Generative Artificial Intelligence

Education Sector

Javier Ruiz-Soler

Senior Technology and Policy Advisor

AERO-AOCE

November 1, 2024

Information and Privacy Commissioner of Ontario

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

BIO

Javier Ruiz-Soler, PhD

Senior Technology and Policy Advisor

My work consists in identifying and analyzing trends in technology (information security governance, privacy enhancing technologies, artificial intelligence technologies, data access issues, and governance) and contributing to developing the IPC's policy capacity on Emerging Technologies.

I hold a PhD in Political Science and Technology.

Agenda

- IPC Mandate
- Brief History of AI
- Generative AI
- Educational AI Governance
- Ontario AI landscape
  - Principles with OPC and other Privacy Offices in Canada
  - Bill 194
- Resources
  - OECD Principles
  - Guidelines use of Gen. AI
  - IPC Procurement Guide
  - IPC Digital Charter for Ontario Schools
  - Consulting

IPC Mandate

Information and Privacy Commissioner of Ontario

Patricia Kosseim

- Ontario's Information and Privacy Commissioner is an officer of the legislature
  - Appointed by and reports to the Legislative Assembly of Ontario
  - Independent of the government of the day
- The IPC has authority under the following laws:
  - *Freedom of Information and Protection of Privacy Act* (FIPPA)
  - *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
  - *Personal Health Information Protection Act, 2004* (PHIPA)
  - *Child, Youth and Family Services Act, 2017* (CYFSA)
  - *Anti-Racism Act, 2017* (ARA)
  - *Coroners Act*

IPC's Overall Role & Mandate

In addition to overseeing provincial access and privacy laws, the office of the IPC also serves the government, public institutions and the public through its mandate to:

- Resolve appeals when access to information is refused
- Investigate privacy complaints related to personal information
- Ensure compliance with the province's access and privacy laws
- Review privacy policies and information management practices
- Conduct research on access and privacy issues and provide comment on proposed legislation and government programs
- Educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

IPC'S VISION

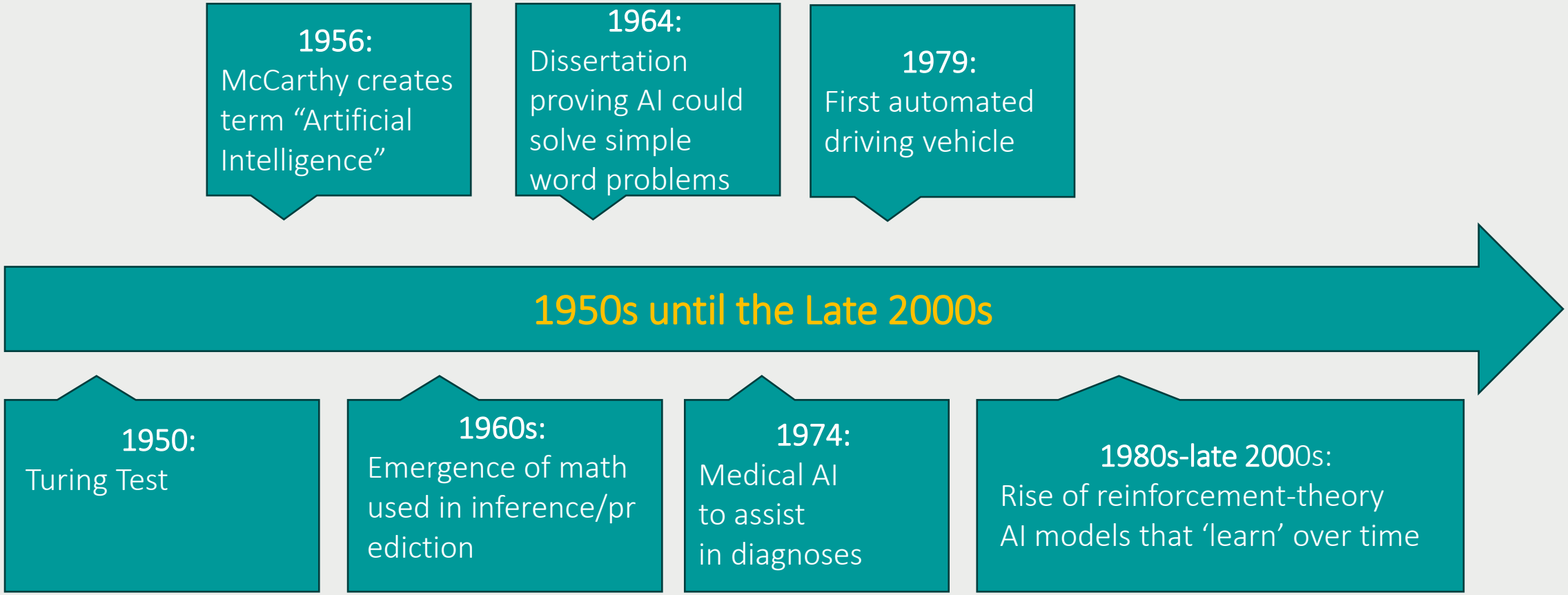
Enhance Ontarians' trust that their access and privacy rights will be respected by ...

