

Check against delivery

**Keynote by Patricia Kosseim, Information and Privacy Commissioner of Ontario
Association of Native Child and Family Services Agencies of Ontario
Child and Family Well-Being Conference
December 5, 2024**

Insights on privacy and access from Ontario's IPC

Introduction

- Good morning, everyone.
- I'd like to thank the Association of Native Child and Family Services Agencies of Ontario for the opportunity to speak with you today.
- I am grateful to the Elders and the Indigenous Youth Advisory Council members joining us today. Your guidance is vital in supporting the well-being of children, youth, and their families.
- I would like to begin by acknowledging that as we gather here, we are meeting on the traditional territory of many nations including the Mississaugas of the Credit, the Anishnabeg, the Chippewa, the Haudenosaunee and the Wendat peoples and is now home to many diverse First Nations, Inuit and Métis peoples.
- I also acknowledge that Toronto is covered by Treaty 13 signed with the Mississaugas of the Credit, and the Williams Treaties signed with multiple Mississaugas and Chippewa bands.
- As Ontario's Information and Privacy Commissioner, I respectfully recognize and acknowledge the long-standing relationship that Indigenous peoples have with the land, and I am grateful to work with and live alongside the nations on this territory.
- I acknowledge my role in the collective responsibility to build a more just and inclusive society where the rights and dignity of Indigenous peoples are fully upheld.
- I am honoured to be here, celebrating with you the growth and impact the Association of Native Child and Family Services Agencies of Ontario has had over the past 30 years.
- Your impact has been recognized nationally, including your recent and well-deserved recognition at the inaugural PICCASO Awards Canada, where your

association was honoured with the Rising Star and Privacy Team of the Year awards.

- These privacy awards commend trailblazers in the data, privacy and information security community in Canada for their exemplary dedication and achievements.
- Furthermore, the awards celebrate rising talent in this field, inspiring them to strive for excellence and innovation in their careers.
- My office has had the pleasure of working with Micheal Miller, the association's Executive Director, who is also a member of the IPC's Strategic Advisory Council.
- Micheal brings a wealth of knowledge and advice to our council table when it comes to ensuring Indigenous perspectives are represented.
- The IPC is committed to continuing to collaborate with your association to explore opportunities and overcome challenges that lie ahead.
- Today, my presentation will reflect on the mandate of the IPC and its connection with principles of data sovereignty and self-determination, as well as the First Nations' OCAP principles.
- I'd also like to speak about the IPC's recent guidance on sharing information in situations involving intimate partner violence and your association's continued work on developing training and resources on this topic.
- As well, I'll provide an update on my office's work related to Part X of the *Child, Youth and Family Services Act*, or CYFSA, since its enactment.
- And I'll wrap up by sharing my perspectives on regulation of artificial intelligence, or AI, emphasizing the need for ethical frameworks and clear legal guardrails to ensure that AI technologies align with community values and protect privacy.

About the IPC

- Let me start off by telling you about the work that the IPC does. My office oversees compliance with five laws, including Part X of the [*Child, Youth and Family Services Act*](#).
- These laws establish rules for how Ontario's public institutions, health care providers, and child and family service providers, may collect, use, and disclose personal information and how they must keep such information secure.
- They also provide the public with a right of access to government-held information and access to their own personal information.

IPC Vision

- When I began my term as the Information and Privacy Commissioner of Ontario in 2020, I set a clear vision for the office to be a modern and effective regulator with real-world impact.
- That means we're committed to being proactive in our approach, modeling responsible behaviour, and ensuring that as we navigate our rapidly evolving digital world Ontarians can trust that their privacy and access rights will be respected.
- Our focus is on the outcomes of our work — securing privacy protection, transparency, fairness. A key part of our strategy involves building collaborative, consultative relationships with associations like yours.
- Our office's vision is rooted in three core principles:
 1. **Advocacy**: Actively advancing the privacy and access rights in key strategic areas that impact people's daily lives. These are:
 - Privacy and Transparency in a Modern Government
 - Children and Youth in a Digital World
 - Next-Generation Law Enforcement
 - Trust in Digital Health
 2. **Responsiveness**: Addressing complaints and appeals in a fair, timely, and meaningful manner.
 3. **Accountability**: Maintaining confidence in the organizational excellence and effectiveness of our office as a regulator.
- Foundational to our work is **our cross-cutting strategies**. We approach all our work through a laser-focus on being:
 - accessible and equitable
 - aspirational but pragmatic
 - consultative and collaborative, and
 - building capacity, both internally and externally
- Also, key to our work is our commitment to our core values: respect, integrity, fairness, collaboration and excellence.

