AI in Ontario's Health Sector
Discussion with AMS-Fitzgerald Fellows

Nicole Minutti

Senior Health Policy Advisor

Information and Privacy Commissioner of Ontario

Information and Privacy
Commissioner of Ontario

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

AMS-Fitzgerald
Fellowship on AI

Apr 2, 2025

Agenda

- The Office of the Information and Privacy Commissioner of Ontario
- Update on Bill 194
- The Shifting Regulatory and Governance Landscape for AI
- Fundamental Principles for the Responsible Development and Use of AI
- AI Scribes in Ontario’s Health Sector: Guidance for Procurement, Implementation, and Use
- Discussion and Questions for the Fellows

The Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

Patricia Kosseim

- Ontario's Information and Privacy Commissioner (IPC) 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 Role in the Health Sector

Health Policy

- Consult with government regarding proposed health-related legislation and regulation
- Provide guidance for the health sector and public
- Participate in speaking engagements and provide presentations
- Conduct three-year reviews of prescribed entities, persons, and organizations
- Participate in consultations with health sector organizations including selected review and comment on health sector organization policies
- Conduct research on access and privacy issues relevant to the health sector
- Consult with Ontario Health regarding interoperability standards

Tribunal

- Investigate privacy complaints under PHIPA
- Resolve access to information/correction appeals
- Issue access and privacy decisions
- Receive/investigate point-in-time privacy breach reports

Communications

- Respond to questions from the public regarding PHIPA through info@ipc.on.ca
- Provide information to the public, including on our website https://www.ipc.on.ca/en
- Receive annual statistical reporting of breaches and prepare annual reports

Update on Bill 194: *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*

Bill 194

- On November 25, 2024, Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* received Royal Assent.
- Bill 194 aimed at strengthening digital infrastructure and data privacy protections within public entities and services in Ontario.
- In addition to making amendments to FIPPA, Bill 194 created a new law, the *Enhancing Digital Security and Trust Act, 2024* (EDSTA) that includes provisions related to:
  - The development and implementation of cyber security programs and reports that are to be submitted to the Minister of Public and Business Service Delivery on cyber security.
  - How public sector entities use AI systems.
  - How children’s aid societies and school boards collect, use, retain or disclose digital information relating to individuals under age 18.
- The EDSTA and some of the amendments to FIPPA came into force on Jan 29, 2025.
- Other amendments to FIPPA will come into force on July 1, 2025.

IPC’s Submission on Bill 194

> *“The legislation, as drafted, would establish significant regulation-making powers in respect of cyber security, AI systems, and digital technologies affecting individuals under the age of 18.*
>
> *The IPC agrees that these areas of societal activity pose high risk to Ontarians’ privacy and human rights and require urgent government intervention.*
>
> *However, as currently worded, Schedule 1 of Bill 194 lacks the statutory protections needed to protect privacy and human rights and fails to provide the level of transparency and accountability that are necessary to secure Ontarians’ trust in how the government will effectively govern these high-risk areas.”*

https://www.ipc.on.ca/en/resources/ipc-comments-bill-194-strengthening-cyber-security-and-building-trust-public-sector-act

IPC’s Recommendations on the AI portion of the EDSTA

- Codify fundamental AI principles and guardrails into the statute.
- Adopt a risk-based regulatory approach for AI.
- Specify no-go zones.