IPC

- Strategic Priorities
- IPC Technology Team
  - AI
  - Cybersecurity
  - Tech Expertise

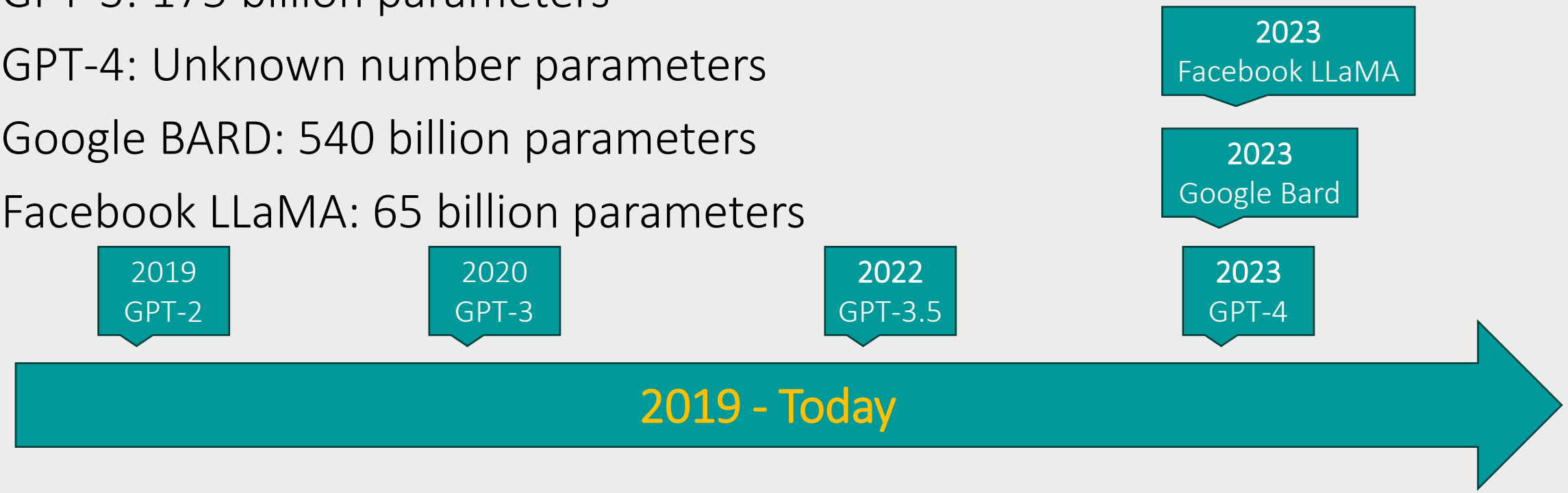
Brief History of AI

AI Then: The First 50 Years



AI Now: The Current Inflection Point

- GPT-2: 1.5 billion parameters
- GPT-3: 175 billion parameters
- GPT-4: Unknown number parameters
- Google BARD: 540 billion parameters
- Facebook LLaMA: 65 billion parameters

