines for trustworthy AI: **https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai**

2 Hiroshima Process. International Guiding Principles for Organizations Developing Advanced AI systems: **https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document04_en.pdf**

3 OECD AI Principles: **https://www.oecd.org/en/topics/ai-principles.html**

4 AI Strategy for the Federal Public Service 2025-2027: **https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-overview.html#toc-3**

5 Ontario Responsible Use of Artificial Intelligence Directive: **https://www.ontario.ca/page/responsible-use-artificial-intelligence-directive**

What is artificial intelligence?

Ontario's *Enhancing Digital Security and Trust Act* (EDSTA), defines an "artificial intelligence system" as:

a) a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments, and

b) such other systems as may be prescribed.

For the purposes of the joint IPC–OHRC principles, we have adopted this EDSTA definition of AI systems. This definition is consistent with the OECD definition of an AI system.[6] The OECD's definition was created following a global consensus-seeking process with an extensive range of interested parties, and as such, represents a broad conception of what an AI system might include.

For clarity, the OECD definition applies to, among other things:

- automated decision-making systems
- systems which are designed to undertake activities that are typically performed using human intelligence and skills
- generative AI systems
- foundational large language models (LLMs) as well as their applications
- traditional AI technologies (e.g., spam filters or other cyber security resources, computer vision systems)
- any other emerging innovative uses of AI technologies

The life cycle of AI

The life cycle of AI includes the following stages:

1. **Design, data, and modelling**: This is the first stage in which system objectives, underlying assumptions, context, and requirements are specified. Data to power the AI system is collected, processed, and checked for quality. The AI system developers then create or select a model or algorithm that is trained or calibrated against the data set.
2. **Verification and validation**: At this second stage, developers assess their model for its performance against objectives. This could include assessing false positives, false negatives, and/or performance under a variety of conditions.
3. **Deployment**: The model and its overall system are launched for use in an environment. The system may begin to monitor the environment, assess collected data using its models, and generate outputs such as predictions, categorizations, decisions, and assessments.

6 OECD Definition: **https://oecd.ai/en/wonk/ai-system-definition-update**

4. **Operation and monitoring**: The AI system is in operation, with its outputs being used in service of the AI system's objectives. The system is monitored based on performance and quality evaluation criteria. Based on monitoring results, the system operators may take the system back to earlier phases to re-evaluate its design and training.[7]

5. **Decommissioning**: The life cycle ultimately extends to the decommissioning of an AI system. Decommissioning may take place because an AI system has reached its end of life or because it is routinely exhibiting unexpected outputs, and its behaviour cannot be corrected. The AI system, and the data used, including previously produced outputs, are retained as lawfully required to justify, rationalize, or explain past actions, as well as to assess the unexpected outputs and how individuals or communities have potentially been affected by them.

Each stage of the AI's life cycle should be assessed against the relevant principles in this document. Assessments at relevant stages should be conducted pursuant to an institution's role as a developer, provider,[8] or user[9] of a given AI system.

Principles for responsible use of AI

These principles are to be considered interconnected and of equal importance.

Principle: Valid and reliable

> AI systems must exhibit valid, reliable, and accurate outputs for the purpose(s) for which they are designed, used, or implemented.

To be valid, AI systems must meet independent testing standards and be shown, using objective evidence, to fulfil the intended requirements for a specified use or application. They must be proven to be reliable by performing consistently, as required, over a specified duration, and in the environments in which they are intended to be used. They must also be robust enough to maintain that level of performance across various other operating conditions, particularly in situations in which experiences and outcomes may differ for Ontario's diverse communities.

Validity and reliability standards contribute to the accuracy of observations, computations, or estimates so that results can be reasonably accepted as being true. However, the accuracy of results also depends heavily on the accuracy, completeness, and quality of the input data provided to the AI system. Even a highly valid and reliable tool can yield poor outcomes if it is provided with inaccurate, biased, or incomplete data.

---

7 Organization for Economic Co-Operation and Development. "The Technical Landscape." Artificial Intelligence in Society. June 11, 2019. **https://www.oecd.org/en/publications/artificial-intelligence-in-society_eedfee77-en.html**

8 A provider is defined as individuals or organizations that develop (including training) AI systems, or that put such services onto the market.

9 A user is defined as a staff member or agent of an organization who makes use of an AI system in the course of their institutional activities. Users do not design or provide the system, but they interact with, rely on, or apply its outputs to support decision-making, deliver services, or carry out organizational functions.

An AI system, therefore, should pass validity and reliability assessments prior to being deployed and be regularly assessed throughout its life cycle to confirm that it continues to produce accurate results and to operate as expected in a variety of circumstances.

Principle: Safe

> AI must be developed, acquired, adopted, and governed to prevent harm or unintended harmful outcomes that infringe upon human rights, including the right to privacy and non-discrimination.

AI systems should be monitored to support, among other considerations, human life, physical and mental health, economic security, and the environment. AI systems should be monitored and evaluated throughout their life span to confirm that they can withstand unexpected events or deliberate efforts that cause harm. This will, in part, require demonstrating that the AI systems have robust cyber security protection, and that human rights and privacy safeguards are firmly in place.

Any new use of a given AI system should undergo a comprehensive assessment process to ensure it will constitute a safe use in the new context. Safe AI systems must also make evident when they are producing unexpected outputs. AI systems should be temporarily or permanently turned off or decommissioned when they become unsafe, and any negative impacts to individuals and groups must be reviewed accordingly.

Principle: Privacy protective

> AI should be developed using a privacy by design approach. Developers, providers, or users of AI systems should take proactive measures to protect the privacy and security of personal information and support the right of access to information from the very outset.

AI systems should be developed using a privacy by design approach that anticipates and mitigates privacy risks to individuals and groups. This approach ensures that privacy protections are embedded into the system from the outset, proactively safeguard personal data, and respect the privacy of all individuals, especially those who are vulnerable or unable to provide informed consent. AI systems often interact with, or process, significant volumes of personal information in their development, training, or operation. The privacy protection principle requires clear lawful authority to collect, process, retain, and use these data. Accordingly, developers, providers, or users of AI systems must comply with applicable federal or provincial privacy laws, directives, regulations, or other legal instruments.[10]

10 AI systems can pose fundamental challenges to principles that have traditionally undergirded privacy legislation. The principle of limiting collection is challenged given that AI systems routinely require large and diverse volumes of data and information to best function. Data and information are sometimes re-used to train AI systems, placing pressure on the principle of purpose limitation, and what is learned during the training phases of AI systems may be retained after the training data is deleted with the effect of challenging the principle of limiting retention. Finally, even where organizations have attempted to anonymize information, the resulting data may sometimes be re-identified by AI systems.

Any use of personal information should be limited to what is required to fulfill the intended purpose. Institutions developing, providing, or using AI systems should reduce the need for large volumes of personal information using privacy enhancing technologies including de-identification methods or the use of synthetic data.

Privacy protective AI systems must build in measures to adjust the training data to mitigate any inherent bias and to ensure the accuracy of AI outputs, particularly where consequential decisions or inferences are being made about individuals or groups based on these outputs.

Individuals should be informed whether and when their personal information is being used in the development, refinement, or operation of an AI system, as well as the purpose and intended use of the AI system. Where appropriate, individuals should be provided with an opportunity to access or correct their personal information, including information about them generated by an AI system. Individuals should be provided with at least a right of review for automated decision processes that do not involve high risk, and the choice of opting out of high-risk automated decision processes that can materially impact an individual's well-being in preference of a human decision maker.[11]

AI systems must also be designed to protect the security of personal information from unauthorized access. Strong security safeguards are essential to ensure that personal information is protected from unauthorized access or misuse through the AI's life cycle.