Bill 194: Ontario’s Missed Opportunity to Lead on AI

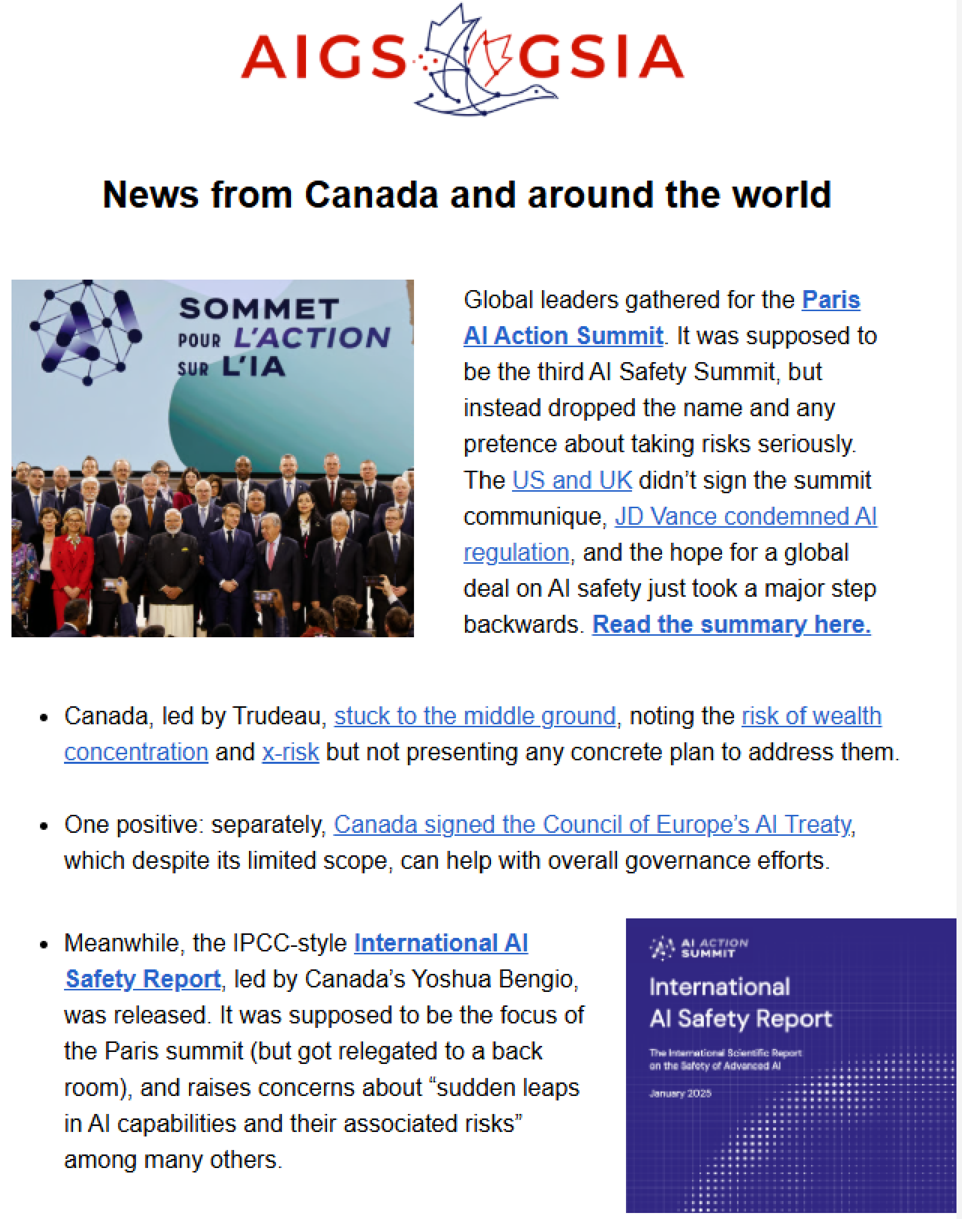
> *“AI is already transforming public services in Ontario, shaping decisions in health care, education, and social services. Done right, AI can enhance efficiency and improve outcomes. Done wrong, it can cause serious harms and have discriminatory impacts.*
> *Bill 194 was Ontario's chance to set clear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

https://www.ipc.on.ca/en/media-centre/blog/bill-194-ontarios-missed-opportunity-lead-ai