Data sovereignty and self-determination

- Early in my mandate, I began a dialogue on data sovereignty and self-determination with Jonathan Dewar, CEO of the First Nations Information Governance Centre and Carmen Jones, Director of Research and Data Management, at the Chiefs of Ontario on our Info Matters podcast.

- We discussed the importance of respecting First Nations data sovereignty as part of the journey towards reconciliation. It's episode seven of our first season and it's available wherever you get your podcasts.
- That episode was subsequently used to facilitate further conversations at the 2022 International Association of Privacy Professionals' Canada Symposium, the 2023 Global Privacy Assembly, and the recent 2024 annual meeting of federal, provincial and territorial privacy commissioners hosted by my office in Toronto.
- As part of these discussions, my colleagues and I across Canada, and around the world, have heard that Indigenous peoples' concepts of privacy are often inherently collective.
- For many Indigenous peoples, the protection of personal data is just one part of a broader set of data privacy considerations and community values.
- This generally conflicts with Canadian privacy laws, where the primary focus is on individual concepts of privacy and access as opposed to collective, community data. Canadian privacy laws also do not typically acknowledge or address the issue of Indigenous data sovereignty.
- Sensitive to these gaps, my office and access and privacy authorities across Canada, are exploring ways collective and group notions of privacy and Indigenous data sovereignty can be respected and incorporated into our work.
- In this context, federal, provincial and territorial privacy commissioners and ombuds across Canada have been issuing calls to public bodies and institutions in our respective jurisdictions.
- In 2023, we issued a joint resolution on [Facilitating Access to Government Information](#) urging institutions and public bodies to recognize the unique barriers impacting Indigenous peoples and groups and actively work to advance reconciliation by respecting principles of data sovereignty and ensuring full and timely access to historical records.
- We are also committed to strengthening our understanding of the OCAP principles of ownership, control, access, and possession, and have made the First Nations Information Governance Centre's training course mandatory for IPC staff.
- My office is prepared to listen and continue to explore how data sovereignty and self-determination can be respected in the context of the IPC's work.

Intimate partner violence guidance

- Intimate partner violence, or IPV, has become a top concern in communities across the country. In May 2024, my office developed guidance for [Sharing Information in Situations Involving Intimate Partner Violence](#).
- The guidance was developed in response to an inquest by the Office of the Chief Coroner for Ontario into the tragic deaths of three women at the hands of their former partner.
- The inquest jury called on the IPC to develop plain language guidance to explain Ontario's privacy laws and empower IPV professionals to make informed decisions about privacy, confidentiality, and public safety, particularly around assessing and reducing IPV risk.
- As we know, responding to IPV is all about taking appropriate action at the right time to protect individuals and their families from the possibility of serious injury or death.
- While a best practice for sharing personal information is to get individual consent, we recognize that this may not always be possible or even advisable.
- Under Ontario's privacy laws, organizations, service providers, and their staff are permitted to share personal information about an individual when there is reason to believe there is a risk of serious harm to an individual's health or safety.
- If a decision about whether to share personal information is made after carefully assessing all available information and the relevant factors, it will generally be considered reasonable and made in good faith under Ontario's privacy laws. You can check out the guidance on our website for more information.
- I'd like to thank your association and its members for providing feedback on the guidance during the development phase. It's important for all of us to recognize that privacy is not, and should not, be a barrier to safety.
- The Association of Native Child and Family Services Agencies of Ontario has been an important contributor to this understanding, and we appreciate your continued work on developing further training materials and guidance on this important issue.
- Based on the feedback of your members, our guidance acknowledges that it is important to understand Indigenous governance and sovereignty rights of First Nations, Inuit, and Métis individuals to respect and uphold their data and privacy rights.
- The design and delivery of IPV prevention programs should also carefully consider the intersectional identities of the individuals they serve. Programs

should include a trauma and violence-informed approach that acknowledges historical, cultural, and internal biases.