Principle: Human rights affirming

> Human rights are inalienable, and protections must be built into the design of AI systems and procedures. Institutions using AI systems must prevent and remedy discrimination effectively and ensure that benefits from the use of AI are universal and free from discrimination.

Human rights law requires that developers, providers, and institutions ensure that they do not infringe substantive equality rights. This can be done by proactively identifying and addressing systemic discrimination in the design and deployment of AI systems on grounds protected under the *Ontario Human Rights Code (Code)*.[12] Institutions should take active measures to mitigate the discriminatory impacts present in AI systems and their associated data sets, such as adjusting training data to resolve any inherent biases detected through ongoing monitoring. In addition, institutions should avoid the uniform use of AI systems with diverse groups. Such a use, though seemingly neutral, may actually result in adverse impact discrimination.

11 Impact assessments are among the leading strategies to identify and assess for risk associated with AI systems. The OHRC (with the Law Commission of Ontario) and the IPC have impact assessments at their respective websites to identify, assess, and mitigate against human rights and privacy risks. For OHRC see Human Rights AI Impact Assessment: **https://www3.ohrc.on.ca/en/human-rights-ai-impact-assessment**. For IPC see Privacy Impact Assessment Guide: **https://www.ipc.on.ca/en/resources/planning-success-privacy-impact-assessment-guide-ontarios-public-institutions**.

12 Ontario Human Rights Code: **https://www.ontario.ca/laws/statute/90h19**.

Institutions have both privacy and human rights obligations to ensure that the collection, processing, and sharing of personal information or pseudonymous or anonymous data does not contribute to or reinforce existing inequalities or discrimination.

Likewise, government and governmental actors must comply with the rights guaranteed under the *Canadian Charter of Rights and Freedoms*, including the rights to freedom of expression, peaceful assembly, and association. This includes, but is not limited to, ensuring that AI systems do not unduly target participants in public or social movements, or subject marginalized communities to excessive surveillance that impedes their ability to freely associate with one another.

Principle: Transparent

> Institutions that develop, provide, and use AI must ensure that these AI systems are visible, understandable, traceable, and explainable to others.

Transparency involves providing clear notice about the use of AI systems, and adopting policies and practices that make visible, explainable, and understandable how AI systems work. Institutions developing, providing, or using AI must also ensure that AI systems are traceable and explainable. Transparency fosters public trust by enabling interested parties to understand how an AI system functions, how it produces its outputs, and the measures being taken to ensure that the AI system operates safely and accurately. Transparency consists of the following characteristics.

First, AI systems must be visible. This means that institutions should provide a public account that explains the operation of the system throughout its life cycle, from design and development to deployment and eventual decommissioning. This documentation may include privacy impact assessments, algorithmic impact assessments, or other relevant materials. Institutions must also be transparent about the sources of any personal data collected and used to train or operate the system, the intended purposes of the system, how it is being used, and the ways in which its outputs may affect individuals or communities. Importantly, this documentation should be written in clear, accessible language that avoids unnecessary jargon and technical complexity. Furthermore, institutions must notify individuals when they are interacting with an AI system and when any information presented to them has been generated by AI systems.

Second, AI systems must be understandable. This means that institutions must be able to explain how the technology operates and why errors may occur. To achieve this, they should document and retain sufficient technical information about the systems they are using so they can provide a full and transparent accounting of the basis on which decisions or actions were taken.

AI system's vendors should design and communicate about their AI systems in such a way that allows institutions that deploy and use them to understand how the AI system operates and how and why its outputs are generated as they are.

Third, AI systems must be explainable. This means institutions must be able to describe both the process (how) and the rationale (why) behind the outputs AI systems generate. This information should be communicated in a clear and accessible manner. The level of detail may

vary according to the audience — whether it is directed to the public, non-experts, individuals, or groups directly impacted by AI systems, or regulators overseeing institutional practices.

Fourth, AI systems must be traceable, meaning it must be possible for institutions to collect a thorough account of how the system operates, which can include:

- model details, such as the intended use of an AI system, type(s) of algorithm or neural network, hyperparameters, as well as pre- and post-processing steps
- training and validation data, including details on data gathering processes, data composition, acquisition protocols, and data labelling information
- AI tool monitoring details, which can include performance metrics, failures, and periodic evaluations[13]

Principle: Accountable

> Institutions should implement a robust internal governance structure with clearly defined roles, responsibilities, and oversight procedures, including a human-in-the-loop approach, to ensure accountability throughout the entire life cycle of their AI systems.

Incorporating robust internal governance structures, including a human-in-the-loop approach, ensures that human oversight is maintained throughout the life cycle of the AI system and allows for real-time intervention as needed.

Up front risk assessments should be carried out to identify and assess risks associated with the AI system, and to develop measures necessary to mitigate against them. Such assessments should include privacy and human rights impact assessments, algorithmic impact assessments, and others as relevant and appropriate.

Institutions should designate a person or persons responsible for overseeing the development, deployment, and/or use of an AI system, and for pausing or decommissioning an AI system that produces unsafe outputs or begins to operate in ways which are not valid or reliable.

Institutions should document their decisions about design and application choices in relation to AI systems. Where such a decision impacts specific groups or communities, they should be meaningfully informed and provided an opportunity to challenge that decision and any related outputs or results and seek recourse accordingly.

Institutions should be prepared to explain and provide plain language documentation on how the AI system works to an independent oversight body, upon request, and undertake any remedial or corrective actions as directed. Institutions must establish a mechanism to receive and respond to privacy, transparency, or human rights questions or concerns, as well as freedom of information requests, or to any challenges concerning how the AI system arrived at a decision or was used during a decision-making process.

13 European Parliamentary Research Service. 2023. “Artificial Intelligence in Healthcare: Applications, risks, and ethical and societal impacts.”

Members of institutions should be empowered through safe whistleblowing protections to report instances where an AI system does not comply with legal, technical, or policy requirements. Whistleblowers should be able to report non-compliance to an independent oversight body responsible for reviewing or overseeing the AI system, without fear of reprisal. Institutions should be subject to review by an independent oversight body with authority to enforce this and the other AI principles and require the organization to undertake remedial or corrective actions associated with the AI system.

Principles for the Responsible Use of Artificial Intelligence

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Tel.: (416)-326-3333
Website: www.ipc.on.ca
Email: info@ipc.on.ca

January 2026

Ontario Human Rights Commission

Commission ontarienne des droits de la personne

Office of the Chief Commissioner

180 Dundas Street West, Suite 900
Toronto ON M7A 2G5

Tel.: (416) 314-4537
Fax: (416) 314-7752

Office of the Information and
Privacy Commissioner of Alberta

Comments from the Office of the Information and Privacy Commissioner Regarding Responsible AI Governance in Alberta

July 15, 2025

Contents

1. Summary

This report highlights the developments in Artificial Intelligence (AI) legislation, and AI provisions in legislation, which subject matter is influenced by the emergence of AI. The conclusions drawn in this report stem from research involving legislative trends concerning the regulation of AI at the provincial, federal and International levels. Included in this report are considerations and recommendations for the Government of Alberta concerning whether and how to legislate the use of AI in Alberta.