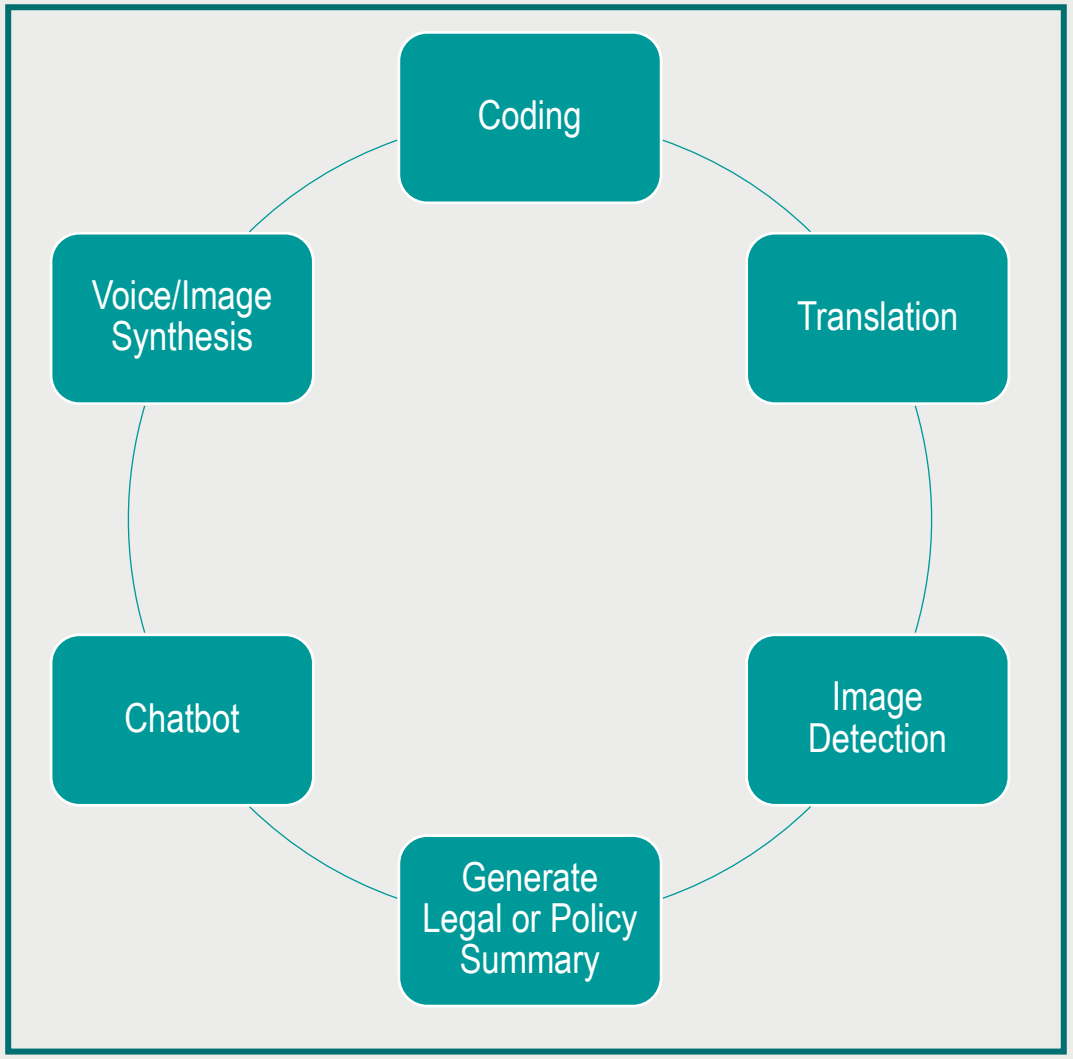


What AI Technologies “Know”

- “Toronto is the provincial capital of Ontario”
- Contemporary large language models and appearance of meaning




Contemporary Use Cases



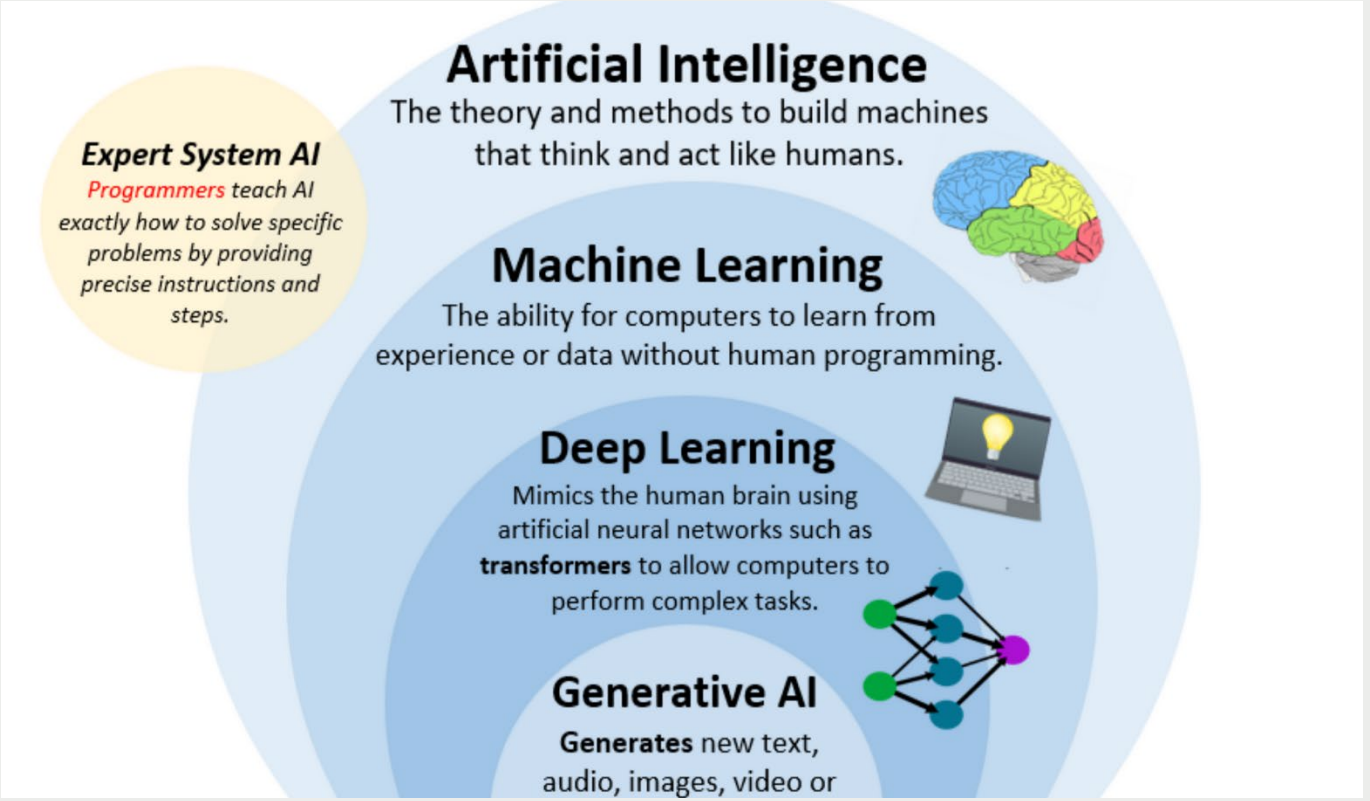
- Bias, Equity, and Discrimination
- Pressing Challenges
- Exacerbating Policy Challenges
- Practical Deployment Question