Shifting Regulatory and Governance Landscape for AI

Paris AI Action Summit

Feb 2025



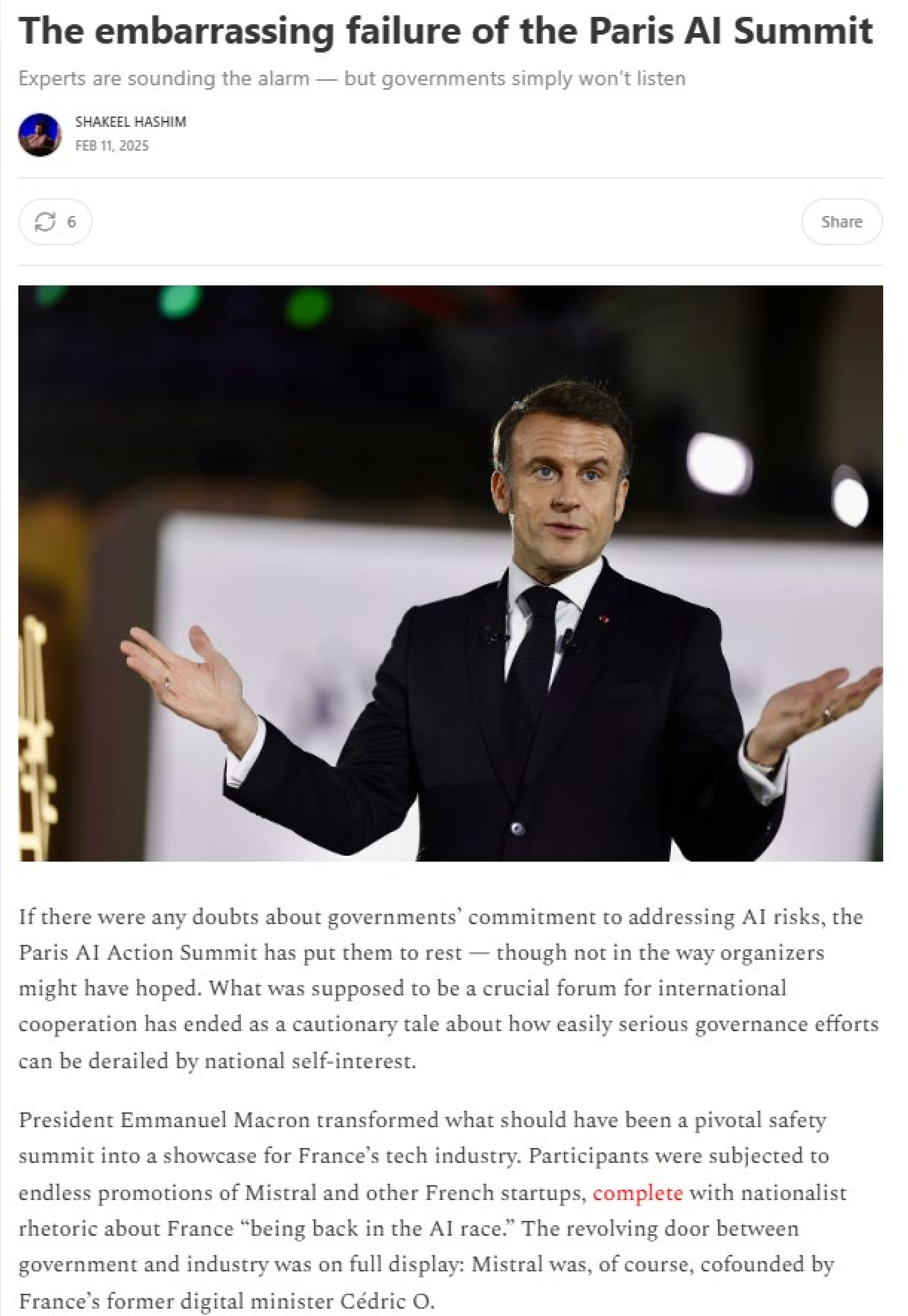
News from Canada and around the world

Global leaders gathered for the **Paris AI Action Summit**. It was supposed to be the third AI Safety Summit, but instead dropped the name and any pretence about taking risks seriously. The US and UK didn't sign the summit communique, JD Vance condemned AI regulation, and the hope for a global deal on AI safety just took a major step backwards. **Read the summary here.**

- Canada, led by Trudeau, stuck to the middle ground, noting the risk of wealth concentration and x-risk but not presenting any concrete plan to address them.
- One positive: separately, Canada signed the Council of Europe's AI Treaty, which despite its limited scope, can help with overall governance efforts.
- Meanwhile, the IPCC-style **International AI Safety Report**, led by Canada's Yoshua Bengio, was released. It was supposed to be the focus of the Paris summit (but got relegated to a back room), and raises concerns about "sudden leaps in AI capabilities and their associated risks" among many others.

AI ACTION SUMMIT
International AI Safety Report
The International Scientific Report on the Safety of Advanced AI
January 2025