- Chapter two sets out the scope and objectives of this report.
- Chapter three gives a summary of legislative recommendations, guidance and engagement reports issued by the Alberta Information and Privacy Commissioner relating to AI.
- Chapter four considers the benefits and requirements for implementing AI specific legislation, how it relates and interacts with Alberta's privacy legislation, and considerations because of the proposed Artificial Intelligence and Data Act (AIDA), EU AI Act , and other international standards.
- Chapter five discusses the legislative framework required to regulate for responsible and safe use of AI in Alberta.
- Chapter six sets out a policy framework, including interim measures, that is needed together with a legislative framework for a comprehensive model for responsible and safe use of AI in Alberta.
- Chapter seven sets out an engagement opportunity to work with the OIPC on developing a comprehensive legislative and policy framework to promote responsible and safe use of AI in Alberta.

2. Introduction and purpose

The Office of the Information and Privacy Commissioner (OIPC) is of the view that Alberta could benefit from a standalone law to regulate AI in the province that works alongside privacy laws, the latter of which will protect the rights afforded to individual Albertans concerning the collection, use or disclosure of their personal or health information to train AI, and to use AI where this involves processing personal or health information. An example of the latter is automated decision-making about Albertans.

The purpose of this document is to:

1. Set out the comments and recommendations we have made concerning these activities during the reviews of the *Freedom of Information and Protection of Privacy Act* (FOIP Act)[1] and the *Personal Information Protection Act* (PIPA);
2. Highlight our view of what needs to be regulated in privacy law versus what needs to be regulated in a standalone AI law;

[1] FOIP Act was repealed on June 11, 2025 and replaced with two Acts, the *Access to Information Act* and the *Protection of Privacy Act.*

3. Consider an Alberta-made AI-specific law in the light of AIDA, as proposed in Bill C-27[2], the EU AI Act, and other international standards and developments;
4. Recommend a comprehensive model for consideration by Government that will enable the responsible development and use of AI in Alberta.

As we have repeatedly stated in our comments and recommendations, the OIPC supports the responsible use of AI in Alberta because we recognize that, although there are risks to its use, there are many benefits that can be realized, including improving quality of public services and enhancing the delivery of health care.

It is our view that to strike the right balance between protecting privacy and achieving these benefits, there must be a legal framework that facilitates the development and use of AI while protecting the public. With the proclamation of the *Protection of Privacy Act* (POPA)[3], the development of this framework is already underway.

3. Previous recommendations

The OIPC issued comments and recommendations during the review of the FOIP Act and PIPA, which focused on the privacy rights that need to be codified in these laws to ensure Albertans are protected from uses of their information which may cause them harm.

Public sector privacy legislation

AI is having a profound impact on the way the public sector works, creates public policy, and interacts with citizens. Risks of inappropriate use of AI have already materialized in many cases[4].

On March 4, 2024, the OIPC submitted to the Department of Technology and Innovation (T&I) a document including a chapter setting out required changes to the FOIP Act regarding requirements for the adoption of AI in the public sector, highlights of which follow.

> *In terms of privacy rights, protections, and duties associated with the use of AI system by public bodies, and to ensure appropriate use, consideration should be given to:*
>
> - *Legislating authorized purposes for collection, use and disclosure of PI* [personal information] *for AI, for example in regards to training and deployment. An approach similar to the Canadian Federal Bill 27 AI provisions (AIDA) or EU AI act, may help ensure regulation where it matters, and no red tape where there is no need for AI regulation by distinguishing between unregulated uses, regulated uses and prohibited uses based on risk to individuals.*
>
> - *Codifying rights to ensure fair and privacy-respecting operation of AI systems, i.e., the right to object to automated decision-making and profiling by AI, the right to be informed about AI use,*

[2] Bill C-27 is a federal Bill intended to amend the *Personal Information and Electronic Documents Act* and sets out 3 new laws including the *Consumer Privacy Protection Act* and the *Artificial Intelligence and Data Act*.
[3] *Ibid.,* 1.
[4] See e.g. https://alaskabeacon.com/2024/10/28/alaska-education-department-published-false-ai-generated-academic-citations-in-cell-policy-document/ and https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

including requirements for the explainability such as plain language notice regarding collection and processing practices by AI systems. It is worth noting that with AI, privacy and fairness are closely connected as the fairness of outcomes relies on accurate PI, and unbiased processing of PI.

There should also be controls on the use of AI by public bodies to mitigate the risks of harm to individuals that may occur as a result of the use of the technology, such as:

- *Ensuring appropriate risk management of high risk and high impact AI applications such as when AI systems may process sensitive PI, which should trigger a duty to complete assessments such as PIAs, algorithmic impact assessments and STRAs. It may also be appropriate to conduct an ethical review.*
- *Incorporating limitation principles regarding collection, use and disclosure of PI for training or deploying AI, i.e., requiring the use of anonymized, synthetic data or de-identified PI whenever possible). Furthermore, purpose specification, accountability for AI systems and the roles of developers and deployers should be defined.*
- *Ensuring access, correction and deletion of PI used by AI systems, creating research provisions in relation to AI, ensuring regulatory oversight and redress mechanisms, and making sure the security of PI when processed by AI, must all be addressed in AI legislation pertaining to the public sector.*

Private sector privacy legislation

As part of its review of PIPA, the OIPC issued recommendations to the Standing Committee on Resource Stewardship. These recommendations generally echoed the high level issues raised for the review of the FOIP Act[5] but also specifically addressed the concerns with the use of automated decision-making in the private sector.

Summary of recommendations on page 8 of the report:

9. *That PIPA be amended to grant individuals the right to:*
    a. *contest automated decision-making; and*
    b. *be notified in plain language about the use of an automated decision-making system to make the decision before it is made.*
10. *That PIPA be amended to require organizations that make a profile, prediction, recommendation or decision about an individual using an automated decision-making system that either assists or replaces human judgment to:*
    a. *include in its publicly available policies and procedures a plain language general account of the organization's use of automated decision-making systems, an individual's privacy rights associated therewith, and how an individual can exercise these rights;*

[5] https://oipc.ab.ca/resource/pipa-review-2024/.

b. *before or at the time of collecting PI directly from the individual, require that individuals be notified about its use of automated decision-making, the significance or consequences of the same, the related rights of the individual, and the name of a person or position in the organization who can answer questions on behalf of the organization about the use of the automated decision-making system;*

c. *if indirectly collected PI is used, the same as under 10. b. applies plus an obligation to disclose where the indirectly collected PI was obtained, and under what authority it is being used;*

d. *inform the individual about the PI being used to make a profile, prediction, recommendation or decision, the source of the information, and the reasons and criteria used that led to the profile, prediction, recommendation or decision;*

e. *establish a process to enable the individual to:*

i. *review the accuracy of its PI used for automated decision-making;*

ii. *contest the use of automated decision-making to create a profile, prediction, recommendation or decision about them; and*

iii. *to request reconsideration by a human after the profile, prediction, recommendation or decision is made.*

11. *That PIPA be amended to require organizations that use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group to:*

a. *report statistics associated with the use of the automated system in a form determined by the Commissioner or by regulation;*

b. *regularly evaluate the outputs of the system to protect against harm and unfairness;*

c. *submit a PIA and/or AIA[6] to the Commissioner for review and comment prior to using the automated system; and*

d. *permit the Commissioner to establish how AIAs are to be conducted and their content and form.*

12. *Where an organization plans to use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group, that PIPA be amended to authorize the Commissioner to:*

a. *audit the use of an automated decision-making system to ensure the system in its design or use minimizes, to the degree possible, any harm or unfairness that may flow to an individual as a result of the use of the system;*

b. *review and comment on PIAs or AIAs submitted by an organization;*

[6] Algorithmic Impact Assessment (including both AI and simpler forms of algorithms).

c. *order an organization to stop using a system that may cause, has caused or is causing harm to an individual or group.*

The report also contained recommendations regarding building blocks and prerequisites for the responsible use of AI, such as, anonymization of personal information (used to train AI), and the reinforcement of privacy rights more broadly, to ensure a balance between enabling innovation and ensuring Albertans' protection of privacy.