Pressing Challenges

1. Training Data: De-biased? Sourced legally?
2. Large Language Model Memories: Emits intimate images?
3. Model Update Costs: Expensive to fix
4. Variable Outputs: Inconsistent generative responses
5. Class Breaks: Break once, break everywhere
6. Attack Surfaces: Experts unsure how to secure

Generative AI

Generative AI



Definition: AI models that create new content, such as text, images, or music, based on the data they are trained or
Examples: ChatGPT, DALL-E, Midjourney.
Purpose: Enable new forms of interaction, enhance creativity, and personalize educational content.

Generative AI in Education: Why Now?

AI Advancements: Rapid improvements in AI capabilities, accessibility, and affordability.
Student Engagement: Opportunities to make learning more interactive and relevant.
Skills for the Future: Preparing students for AI-integrated workplaces.

Applications of Generative AI in Education

1. Personalized Tutoring: Adaptive learning experiences tailored to individual student needs.
2. Automated Assessment: AI-assisted grading and feedback on written assignments and exams.
3. Content Creation: Generating educational content such as quizzes, lesson plans, and multimedia resources.
4. Language Support: AI-powered language translation and learning aids.
5. Creative Inspiration: Tools for art, music, and literature classes to stimulate creativity.

Benefits of Generative AI in Education

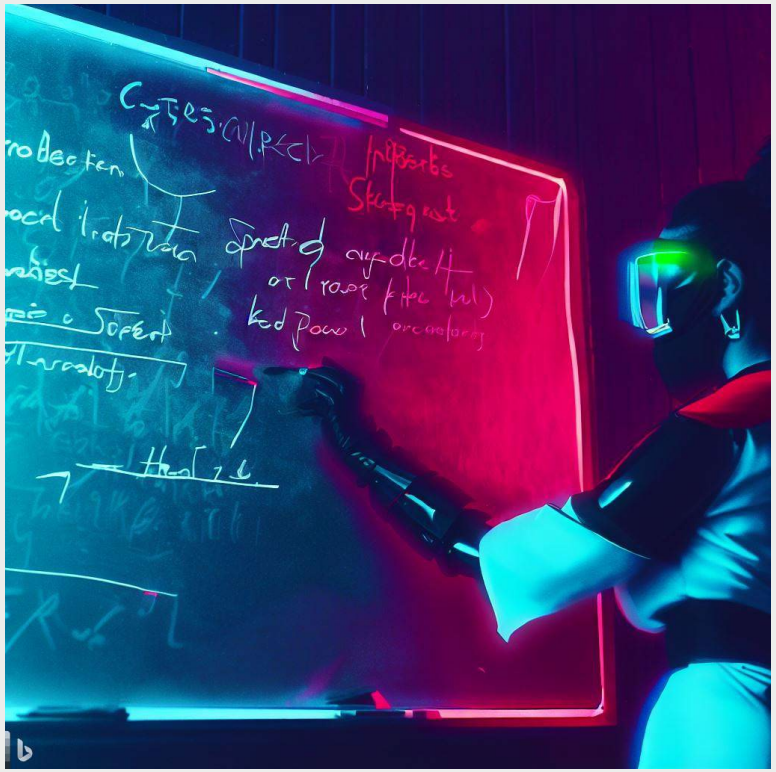
Personalization: Tailored learning experiences for each student's pace and style.
Scalability: Supports large numbers of students with automated resources.
Accessibility: Offers multilingual support and accommodates diverse learning needs.
Efficiency: Reduces teachers' workload, allowing more time for direct student interaction.