https://aigs.ca/ newsletter Feb 28, 2025



The embarrassing failure of the Paris AI Summit

Experts are sounding the alarm — but governments simply won't listen

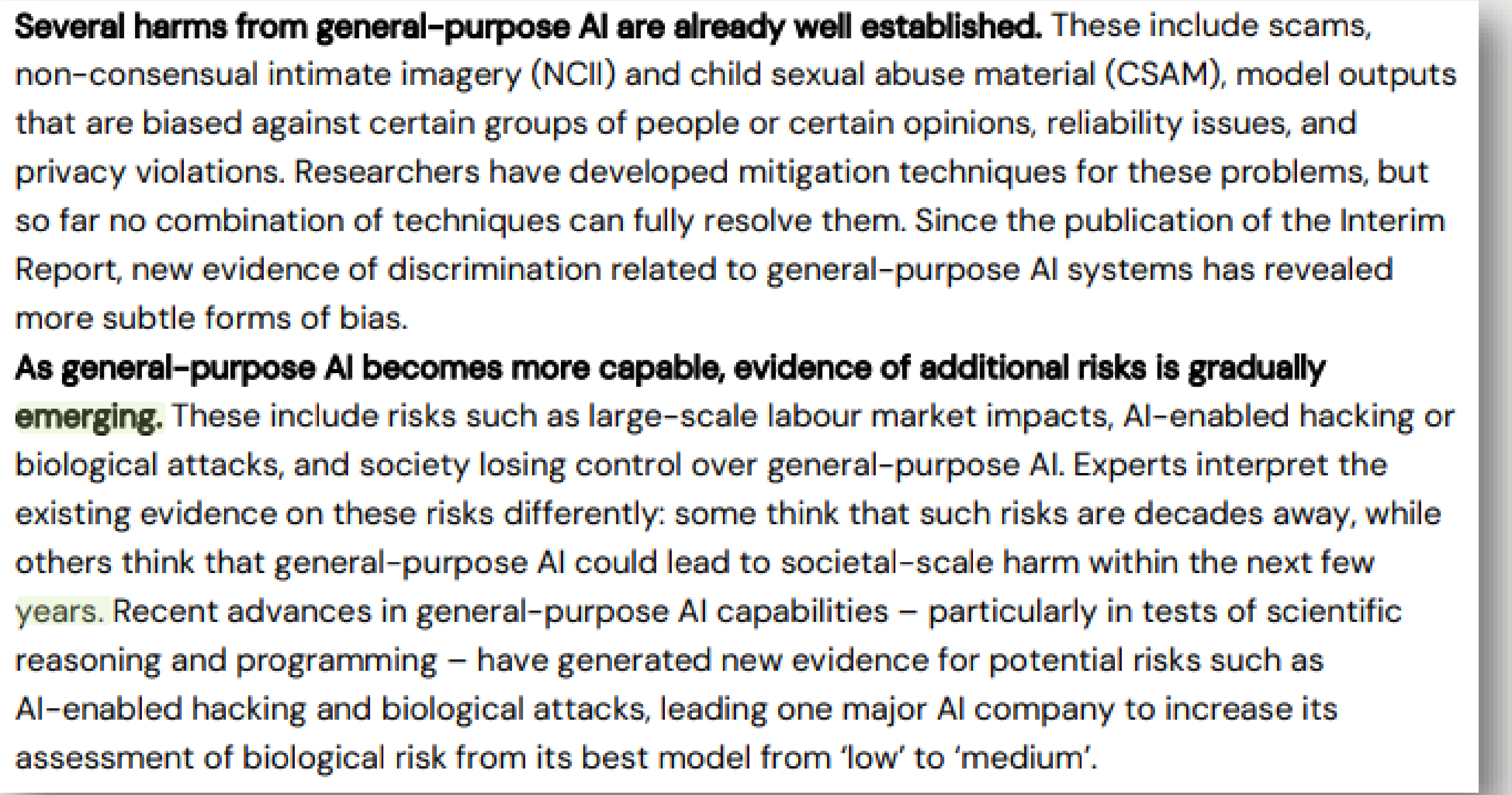
SHAKEEL HASHIM
FEB 11, 2025

If there were any doubts about governments' commitment to addressing AI risks, the Paris AI Action Summit has put them to rest — though not in the way organizers might have hoped. What was supposed to be a crucial forum for international cooperation has ended as a cautionary tale about how easily serious governance efforts can be derailed by national self-interest.

President Emmanuel Macron transformed what should have been a pivotal safety summit into a showcase for France's tech industry. Participants were subjected to endless promotions of Mistral and other French startups, complete with nationalist rhetoric about France "being back in the AI race." The revolving door between government and industry was on full display: Mistral was, of course, cofounded by France's former digital minister Cédric O.

