



AI IN THE WORKPLACE: USE, PRIVACY & POLICY

Presented By: Michael Watt,
Loren Mallett, & Jeffrey Zhang

June 17, 2026 | 11:00AM – 12:00PM PST



YOUR **PERSPECTIVE** OUR **FOCUS**™



Today we will cover:

1	Introduction
2	Common AI in the Workplace
3	Privacy Legislation & AI
4	Future Regulatory/Legislative Developments
5	Best Practices for Use of AI Systems - Personal Information Considerations
6	AI in Hiring + Employment
7	Takeaways



INTRODUCTION

Opening Comments



Our lawyers are both solicitors and litigators handling matters in the corporate commercial world. We are here to help improve workplace policies or protect clients when existing policies fail.



We will outline the basics of Artificial Intelligence (AI) and further identify legal concerns arising from the use of AI in the workplace.



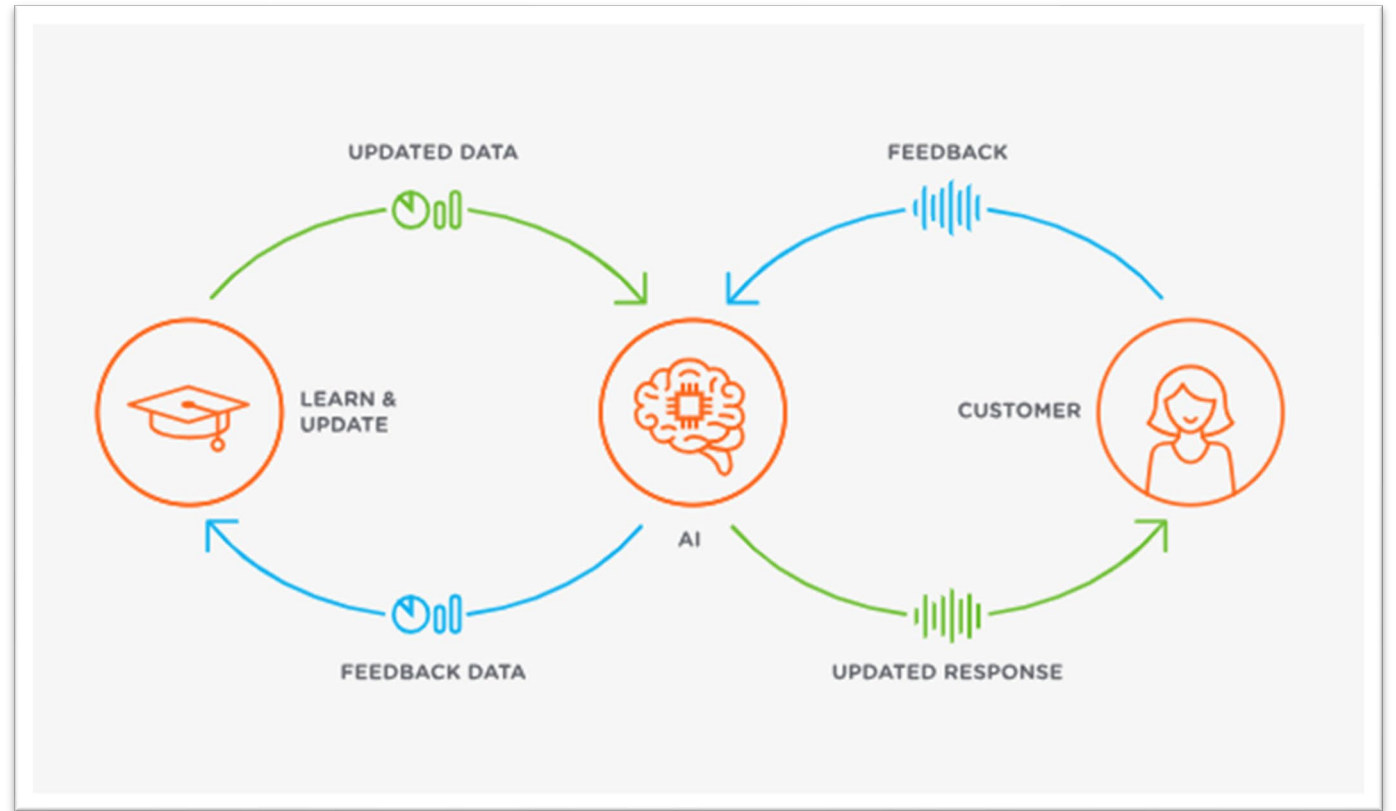
The AI space is rapidly changing and thus we will focus on the fundamentals rather than try and showcase the 'latest and greatest' AI innovations.



Ask questions at any time!

Introduction – What is AI?

- Field of computer science involving computing systems that are programmed to behave in a way that would be considered intelligent.
- Concerned with the creation of a process of thinking.



Source: Interactions – Machine Learning
<https://www.interactions.com/machine-learning/>

Introduction - LLMs

Large Language Models (“LLM”)

- What It Is: An LLM is a statistical model trained on massive amounts of text data. Its primary job is to predict the next most logical word or phrase based on the prompt it receives.