Furthermore, in cooperation with privacy commissioners (and Ombuds) across Canada, we issued high level principles for responsible, trustworthy and privacy-protective generative AI[7], which can be taken into consideration when drafting legislation.

Some of the most harmful applications of AI seen to date have originated from the private sector[8]. Without sufficient regulation, the cost to the public purse of enforcing fundamental rights is considerable given the efforts expanded to fighting infractions of such rights in the courts[9].

Health privacy legislation

We are aware that there are many use cases for the development of AI in Alberta to enhance the provision of healthcare, and active adoption of AI in healthcare is taking place at a rapid pace in Alberta.

In the absence of legislation, the OIPC has issued guidance to provide some information and best practices regarding the privacy-preserving adoption of AI in a small custodian setting[10]. If changes to HIA are made and AI is addressed, it should follow the same high-level recommendations as provided for in PIPA and the FOIP Act[11], but also take into consideration the higher sensitivity of health information (HI), and high impact when using AI in healthcare-related processes, as compared to most other types of information or AI applications. Consequently, high standards should apply for AI applications processing HI in terms of information security, due care and testing for reliable outcomes, human control and other aspects that will help detect and prevent harm. The OIPC's recent survey of Albertans highlighted that there are serious concerns and apprehension regarding the use of AI as part of health care delivery, and they see benefit to measures such as requiring transparency and human oversight.

4. Regulating Artificial Intelligence in Alberta

Scope of AI specific legislation

Generally, AI legislation has been created for the purpose of allowing safe, transparent, traceable, non-discriminatory use of AI. These laws establish the conditions for the development and use of AI systems while protecting against harms.

---

[7] https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/ .
[8] See e.g. the investigation and orders from the OIPC related to Clearview AI, here https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ and here https://oipc.ab.ca/clearview-ai-order/
[9] https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=408:clearview-ai-and-compliance-with-canadian-privacy-laws&Itemid=80.
[10] https://oipc.ab.ca/resource/ai-guidance-for-small-custodians-on-the-use-of-artificial-intelligence/.
[11] *Ibid.*, 1.

For example, the proposed Bill C-27's *Artificial Intelligence and Data Act* (AIDA) aims to protect Canadians from high impact uses of AI, and at the same time promote the responsible development of AI in Canada and elevate the global standing of Canadian firms participating AI development. Its risk-based approach, and key definitions and concepts, are designed to align with internationally set standards (by law and otherwise), such as the EU AI Act, the OECD AI Principles, and the U.S. NIST AI Risk Management Framework.

Common elements contained within these laws ensure the following:

- safety, robustness and security;
- transparency and explainability;
- traceability and accountability;
- non-discrimination and non-bias;
- human oversight;
- fairness;
- preservation of privacy; and
- respect for human rights and democratic values.

Relation between AI legislation, privacy legislation and other legislation

Both AIDA and the EU AI Act focus most requirements and effort on AI systems that are considered high impact on, or high risk for society. The EU AI Act originates from and works within the EU digital strategy and is part of a framework of related laws[12] such as General Data Protection Regulation (GDPR), the European Health Data Space Regulation (EHDS), the Digital Services Act (DSA), Digital Markets Act (DMA) and the Network and Information Security Directive (NIS2). AIDA and CPPA, as part of Bill C-27, are one of the ways implementation of Canada's Digital Charter is taking place.

1. **A standalone AI law in Alberta would benefit from assuring a high level of conformance with the common elements outlined above to ensure reasonable protection from harm to individuals and enable access to international markets.**
2. **Although conformance is important, such a law could still be customized to the unique context of Albertans' values and industries and assure a measure of provincial control wherever provincial jurisdiction would apply. Additionally, it would be necessary to have such a law to provide for those aspects beyond federal jurisdiction (health and public sectors, provincial commerce).**
3. **AI laws generally form part of legislative frameworks addressing broader digital strategies[13]. The Government of Alberta's Department of Technology and Innovation is**

[12] For a more complete consideration of EU legislation see this overview.
[13] See for example Canada's Digital Charter, or the EU's digital decade initiatives.

already working on creating such a strategy[14]. Changes to privacy legislation and the creation of standalone AI legislation would benefit from integration with such a legislative framework thereby addressing digital transition broadly.

AI legislation alone is not enough to sufficiently regulate all the impacts of AI. AI specific legislation benefits from other laws that work in conjunction with it. For example, regulating automated decision-making used to make decisions that may directly affect an individual and prohibited or restricted uses of AI for certain activities, such as profiling, are generally contained in privacy laws as they form part of the suite of privacy rights in most jurisdictions. In addition, related subjects that serve as building blocks for the development of various types of AI systems are also generally found in privacy laws, such as the requirement to use non-personal information to train AI or controls on the use of personal information for the same if permitted, controls on data matching, and information security requirements to protect this information.

4. To prevent harm and respect the fundamental rights and freedoms of Albertans, regardless of any AI legislation being enacted, Alberta's privacy laws need to continue modernizing to ensure that they each offer sufficient privacy protections when personal information or, derivatives, such as non-personal information, of Albertans is used to train AI or AI is used to make decisions that directly affect them.

Somewhat like the relationship between the AI EU Act and GDPR, the proposed AIDA is designed to work with the proposed *Consumer Privacy Protection Act* (CPPA)[15]. CPPA is meant to replace the *Personal Information Protection and Electronic Documents Act* (PIPEDA). CPPA's terms, such as automated decision systems, overlap with AIDA's definition of AI systems. The difference in scope is set out in each Act's purpose statements. CPPA's provisions are primarily concerned with authority to process personal information in the first place and the accuracy of personal information when decisions[16] are made about an individual. It also ensures that when AI is used to make decisions that affect an individual, there is transparency about the use and explainability[17] of the same. AIDA applies to AI more broadly and its provisions aim to reduce risks to a broader set of individual rights[18]. This may include automated decision-making, but also other uses of AI as long as they either affect individuals or have an adverse impact due to systemic bias in a commercial context.

POPA and its regulations, as recently enacted, did not incorporate most of our recommendations regarding regulating AI. The only AI related provisions in POPA are:

[14] https://www.alberta.ca/digital-strategy-engagement.
[15] Within Bill C27.
[16] CPPA Section 56(2)(a).
[17] CPPA Section 62(2)(c) and Section 63(3) and (4).
[18] AIDA Section 7-12.

- the obligation of public bodies to notify individuals about the use of automated decision-making or content generation at the time of collection of the personal information[19];
- the use of automated decision-making by the public bodies generally[20]; and
- accuracy and retention obligations for personal information used in automated decision-making[21].

There is currently no requirement to:

- document decision factors[22] (other than the retention requirement regarding personal information and the decision itself[23]);
- right to opt-out of, object to, or ability to ask for human review of automated decisions; or
- establish a channel for complaints specific to the process or outcomes regarding automated decision-making.

To regulate AI generally and automated decision-making particularly, ensuring Alberta's legislation is harmonized with standards set in other Canadian provinces, the EU and various other countries[24] that have modernized their privacy laws and are contemplating or have introduced AI specific laws[25], is important. Doing so will both protect Albertans and provide recourse against harms, and at the same time enable entities that deploy and develop AI to more easily ensure compliance of their products and services, i.e. in line with the requirements of Alberta's major trading partners.