https://www.transformernews.ai/p/paris-ai-summit-failure

International AI Safety Report (Jan 2025): Some Key Findings



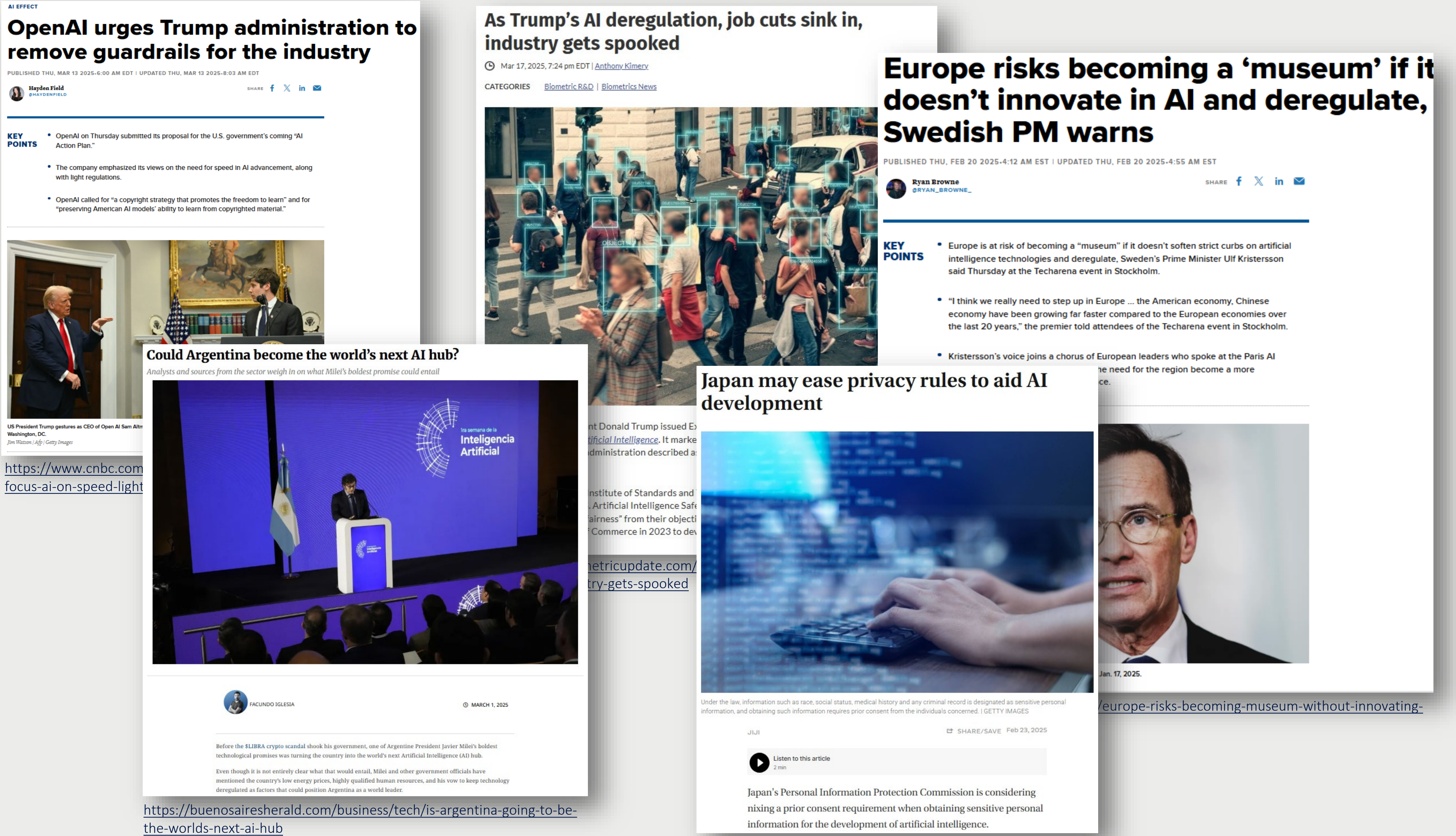
Several harms from general-purpose AI are already well established. These include scams, non-consensual intimate imagery (NCII) and child sexual abuse material (CSAM), model outputs that are biased against certain groups of people or certain opinions, reliability issues, and privacy violations. Researchers have developed mitigation techniques for these problems, but so far no combination of techniques can fully resolve them. Since the publication of the Interim Report, new evidence of discrimination related to general-purpose AI systems has revealed more subtle forms of bias.