Challenges and Considerations

Ethical Concerns: Privacy, data security, and consent for AI usage.
Academic Integrity: Managing risks of plagiarism and over-reliance on AI tools.
Bias and Fairness: Avoiding biases that could perpetuate educational inequality.
Teacher Training: Ensuring educators are equipped to integrate AI effectively.

Role of Teachers and Educators

Facilitators of AI Use: Guide students in responsible and ethical AI usage.
Adaptation and Training: Developing new skills to complement AI capabilities.
Critical Thinking Encouragement: Helping students question and validate AI-generated content.



Future of Generative AI in Education

Lifelong Learning Pathways: Personalized curriculum support from early education to higher ed.
Enhanced Collaboration: AI for student collaboration, knowledge sharing, and project-based learning.
AI as a Learning Partner: Vision for generative AI as an integrated educational tool assisting across subjects.

Educational AI Governance

Educational Tools AI Governance

- Students go out: use of AI for academic work with integrity questions, risks, etc. Need for Risk management.
- Institutional tools: purchased or free for education. Vendor might process PI.
- Referral tool: teacher says “go find AI tool for this assignment”.

Privacy Impact Assessment: is a tool for organizations to manage risk. Identify, assess and mitigate privacy risks.

Most schools conduct PIA when adopting new technology.

If teacher (institutional agent) uses ChatGPT for work, which is to develop business, in this case educational business. That becomes an institutional tool. Without proper program or deployment, it might cause risks (for example typing PI, etc.). *Similar to the concept of shadow IT risk.*

Ontario AI Landscape

State of Art in the Province

Cont'd

Principles with OPC and other Privacy Offices

- Considerations for the application of key privacy principles to generative AI technologies
  - Legal Authority
  - Appropriate Purpose
  - Necessity and Proportionality
  - Openness
  - Accountability
  - Individual Access
  - Limiting collection, Use and disclosure
  - Accuracy
  - Safeguards

Link: Principles for responsible, trustworthy and privacy-protective generative AI technologies - Office of the Privacy Commissioner of Canada

Cont'd

Bill 194

- Ontario government introduced Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, aimed at strengthening digital infrastructure and data privacy protections within public entities and services in Ontario
  - Require public sector entities to develop and implement cyber security programs, and submit reports on cyber security.
  - Regulate how public sector entities, identified by regulation, use artificial intelligence ("AI") systems.
  - Allow the government to make regulations on how children's aid societies and school boards collect, use, retain or disclose digital information relating to individuals under age 18.

Cont'd

Bill 194 and AI

- Provide information to the public about their use of the AI system;
- Develop and implement an accountability framework respecting their use of the AI system (which may require roles and responsibilities for specified individuals);
- Take steps to manage risks associated with the use of the AI system (which may include reporting and record-keeping);
- Use (or not use) the AI system in accordance with any prescribed requirements;
- Disclose information about the technical use of the AI system; and
- Ensure that an individual exercises oversight of the use of the AI system and what additional information that individual must make available (which may include publishing how inquiries may be made about the entity's use of such systems).

Resources

Cont'd

Resources

- Risk Assessment: AI Risk Management Framework | NIST
- Government of Canada Algorithmic Impact Assessment tool: Algorithmic Impact Assessment tool - Canada.ca
- OECD Responsible AI: AI principles | OECD
- Guidelines use of Gen. AI: Principles for responsible, trustworthy and privacy-protective generative AI technologies - Office of the Privacy Commissioner of Canada
- IPC Procurement Guide: https://www.ipc.on.ca/en/resources/privacy-and-access-public-sector-contracting-third-party-service-providers
- Digital Privacy Charter for Ontario Schools: Digital Privacy Charter for Ontario Schools | Information and Privacy Commissioner of Ontario (ipc.on.ca)
- IPC Consultations: Policy consultations | Information and Privacy Commissioner of Ontario (ipc.on.ca)

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965