PIPA and the *Health Information Act* (HIA) are expected to be amended in the near future, and the chance should not be missed to include adequate and internationally and provincially harmonized requirements regarding automated decision-making and, if no legislation regarding AI is forthcoming, AI more broadly, in these laws.

Considering AIDA in the Alberta context

AIDA - Scope and Framework

AIDA applies to "persons", which are defined to include a trust, a joint venture, a partnership, an unincorporated association and any other legal entity. AIDA applies to any person "who is responsible for an artificial intelligence system, including a high-impact system, if in the course of international interprovincial trade and commerce, they design, develop or make available for use the artificial intelligence system or manage its operation"[26]. Persons subject to AIDA are *inter alia* required to do the following.

- Assess whether its AI system is a high-impact system[27].
- If it is a high impact system:

[19] POPA section 5(2)(d).
[20] POPA ministerial regulation 6(1)(b)(iii).
[21] POPA section 6.
[22] See e.g. Quebec Law 25 section 21 amending 65.2(2).
[23] POPA section 6 (b).
[24] For example, Brazil's *Lei Geral de Proteção de Dados Pessoais* (General Data Protection Law).
[25] See IAPP's AI law tracker for an overview of AI laws in force, bills introduced, and other related policy instruments https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf.
[26] AIDA Section 5(2).
[27] AIDA Section 5(1) and AIDA's amendments schedule 2.

    - establish measures to identify, assess and mitigate the risk of harm or biased output that could result from the use of the system; and
    - establish measures to monitor compliance with these mitigation measures.
- Keep records of these measures and reasons concerning the assessment of risk.
- Publish in plain language a description of the system with an explanation of:
    - how it will be used;
    - the types of content it intends to generate and the decisions, recommendations or predictions it is intended to make; and
    - the risk mitigation measures.
- Notify the responsible federal minister if the use of the AI system results or likely to result in material harm.

AIDA, as currently proposed, largely follows the EU AI Act in this respect. Differences are its scope[28], i.e. the AI Act applies to the public sector, health sector, and member state internal trade and commerce, with only very limited exceptions. The oversight model used in the AI Act is another significant difference, as it leverages the EU's Data Protection Authorities[29] and allows member states to create or assign independent AI regulators[30] as opposed to AIDA's model (discussed below).

Apart from some well documented, and well-founded critiques[31], AIDA may go a long way in regulating interprovincial trade and commerce but obviously leaves jurisdictional gaps for the federal government, and where provincial and territorial jurisdictions apply. AIDA does not apply to intraprovincial trade and commerce in Alberta. Nor does it apply to public sector entities, including public bodies and public health custodians.

AIDA - Oversight

From an oversight perspective, AIDA allows for information relating to regulated activities to be disclosed to the federal Privacy Commissioner[32], but delegates administration and enforcement of AIDA to the minister responsible for AIDA. AIDA permits the minister to designate an Artificial Intelligence and Data Commissioner from within the minister's department to assist the minister. AIDA does not apply to a "government institution" as defined in the *Privacy Act* or to a "federal or provincial department or agency and who is prescribed by regulation".[33] By virtue of the trade and commerce power used by the federal government for AIDA, as indicated, it would also not apply to organizations' activities concerning the use of AI occurring within Alberta.

Although this model of oversight may be sufficient[34] for AIDA, because there is no direct conflict of interest between the entity tasked with oversight (the minister) and the subject of oversight

[28] See EU AI Act Article 2.
[29] See EU AI Act Article 5 and 21.
[30] See https://artificialintelligenceact.eu/national-implementation-plans/.
[31] See e.g. the open letter from various academics and civil liberty groups send to minister François-Philippe Champagne, responsible for AIDA https://openmedia.org/files/AIDA_JOINT_LETTER_FOR_SIGN_ON_(1).pdf .
[32] AIDA Section 26(1)(a).
[33] AIDA Section 3.
[34] It should still be noted that making a minister responsible for oversight is less robust than assigning such responsibilities to an officer that reports to the legislature, which for that reason is the standard model of oversight in much of the western world.

(international and interprovincial trade and commerce), in Alberta, such a model is not desirable given the need to ensure independence of oversight on government use of AI.

5. Any AI Commissioner or other official with an oversight role on AI in Alberta should, especially where it pertains to the public sector use of AI, report directly to the legislature, similar to the Auditor General, Ombudsman, and the Information and Privacy Commissioner.

Efficient oversight of Alberta-made AI legislation

The Information and Privacy Commissioner wears two hats. As Information Commissioner, the Commissioner is responsible for monitoring compliance with the access to information provisions in POPA, ATIA, PIPA and HIA and for advocating for information rights of Albertans. As Privacy Commissioner, the Commissioner is responsible for monitoring compliance with our privacy laws, POPA, PIPA and HIA and for advocating for privacy rights.

Personal information is very often a core component of AI development and deployment, and many of the harms associated with the use of AI stem from the (mis)use of personal information[35]. The OIPC is already reviewing privacy impact assessments concerning the use of AI by entities subject to our privacy laws. Building on the existing expertise and processes, the OIPC is well positioned to include oversight, and assessment of AI systems in accordance with an Alberta-made AI Act as part of its tasks. OIPC oversight under an AI act could include: assessment of compliance regarding AI-specific privacy rights and obligations; reviewing risk assessments, and contributing to systemic oversight on fundamental rights and public interest provisions. Fairness, accountability, transparency, and security are principles that the OIPC routinely operationalizes from an access to information and privacy perspective and will be equally important under AI legislation.

As with the EU AI Act[36], red-tape can be reduced by harmonizing privacy impact and conformance, algorithmic, or fundamental rights impact assessments[37]. Public funds can be efficiently used by building on the OIPC's existing processes and skills and applying them to such oversight roles (e.g. reviewing and following up on these assessments) as an AI Act would require.

[35] Unethical/illegal forms of, *inter alia*, profiling, biometrics, biased decision making, social scoring, vulnerability exploitation (subliminal techniques, emotional recognition etc.), criminal risk assessment, etc.
[36] See EU AI Act, Articles 27(4), 43 and 26(9).
[37] As the case may be under a new Act. The EU AI Act leverages Conformance, and Fundamental Rights Impact Assessment (FRIA) alongside and in concurrence with GDPR's Data Protection Impact Assessment (DPIA). The Canadian Federal Government has made Algorithmic Impact Assessments (AIA) mandatory under its *Directive on Automated Decision-Making.*

6. **Responsibilities for oversight regarding the processing and use of AI in public, health, and private sector could for significant parts be assigned to the Information and Privacy Commissioner, similar to how this has been structured under the EU AI Act.**

7. **To reduce red tape and ensure efficient and effective use of oversight resources, consideration should be given to, in addition to or in lieu of the creation of a specific AI oversight body, leveraging expertise and powers of existing oversight bodies, as regulated AI use will likely intersect with the jurisdictions of the Ombudsman, Human Rights Commission, and Information and Privacy Commissioner. Sector specific bodies such as Research Ethics Boards and the Fraud and Consumer Protection Agency function of the Department of Service Alberta and Red Tape Reduction, and similar entities, could be equipped and are well suited to extend their roles for specific oversights tasks related to AI.**

8. **Consideration should be given to streamlining compliance obligations for organizations subject to AI legislation, with such obligations under privacy and other legislation.**

An Alberta AI Law is needed to clarify the rules and instill trust and confidence

With AIDA focusing on high impact AI systems, and CPPA focusing on the processing of personal information and potential harms occurring from this processing, these acts together work to protect individuals from harms that may occur through the design and use of AI systems, including protection from privacy harms. In Alberta a similar approach is possible.