- This approach can help prevent further victimization of individuals.
- We took our learnings in developing this IPC guidance to our FPT colleagues and asked them to join us in championing this issue across the country.
- This resulted in a joint national resolution on information sharing in situations involving intimate partner violence, released just last week. Our joint resolution calls on public, private, health, and social services sector organizations to consider the unique experiences of First Nations, Inuit, and Métis individuals and communities and work to advance reconciliation, by respecting Indigenous principles of data sovereignty.

Part X of the CYFSA

- As I mentioned earlier, my office oversees Ontario's access and privacy laws, including Part X of the CYFSA.
- Enacted in 2020, Part X sets out rules on privacy and access to personal information intended for service providers, including Indigenous child and family well-being agencies.
- Although we are almost five years in, Part X is still a relatively new piece of privacy legislation.
- My office continues to learn about the child and family service sector, including the way Indigenous child and family well-being services are delivered.
- We take the position that all children and youth who receive services under the CYFSA are inherently vulnerable.
- Many belong to marginalized and disadvantaged populations, which places them and their families at greater risk of inequitable outcomes during service delivery.

IPC Submission to MCCSS

- For these reasons, it is essential that service providers and the Ministry of Children, Community and Social Services are accountable and transparent with respect to the collection, use, and disclosure of personal information.

- In July 2023, the IPC provided comments and recommendations to the Ministry, as part of the first Five-Year legislative review of the CYFSA.
- Our comments and recommendations are consistent with our previous submissions to the ministry — our focus remains on strengthening the access and privacy protections under the law and its regulations.
- In alignment with your association’s submission as part of the five-year review, my office is calling for amendments to Part X to make the ministry more accountable when collecting, using, and disclosing the sensitive personal information of vulnerable individuals.
- My office has issued 19 CYFSA decisions to date. These are available in a searchable database on the IPC’s website.
- These decisions have been primarily related to:
 - examining an individual’s right of access, including whether the record is dedicated primarily to the provision of a service,
 - the application of several exemptions from the right of access
 - the exclusion of adoption records from the scope of Part X,
 - a service provider’s duty to correct a record, and
 - the right of access to a deceased person’s personal information.
- As our knowledge continues to develop, I would encourage all agencies providing services under Part X to review the decisions from my office. They provide practical real-world guidance on Part X.
- As First Nations continue to assert and exercise jurisdiction of child and family services, supported by the federal legislation, we are watching these developments closely.
- My office has been examining how the federal Act respecting First Nations, Inuit and Métis children, youth and families intersects with my office’s oversight role under Part X of the CYFSA. This includes consideration of the recent Supreme Court decision affirming Indigenous communities inherent right of self-government, which we will of course respect and defer to.

The Future of AI

- As we know, artificial intelligence is in the headlines almost every day and it’s very much top of mind for us at the IPC.

- When it comes to the future of AI, I recently had a chance to speak with [Jeff Ward](#), CEO of Animikii, a values-driven Indigenous technology company based in B.C.
- We discussed the longstanding connection between technology and culture, and how incorporating Indigenous values and principles into the development of new technologies can empower communities.
- Jeff is a member of the [Global Partnership on Artificial Intelligence](#) working group on responsible AI, which is grounded in a vision of AI that is human-centred, fair, equitable, inclusive and respects human rights.
- He also spoke about a project his company is working on with the Six Nations Survivors' Secretariat. The secretariat was established to organize and support efforts to uncover, document, and share the truth about what happened at the Mohawk Institute residential school during its more than 140 years of operation.
- This project involves massive amounts of data about survivors, their families, and their communities. And this data is in many different systems — from provincial and federal governments, within churches, the RCMP, and others.
- They are looking at ways of integrating the data through technology, in ways that can benefit the community as a whole. It's a powerful real-life example of community data interests at work versus the traditional thinking about privacy rights as individually based.
- We also talked about the OCAP principles, and other data frameworks that exist such as the FAIR principles — findable, accessible, interoperable, and reusable.
- And he told me about the CARE principles for Indigenous data governance, which stands for collective benefit, authority to control, responsibility, and ethics. It's not only about respecting collective data, but also the data of individuals and from non-human entities like the land and waters.
- It was an insightful conversation that focused on ensuring that the use of AI technologies align with a communities' values and rights.
- You can listen to it on our website, or on Apple podcasts, Spotify, or wherever you download your podcasts.