As general-purpose AI becomes more capable, evidence of additional risks is gradually emerging. These include risks such as large-scale labour market impacts, AI-enabled hacking or biological attacks, and society losing control over general-purpose AI. Experts interpret the existing evidence on these risks differently: some think that such risks are decades away, while others think that general-purpose AI could lead to societal-scale harm within the next few years. Recent advances in general-purpose AI capabilities – particularly in tests of scientific reasoning and programming – have generated new evidence for potential risks such as AI-enabled hacking and biological attacks, leading one major AI company to increase its assessment of biological risk from its best model from 'low' to 'medium'.

https://assets.publishing.service.gov.uk/media/679a0c48a77d250007d313ee/International_AI_Safety_Report_2025_accessible_f.pdf

The Shifting Regulatory and Governance Landscape

The Economist
Why the AI crash is good news
A federal-spending freak-out
Could Trump and Xi divide up the world?
How covid boosted America's murder rate
FEBRUARY 1ST–7TH 2025
The revolt against regulation



AI EFFECT

OpenAI urges Trump administration to remove guardrails for the industry

PUBLISHED THU, MAR 13 2025-6:00 AM EDT | UPDATED THU, MAR 13 2025-8:03 AM EDT

Hayden Field
@HAYDENFIELD

SHARE

KEY POINTS

- OpenAI on Thursday submitted its proposal for the U.S. government's coming "AI Action Plan."
- The company emphasized its views on the need for speed in AI advancement, along with light regulations.
- OpenAI called for "a copyright strategy that promotes the freedom to learn" and for "preserving American AI models' ability to learn from copyrighted material."

US President Trump gestures as CEO of Open AI Sam Altm
Washington, DC.
Jim Watson | Afp | Getty Images

https://www.cnbc.com
focus-ai-on-speed-light

As Trump's AI deregulation, job cuts sink in, industry gets spooked

Mar 17, 2025, 7:24 pm EDT | Anthony Kimery

CATEGORIES Biometric R&D | Biometrics News

nt Donald Trump issued Ex
tificial Intelligence. It marke
dministration described a

Institute of Standards and
. Artificial Intelligence Safe
fairness" from their objecti
Commerce in 2023 to dev

netricupdate.com/
try-gets-spooked

Europe risks becoming a 'museum' if it doesn't innovate in AI and deregulate, Swedish PM warns

PUBLISHED THU, FEB 20 2025-4:12 AM EST | UPDATED THU, FEB 20 2025-4:55 AM EST

Ryan Browne
@RYAN_BROWNE_

SHARE

KEY POINTS

- Europe is at risk of becoming a "museum" if it doesn't soften strict curbs on artificial intelligence technologies and deregulate, Sweden's Prime Minister Ulf Kristersson said Thursday at the Techarena event in Stockholm.
- "I think we really need to step up in Europe ... the American economy, Chinese economy have been growing far faster compared to the European economies over the last 20 years," the premier told attendees of the Techarena event in Stockholm.
- Kristersson's voice joins a chorus of European leaders who spoke at the Paris AI
he need for the region become a more
ce.

Jan. 17, 2025.

/europe-risks-becoming-museum-without-innovating-

Could Argentina become the world's next AI hub?

Analysts and sources from the sector weigh in on what Milei's boldest promise could entail

FACUNDO IGLESIA

MARCH 1, 2025

Before the $LIBRA crypto scandal shook his government, one of Argentine President Javier Milei's boldest technological promises was turning the country into the world's next Artificial Intelligence (AI) hub.

Even though it is not entirely clear what that would entail, Milei and other government officials have mentioned the country's low energy prices, highly qualified human resources, and his vow to keep technology deregulated as factors that could position Argentina as a world leader.

https://buenosairesherald.com/business/tech/is-argentina-going-to-be-the-worlds-next-ai-hub

Japan may ease privacy rules to aid AI development

Under the law, information such as race, social status, medical history and any criminal record is designated as sensitive personal information, and obtaining such information requires prior consent from the individuals concerned. | GETTY IMAGES