As indicated, there have been changes to modernize our public sector privacy law, POPA, which addresses certain aspects of automated decision-making, but as we indicted above, does not go far enough to adequately protect privacy when AI is used by public bodies. We anticipate both PIPA and HIA to be amended in the near future and we will advocate for adequate provisions in these laws to protect the privacy rights of Albertans in the use of AI by custodians and private sector organizations. It is unclear as of the date of writing this report whether Bill C-27 will proceed as is or be replaced. Use of AI is rapidly advancing in Alberta by businesses operating within Alberta. There are harms that can occur to the public without an adequate legislative framework to protect them, including in privacy and other AI regulating laws. To that end, we strongly encourage the Government of Alberta assess the gaps regarding the protection of Albertans from the harms that may flow from use of AI by public bodies, custodians and private sector organizations by regulating AI in the province, which, in our respective view, will build trust in the use of AI by both the public and Alberta-based entities, and instill greater confidence by these entities in the use of AI in the province.

9. POPA, PIPA, and HIA should be complemented by a standalone AI law to achieve a similar coverage to AIDA and the CPPA for the prevention and reduction of harm to Albertans under provincial jurisdiction (i.e. business activities concerning the use of AI in Alberta, and the provision of health care and government programs and services in Alberta). An AI Act should be broad in scope, and work harmoniously with privacy legislation, and other legislation needed to execute Alberta's digital strategy while ensuring adequate protection for Albertans.

Privacy legislation in Canada and internationally is being, and should be, further modernized to specifically regulate those uses of AI that rely heavily on personal information, such as requiring that personal information be anonymized prior to being used to train AI. This approach would be similar to AIDA and CPPA, or the EU AI Act and GDPR in the EU. In Alberta, POPA has laid the foundations for a similar approach by including provisions defining and/or regulating non-personal data, synthetic data, data matching, data derived from personal information, and some activity concerning automated decision-making.

In the previous chapter we highlighted that AIDA misses the mark in key areas such as scope and oversight. An AI law made in Alberta could address these gaps and greatly strengthen the protection of Albertans. The necessity to do so is apparent in the following ways:

- Regulation is needed to both ensure protections and rights to Albertans and eliminate uncertainty for entities who want to adopt AI for all sorts of commercial or otherwise beneficial purposes in all sectors. In the U.S., individual states are taking the initiative to regulate AI in absence of meaningful action by the federal government.
- Our survey of Albertans underscores this issue, showing high concern with, and low support for the use of AI in healthcare and government service delivery[38]. Albertans do say their comfort for this practice increases when controls and restrictive measures are applied to the use of AI[39].
- The majority (ca. 65%) of our health custodian respondents to our engagement survey[40] indicate that they have concerns about patient privacy with the use of AI, both regarding the nature of the technology but even more related to the business models and practices used to make AI profitable to vendors. Furthermore, responses highlight uncertainty about what the requirements for implementing the technology safely and adequately are, and if patient data is sufficiently protected from vendors' interests by regulation. Although nearly all see the upside AI can bring, there does not seem to be the comfort needed to comprehensively adopt the technology and its benefits due to lack of clear standards, vendor transparency, and oversight.

To highlight the concerns in two of the respondents' own words:

> *"New technology is an inevitable transition in modern healthcare. But as they are new and outside existing systems of course I worry. There needs to be a standard so we can trust these*

[38] See page 44-48 of our general public HIA engagement report.
[39] Ibid. page 49-53.
[40] See our custodian engagement survey results.

technologies will meet the needs of our patients. For instance I use an EMR in one clinic environment which facilitates charting via AI if enabled. I do not enable this feature because endorsement by the CPSA is murky with respect to privacy. If there was clear guidance regarding this technology for Alberta from the CPSA or the ministry then I would expect the product developers would be incentivized to meet that standard so I could actually use it. "

"We need a clear way of working on these technologies in a safe environment. Lack of laws surrounding how to manage this is causing a lag in our ability to apply this technology and improve efficiency and patient care."

5. Broader AI legislative framework

As discussed in the previous chapter, successful implementation of AI legislation is an effort between various laws, regulations and practices that together with an AI specific law, and privacy laws form an AI legislative framework. Below are some of the more important building blocks of such a framework. Note that some of these building blocks apply generally to the use of AI, and others are specific to use in the public sector, for which additional considerations apply.

Fundamental rights and freedoms

As indicated in the Commissioner's comments on amendments to PIPA[41], privacy laws protect informational privacy rights of Albertans which are enshrined in POPA, HIA and PIPA. Privacy law in Canada stems from a number of sources including the UN Declaration on Human Rights, fair information principles, and good governance principles (e.g. relating to access, correction, transparency and accountability). Canadian courts have recognized these rights as essential to protecting individual autonomy. While these laws provide some protection regarding the use of AI, they are insufficient when it comes to protecting Albertans from the broader impacts of AI. Therefore, privacy laws must be complemented by and work in tandem with AI specific legislation and other legislation as may be needed to adequately address the risks and societal impacts regarding the use of AI.

10. **AI legislation or privacy legislation should include prohibitions or restrictions on training or using AI with specific sensitive personal information unless when used for prescribed purposes (e.g. scientific or public interest).**
11. **AI specific legislation should consider if certain uses of AI are to be prohibited, e.g. for purposes as found in the EU AI Act, as well as in AIDA.**
12. **A framework of legislation, including AI specific legislation, should be developed to fully protect Albertans' rights and freedoms for any use of AI in the province.**

[41] Beginning at p. 21, https://oipc.ab.ca/wp-content/uploads/2024/06/OIPC-Submission-to-PIPA-Review-May-2024.pdf.

Due care where rights and freedoms are involved

Certain AI models are at risk of model collapse and bias, and susceptible to deliberately placed traps (model poisoning and malicious prompt engineering). A more comprehensive list can be found in the footnotes. Generative AI shows weaknesses such as affirmation bias, overfitting and hallucinating, limiting its usefulness or requiring strict human oversight. Awareness of these two types of limitations, and tools to detect and deal with them, as well as general knowledge about the capabilities and limitations of AI, should be required for staff working in projects deploying such AI, especially where fundamental rights and freedoms may be at stake. Doing so will create a degree of AI fluency in the workforce. Without a sufficient degree of AI fluency, incidents such as data breaches or violations of privacy and other fundamental rights are likely outcomes. Apart from the skills of the workforce, organizations must learn to adapt their processes to leverage the benefits from AI, while monitoring its outcomes and risks, and compensating for its weaknesses and limitations.

When stakes are higher (say government uses AI to assist in the provision of services or to generate or collect inputs in making decisions about public policy), due care is of particular importance, such as by continuous monitoring of the effects and outcomes against principles of good governance, fairness, and fundamental rights such as privacy, human rights, etc.

13. AI specific legislation would benefit from the inclusion of authoritative standards or codes of practice for testing, auditing and organizational due care generally required to ensure applicable legislative requirements, especially in regards to fundamental rights and freedoms, are operationalized and effective[42].