Risks and benefits of AI

- While AI holds a lot of potential to improve life in our communities, we must also be mindful of the risks to our privacy and human rights.
- For example, a recent article discussed that AI generated art is causing a [significant threat](#) to Indigenous peoples' income, art and cultural knowledge.
- Art is central to Indigenous cultures, ceremonies, and identity. Using AI tools anyone can “create” Indigenous art, misappropriating the styles of real artists.
- Moreover, AI can replicate and amplify real-world bias and discrimination based on historical datasets that algorithms are trained on.
- So, if datasets are biased from the very beginning, outputs from these technologies will reinforce that bias, only exacerbating the problem.
- This can lead to individuals from vulnerable and marginalized communities being unfairly treated or negatively targeted by flawed AI applications.
- For example, in one recent study, researchers found that depending on the dialect used for input into their AI model, the results could lead to prejudicial assumptions about people's character, employability, and criminal tendencies.
- When we think about the application of AI in the public sector, for example in the delivery of government services, the need for strong AI governance to prevent these kinds of things from happening is clear.
- Children are particularly at high risk of the negative impacts of AI technologies, as they are less able to identify or challenge biased or inaccurate information.
- Young people are also generally less able to understand and appreciate the long-term implications of the data they share, which is why they need even stronger privacy safeguards.
- Children should be able to benefit from technology safely and free from fear that they may be targeted, manipulated, or harmed.
- My office is very interested learning more from the experiences of children, youth and their families regarding the impact of AI technologies, especially in Indigenous communities.

IPC advocacy for responsible AI

- Part of good governance involves having clear and enforceable AI principles to uphold and protect our fundamental human rights.

- Over the past few years, my office has strongly advocated for clear, coherent, and effective AI principles that are enshrined in law.
- Last year, the IPC issued a [joint statement](#) with the Ontario Human Rights Commission, which is available on our website.
- We urged the provincial government to develop and implement effective guardrails for the use of AI technology in the public sector, addressing safety, privacy, accountability, transparency, and human rights.
- These guardrails are essential for Ontario to fully derive the benefits of AI technologies in a way that is ethically responsible, accountable, sustainable, and supported by public trust

Bill 194

- Last week, the Ontario government passed Bill 194, the [Strengthening Cyber Security and Building Trust in the Public Sector Act](#).
- This new law creates conditions to regulate the use of AI by public sector entities, amongst other things.
- It applies to provincial and municipal public institutions, as well as institutions that handle children's data such as school boards, children's aid societies, and Indigenous child and family well-being agencies.
- Bill 194 sets out regulation-making authority with respect to transparency, accountability, risk management, technical standards and oversight, as well as certain prohibited uses.
- While these are important steps, there is room for improvement and the IPC filed a submission with the legislative assembly with our recommendations. It's available on our website.
- 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. And in our view, these should be enshrined in statute.
- 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 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 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.
- 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.
- We were not alone in calling for guardrails to be enshrined in the law. The Ontario Human Rights Commission, the Law Commission of Ontario, the Ontario Bar Association, and leading academics in the area of privacy law raised similar issues.
- Our recommendations were also aligned with your association's submission to government on Bill 194 as well.
- For example, we both acknowledged that there is a need to address digital technologies aimed at children, which will also be the subject of future ministerial regulation.
- We agree that a better approach would have been to strengthen provisions within existing legislation to avoid duplication.
- Both the IPC and your association strongly advocated for consistent legal and regulatory requirements related to digital technologies used in schools, children's aid societies, and Indigenous child and family well-being agencies.
- Having a strong and consistent regulatory framework in place can help to remove some of the ambiguity around these tools and help ensure they are used safely and ethically.
- Unfortunately, our recommended amendments were not made to Bill 194. However, as the government moves forward with subsequent regulations, we will be advocating for a harmonized approach with other national and international regulatory regimes.

Closing

- In closing, I would like to thank you again for the great honor to speak at this today's meeting and I look forward to continuing our work together.
- Our office is always open to consultations, and we encourage you to reach out.
- Working together, we can make progress towards our shared goal which is to continue to support the well-being of children, youth, and their families.
- Thank you.