JIJI

SHARE/SAVE Feb 23, 2025

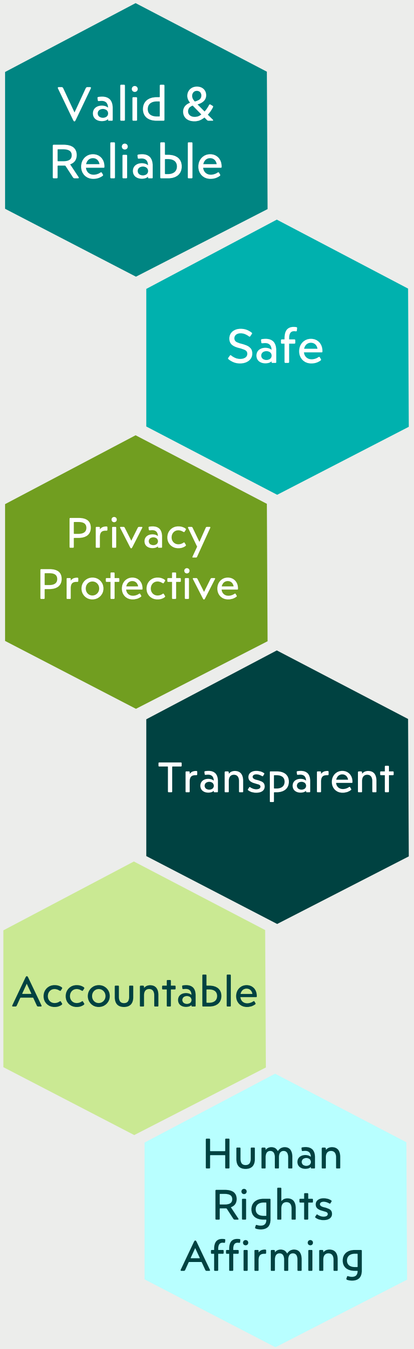
Listen to this article
2 min

Japan's Personal Information Protection Commission is considering nixing a prior consent requirement when obtaining sensitive personal information for the development of artificial intelligence.

https://www.japantimes.co.jp/news/2025/02/23/japan/crime-legal/personal-info-law-revision-ai/

Fundamental Principles for the Responsible Development and Use of AI

Fundamental Principles for the Responsible Development and Use of AI



Valid & Reliable

Safe

Privacy Protective

Transparent

Accountable

Human Rights Affirming

From the IPC’s submission on Bill 194

- There are many sets of principles related to AI that have been developed worldwide - across these we can see universal principles emerging.
- At a fundamental level, public sector entities developing or deploying AI systems must ensure that such systems are:
    - Valid and reliable
    - Safe
    - Privacy protective
    - Transparent
    - Accountable
    - Human rights affirming

AI Scribes in Ontario’s Health Sector

Guidance for Procurement, Implementation, and Use

What is an AI Scribe?

- Fundamentally, an AI scribe is a transcription tool that can summarize health care visits and populate this information into a health information custodian’s (custodian) electronic medical record.
- They may also produce medical notes, reports, or referral letters.
- Some offer additional features such as recommended diagnosis, treatment, prescription medications, and laboratory tests.
- Some vendors are actively seeking to expand to other settings including physiotherapy, chiropractic, and mental health.

AI Scribe Guidance for the Health Sector

- AI scribes have the potential to bring relief to the primary care crisis in Ontario, but there is a risk that they may worsen or create new problems if they are not robustly developed and maintained.
- It is important for custodians to consider the potential harms and challenges of AI in the health sector, especially related to accountability, validity, reliability, safety, privacy, transparency, and human rights.
- As AI scribes evolve and implementation expands, so too will the risks and human rights considerations.

Accountable

Valid & Reliable

Privacy Protective

Safe

Transparent

Human Rights Affirming

Accountable

- Under PHIPA, custodians are ultimately accountable for the actions of their agents and any other party acting on their behalf to collect, use, disclose, retain, transfer, or dispose of records of personal health information that are in their custody or control.
- Before procuring, implementing, and using an AI system like an AI scribe, custodians should have a robust AI Governance and Accountability Framework in place.

AI Governance and Accountability Framework

Recommended components

- AI governance committee
- Policies, practices, and procedures
- Training and awareness
- Initial and ongoing assessment, monitoring, and testing
- AI risk management framework
- Human oversight
- Complaint and inquiry mechanisms
- Recourse, reporting, and notification mechanisms
- Confidentiality and end user agreements
- Contractual safeguards

Accountable

Valid & Reliable

Privacy Protective

Safe

Transparent

Human Rights Affirming

Valid and Reliable

- Robust design and third-party assessment
  - Before procuring, implementing, and using AI scribes, custodians are expected to take steps to ensure it has been the subject of robust design and has been rigorously tested, ideally by an independent third-party.
- Role of custodians in ensuring accuracy
  - Under PHIPA, custodians are required to take reasonable steps to ensure that the personal health information they use and disclose is accurate, complete, and up to date.
  - Custodians who procure, implement, and use AI scribes must have adequate administrative and technical safeguards in place to protect records of personal health information from inaccuracy.

Accountable
Valid & Reliable
Privacy Protective
Safe
Transparent
Human Rights Affirming

Privacy Protective

- Legal authority and compliance
  - Custodians have obligations under PHIPA that cover the collection, use, and disclosure of personal health information, and this includes through the use of an AI system like an AI scribe.
- Consent
  - Custodians must ensure that individuals are meaningfully informed of the use of an AI scribe.
  - Where the collection, use or disclosure of PHI is done with consent, custodians must ensure that individuals are provided an opportunity to withhold consent prior to using the AI scribe.
- Access and correction of health records
  - Custodians must ensure that adequate administrative and technical measures are in place to ensure they meet their obligations to provide individuals with access to and correction of records of their PHI that are generated or altered by AI scribes.
- Data minimization and purpose limitation
  - In the context of AI scribes, custodians must consider whether they have the authority to disclose PHI to the AI scribe vendor or if other information, such as de-identified data would serve the purpose.