AI usage in areas of public interest

In areas of public interest, such as with misinformation and deepfakes during elections and during emergency situations (e.g., a pandemic or natural disaster), the use of AI can result in a real threat to public order and social stability. There is a strong case to be made for mandatory transparency of AI use to generate or distribute information (including images, videos, social media posts and news articles) in the public domain that has importance for elections, emergencies and similar high stakes public interest events. A precedent for transparency and labeling requirements for AI use relating to information generated for such events exists, e.g., Spain and China. There is currently no regulator that would be an obvious candidate for providing oversight of such requirements in Alberta, but the OIPC has many tools and processes in its existing mandate that would, with minor adaptions, be able to facilitate such oversight.

14. Through legislation, malicious uses of AI to disrupt public order or influence public opinion around elections must be made transparent, monitored and where necessary, limited by prohibitions, restrictions and penalties.

[42] For an example of how this could work, see the EU's implementation of same.

De-identification regulation

AI relies on large quantities of data for both training and regular operations. Where such data constitutes personal information, or health information, legal authority is required for processing. If no legal authority exists, or authority exists but high risks of processing remain, various forms of de-identification can help reduce the risks. Various degrees of de-identification, such as creating synthetic data, can help ensure the benefits of AI are reaped without having to resort to high risk processing[43]. Recent changes included in POPA[44] enable the ability to create such data.

Although AIDA includes references to anonymized data[45], there is no framework to help determine what is needed to determine if data is in fact anonymized. CPPA has a definition[46] that can serve as the basis for a standard to achieve such an assessment.

15. **AI legislation should incorporate privacy by design principles, including for training AI, and require the use of least privacy invasive forms of information for training AI wherever possible (in order of preference: anonymized information or synthetic data, de-identified information, pseudonymized information, personal information).**

16. **Privacy legislation should specify the requirements for information to qualify as anonymized information, synthetic data, de-identified information, pseudonymized information, and personal information.**

Automated decision-making

Automated decision-making may be done with the help of AI, or simpler algorithms to increase efficiency of accuracy for decision-making. However, there are risks to deploying AI in such a capacity when it makes decisions based on personal information and/or affects an individual, and many incidents stemming from the use of AI have been documented[47]. To balance out the risk of using AI in such a capacity, measures such as the right to object, challenge, or the right to request human review have been included in privacy laws, such as GDPR and Quebec's Law 25. Any legislative amendments to privacy laws in Alberta should incorporate such important balances in addition to the transparency requirements already included under POPA's section 5(2)(d) for automated decision-making.

[43] See chapter 6.5 of the March 4, 2024 OIPC submission *Freedom of Information and Protection of Privacy Act Comments and Recommendations from the Commissioner* for more information.
[44] See e.g. section 21 and the rest of Part 3 Division 2 of POPA.
[45] AIDA section 6.
[46] CPPA section 2(1).
[47] See e.g. the Royal Commission into the Robodebt Scheme, Royal Commission, 2023.

17. **Where an individual may be affected by an AI-made decision, including when the decision is based on personal information or information directly derived from or matched with their personal information, this aspect of automated decision-making should be regulated by privacy legislation.**

18. **Where fundamental rights of individuals or groups, e.g., as a result of bias, may be more broadly affected by AI uses, such as through automated or assisted decision-making, AI legislation should provide recourse and oversight by various regulators, similar to the EU AI Act[48].**

19. **In some cases, the two areas above may overlap with the duties of other regulators (e.g., consumer protection, ombuds, human rights). There should be provisions that permit the sharing of information as may be necessary, and to jointly investigate these matters among regulators as applicable.**

Information security requirements

There are information security vulnerabilities, risks and harms that are specific to AI. Legislation regarding AI should acknowledge this and ensure that responsible entities take the appropriate measures to prevent harms from materializing. To operationalize these measures. industry standards or codes of conduct should exist, and additional resources should be created to help detect and address these AI specific risks[49] . Information security of AI should be made mandatory by law, but operationalized at a lower level to allow for dynamic adaption to advances in technology.

20. **To prevent privacy harm and other harms to Albertans via security compromise of AI systems, legislation should be created or adjusted that ensures adequate information security requirements apply to such systems. Such a requirement could be addressed in privacy legislation, AI legislation and/or information security-specific legislation. Furthermore, vulnerabilities specific to AI must be taken into account in information security regulations or standards[50].**

21. **It is of great importance that accountability for AI information security is clear, i.e., what is the responsibility of the developer of the AI system, and what of the entity deploying the AI. This relationship should be regulated, e.g., to ensure reporting of breaches by the former to the latter party.**

[48] See Articles 74 and 77 of the EU AI Act.
[49] https://genai.owasp.org/llm-top-10/.
[50] https://owasp.org/www-project-ai-security-and-privacy-guide/.

Privacy-related harms are not solely addressed in privacy or AI-specific legislation

Not all harms stemming from a violation of privacy are addressed under Alberta's privacy laws or would be sufficiently addressed in a generic AI specific law. Certain aggravated abuses of personal information are addressed under the criminal code[51] or specific laws[52], such as the creation and distribution of deepfake pornography or child sexual abuse materials (CSAM). It should be noted that Alberta's *Protecting Victims of Non-Consensual Distribution of Intimate Images Act* is missing the modernization that has taken place in BC[53], which also address 'altered images', thereby somewhat addressing the role of AI in the creation of such materials.

22. Consider amending or creating AI-related laws in conjunction with privacy or AI specific law to create a framework that protects Albertans in the best possible way. Alberta's *Protecting Victims of Non-Consensual Distribution of Intimate Images Act* is one such example.

Public sector-specific considerations

Transparency regarding public sector AI usage

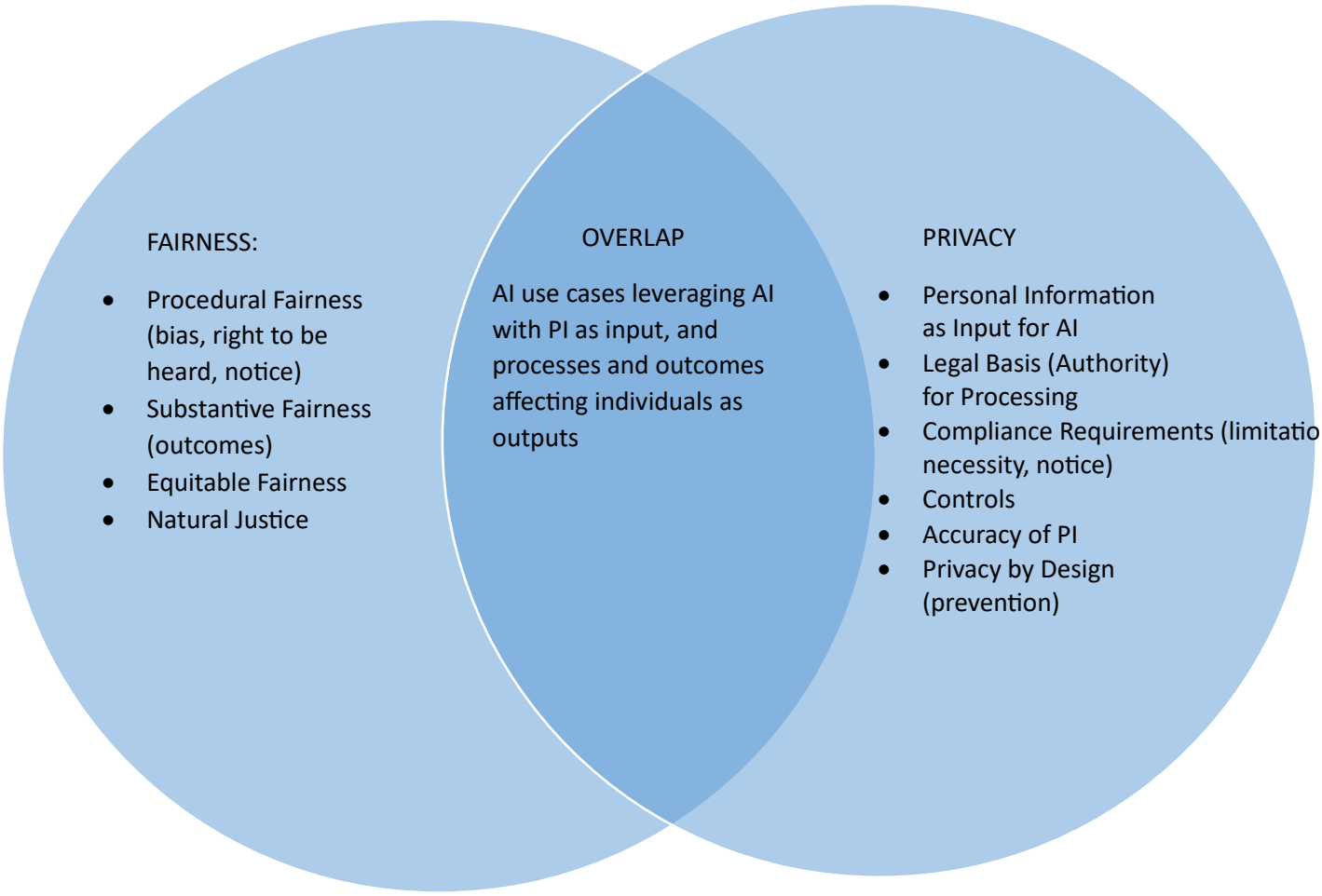
Specific to the public sector, either by legislation or policy, a duty of transparency regarding AI in use by public bodies should be considered to increase trust and ensure effective oversight. There are international examples for public sector AI use being registered in a publicly accessible database. The database includes algorithms (not just strictly AI) processing personal information, and algorithms used to support public decision-making, policy evaluation, etc. A public AI registry can help legislators, regulators, auditors, policy makers, citizens, journalists and researchers find information relevant to their interest or function, and promotes accountability and transparency in a tangible way.

23. Consider creating regulations or policy that requires public bodies to be transparent regarding their use of AI, by registering such uses in a publicly accessible and searchable AI registry.

[51] https://laws-lois.justice.gc.ca/eng/acts/C-46/section-162.1.html.
[52] https://kings-printer.alberta.ca/1266.cfm?page=P26p9.cfm&leg_type=Acts&isbncln=9780779797097.
[53] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/23011.

Administrative fairness and good governance

Given the tight overlap between AI's inputs, processing and outputs, evaluation of AI use in the public sector is best done with a multi-jurisdictional approach. Lawfulness can often best be determined when simultaneously evaluating privacy and fairness due to the inherent interrelatedness.



Furthermore, given the relative newness of AI in the public sector, any uses of AI should be held to high standards, meaning more care should be given to administrative fairness and good governance. This is challenging because the relative newness of the technology means that organizations dealing with AI are still developing tacit knowledge, institutional capacity, and heuristics specific to AI that these same public sector organizations can typically rely on when implementing new public policy, programs or projects. Before commencing the use of AI, the strategic decision how to use, or not use AI in specific areas should be weighed against the requirements of fairness and principles of good governance.

24. Both public sector privacy and AI-specific legislation would benefit from explicitly building fairness and good governance principles into these Acts[54].

6. Comprehensive model for responsible and safe use of AI in Alberta

Governance programs, guidance, and assessments can be used as a stop-gap measure to manage some of the risks stemming from AI in absence of AI-specific legislation. Such material must align with already established international principles and practices. Once legislation has been developed, such programs, guidance, and assessments should adopt, reflect and reference all specific requirements of that legislation. Below is a description of certain measures that should be adopted in the private, health, and public sectors in Alberta to protect the public from the potential harms of AI until a comprehensive legislative framework for the responsible development and use of AI is established in the province.

Private sector

Businesses should verify their PIPA compliance and implement best practice when considering the use of AI to process personal information. To do so, they should follow guidance already published jointly by federal, provincial and territorial privacy commissioners[55].

Below are other considerations to limit adverse impacts in the absence of comprehensive AI legislation.

- High risk uses should be limited, registered and/or made transparent. High risk uses could be derived from AIDA and the EU AI act, or established by a joint task force of industry, academic and regulatory experts. Regulations could be established to limit the uses of personal or health information to train AI, and require registration and/or transparency of AI systems, e.g., via PIPA, sections 55(5) and 55(1)(b), leveraging 'personal information codes'.
- The same code could be used to require organizations using AI to account for and monitor for breaches, bias, discrimination, and other harms. Due to the inherent limitations of self-regulation, this will not be a satisfactory solution in the long term, but it can be a path to ease the eventual inclusion of such requirements in an AI act.
- Collaboration between government, regulators, and industry representatives could be used to develop tools and guidance such as algorithmic impact assessments, codes of practice, etc. to help guide conduct in the absence of specific legislation.

[54] See https://arxiv.org/pdf/2501.12962 for a description of the provisions for, working of, and shortcomings of fairness in the EU AI Act.

[55] https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.

Health sector

- A similar approach as taken in the private sector could be taken to ensure stop-gap measures are in place to help guide the use of AI in the health sector, paying special attention to the higher sensitivity of health information over most personal information.
- Regulatory bodies and associations are already taking steps to ensure custodians are guided in preventing harm, and ensuring good conduct, when it comes to the use of AI[56].

Public sector

AI Governance program

The OIPC is aware that building blocks for AI governance (e.g., responsible AI framework, data ethics framework) are already developed or being developed for use in Government. AI governance could be reinforced with the inclusion of guidance, training and pre-implementation assessments specific to AI use. Furthermore, the public registry as referred to in Recommendation 23 would greatly contribute to the accountability and transparency aspects of Government's ambition to promote good governance in the development and use of AI in the province.

Guidance for public bodies

Guidance helps public bodies successfully adopt AI in accordance with legislative and policy requirements, while accounting for risks. It provides knowledge to staff leading or supporting such projects to adequately set up programs that leverage AI, from design and procurement, to monitoring and evaluation.

Initial AI Assessment

AI assessments can be used as a high level initial screening of AI projects to ensure they are in the public interest, and the project team is aware of any regulatory and policy requirements applicable. Assessments help with implementing the AI guidance for the project or program by providing checklists for the sequential steps in the implementation process. This includes ensuring that projects and programs meet legislative and policy requirements and include good governance principles, such as assessing administrative fairness, identifying and managing risks, and ensuring due process is followed. Assessments can also be used to prevent the commencement and waste of resources on projects or programs that would include prohibited activities and may be used to ensure approval and extended risk management of high risk projects.

Specific assessments where needed

The AI assessment will include preliminary checks that will help public bodies decide if additional due diligence is required by law, or otherwise appropriate. As such, processing of personal information will direct public bodies to conduct more fulsome assessments such as PIAs. Involvement of vital infrastructure may prompt them to conduct security threat risk assessments (STRAs). AI used in public decision-making should prompt a fairness assessment, etc.

[56] publications by the CSPA, AMA and CMPA on the specific topic of AI exist and set out policy, guidelines and expectations for members. The OIPC has issued guidance specific for small custodians considering the use of AI.

7. Engagement with the OIPC

The OIPC would be pleased to engage with Government and representatives from the health and private sector on the development of a legislative and policy framework to guide responsible and safe development and deployment of AI in the province.