Accountable
Valid & Reliable
Privacy Protective
Safe
Transparent
Human Rights Affirming

Safe

- Assessments
  - Privacy Impact Assessment (PIAs)
  - Threat Risk Assessments (TRAs)
  - AI specific assessments (e.g. Algorithmic Impact Assessments)
  - Vendor assessments
  - Ethical assessments
- Ongoing monitoring and testing of the AI model
  - Custodians should take reasonable steps to ensure that the AI scribe is subject to monitoring and testing that is both regularly scheduled as well as based on certain trigger thresholds.
- Collection and retention of recordings and transcripts
  - Custodians must carefully consider their legal authority to collect and retain recordings and transcripts and the necessary safeguards to protect them.
- Disclosure and data sharing with AI scribe vendors
  - Custodians must not disclose personal health information without a legal authority to do so and must have appropriate administrative, technical, and physical safeguards in place.

Accountable

Valid & Reliable

Privacy Protective

Safe

Transparent

Human Rights Affirming

Safe

Cont’d

- Custodian monitoring, auditing, and logging and agents
  - Custodians must ensure they have robust administrative, technical, and physical safeguards in place to protect records of PHI against unauthorized use or disclosure by their agents.
- Safeguarding against cybersecurity breaches
  - Custodians must ensure that they and their AI scribe vendor both have in place robust administrative and technical safeguards to prevent, detect, mitigate, and remediate against cybersecurity attacks.
- Secure storage and transfer of PHI when using AI scribes
  - PHIPA sets out obligations for custodians that require them to transfer and store records of PHI in a secure manner.
- Secure disposal of PHI when using AI scribes
  - If a decision has been made to dispose of the AI scribe’s recordings or transcripts, custodians need to ensure they are meeting their obligations under PHIPA related to secure disposal.

Accountable

Valid & Reliable

Privacy Protective

Safe

Transparent

Human Rights Affirming

Transparent

- Custodian transparency
  - Written public statements
  - Contact person and responding to inquiries and complaints
  - Access and correction of records of PHI
  - Breach notification, reporting obligations, and complaints to the IPC
- AI scribe vendor transparency
  - Transparency of vendor privacy policy and data practices
  - Transparency measures related to the AI model
  - Technical measures to support transparency

Human Rights Affirming

Accountable

Valid & Reliable

Privacy Protective

Safe

Transparent

Human Rights Affirming

- Ethical assessments
  - Prior to procuring, implementing, or using an AI system, custodians must consider whether their application in the health sector is appropriate and ethical.
  - The OHRC and the Law Commission of Ontario have developed a Human Rights AI Impact Assessment to assist in the prevention, detection, and mitigation of bias and discrimination and to uphold human rights obligations throughout the AI lifecycle.
- Consultation with affected individuals and groups
  - Custodians should take steps to ensure sufficient consultation and involvement with affected individuals and groups when they procure, implement, and use AI scribes.

Discussion and Questions for the Fellows

Questions for the Fellows

- What types of AI solutions are being considered or have been implemented in your organizations and what is your impression of them so far?
- When it comes to safeguarding patient privacy, what are some of the biggest challenges you are facing as you think about developing or procuring AI solutions?
- What sort of guidance would you find helpful from the IPC as you consider developing, procuring, implementing, or using AI in your organizations?

Additional Resources

IPC-Related References

- Bill 194: Ontario’s missed opportunity to lead on AI (Blog post)
- Written Submission on Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024
- Artificial intelligence in health care: Balancing innovation with privacy (IPC Podcast)
- **Privacy Complaint Report PI21-00001**
- Joint statement on the use of AI technologies (Ontario IPC and Ontario Human Rights Commission)
- Principles for Responsible, Trustworthy and Privacy Protective Generative AI Technologies (Joint resolution of the federal, provincial, and territorial information and privacy commissioners)
- Resolution on Generative Artificial Intelligence Systems (Joint resolution of the Global Privacy Assembly)
- Statement on Generative AI (Roundtable of G7 Data Protection and Privacy Authorities)
- IPC Ontario Comments on Ontario’s Trustworthy AI Framework

Thank you!

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