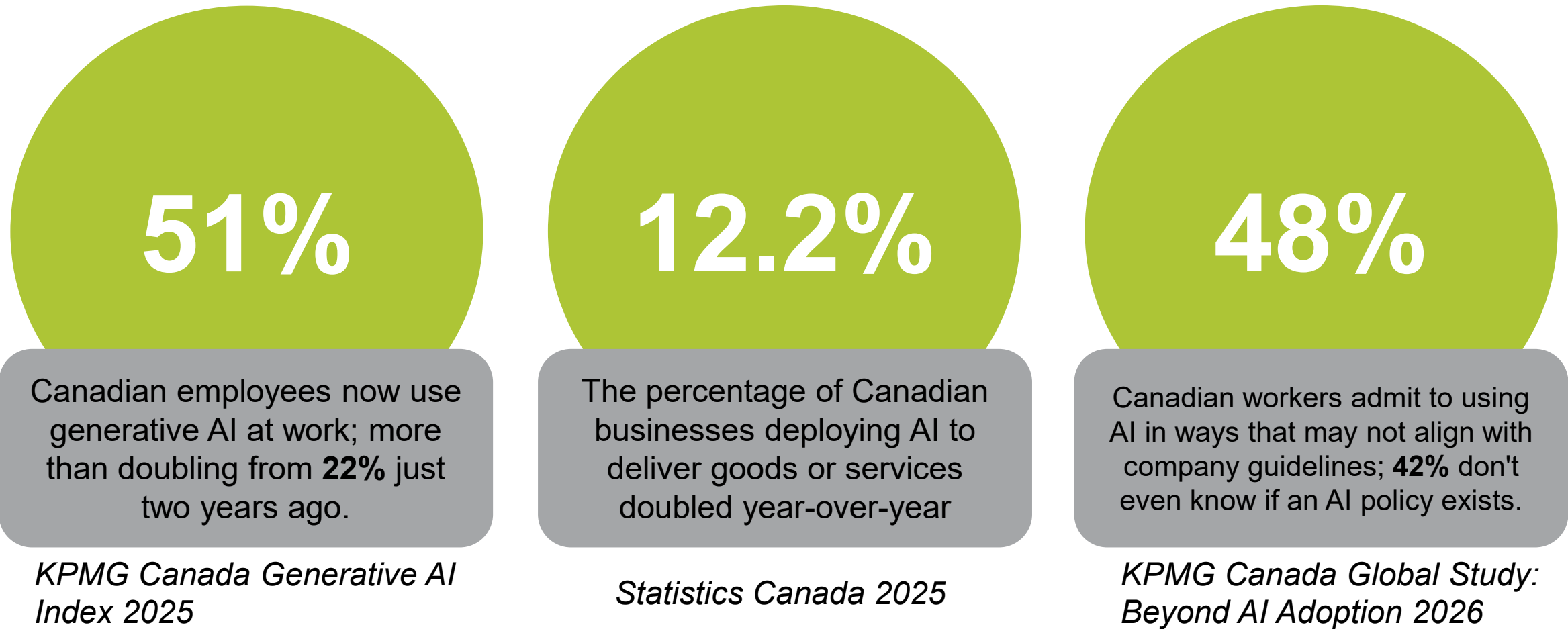
Examples: Claude, ChatGPT

- Despite being “trained” on a plethora of data, it doesn't "know" facts; it knows language patterns.

Basic Workplace Functions:

- Text Generation: Drafting emails, standard operating procedures, or job descriptions.
- Synthesis: Summarizing 50-page reports, meeting transcripts, or market research.
- Data Translation: Converting unstructured notes into organized tables or writing code.

Canadian AI Use in the Workplace



51%

Canadian employees now use generative AI at work; more than doubling from **22%** just two years ago.

KPMG Canada Generative AI Index 2025

12.2%

The percentage of Canadian businesses deploying AI to deliver goods or services doubled year-over-year

Statistics Canada 2025

48%

Canadian workers admit to using AI in ways that may not align with company guidelines; **42%** don't even know if an AI policy exists.

KPMG Canada Global Study: Beyond AI Adoption 2026

Introduction - An AI Obsession

Reasons for Rapid AI Adoption

- **Zero Technical Barrier**
 - Generate prompts for any need
- **Accessible Productivity**
 - Simplify: emails, summaries, and data
- **The Canadian Productivity Gap**
 - At a macro level, Canadian executives are aggressively pushing AI adoption to combat Canada's persistent economic productivity stagnation.

From: KPMG: “Canada is lagging behind global peers in AI trust and literacy” (June 2025)



Introduction – Attitudes Towards AI in Canadian Law

- ***Espinosa Cotacachi v. Canada (Citizenship and Immigration)*, 2024 FC 2081** – Found that immigration officers' use of an AI Tool: Chinook was permitted and did not raise issues of reasonableness or procedural fairness. Court stated:
“[23] The Court has consistently held that an officer's use of Chinook to process applications does not, on its own or without clear evidence, raise issues of reasonableness or procedural fairness...”
- ***A2501051 (Re)*, 2025 CanLII 97422 (BC WCAT)** – Tribunal found that while no current rules existed regarding AI use in submissions, parties still needed to adhere to the Code of Conduct and not put forth information known to be untrue.

Attitudes Towards AI in Canadian Law

Courts have managed AI in two ways:

- Recognize the existence of AI, research, test, and scrutinize the programs until they are defensible in their reliability and accuracy.
 - Ex. *Cotacachi*
- Use existing rules and legislation to fill the gaps, making decisions based on the effects of AI use rather than intention.
 - Ex. *A2501051*



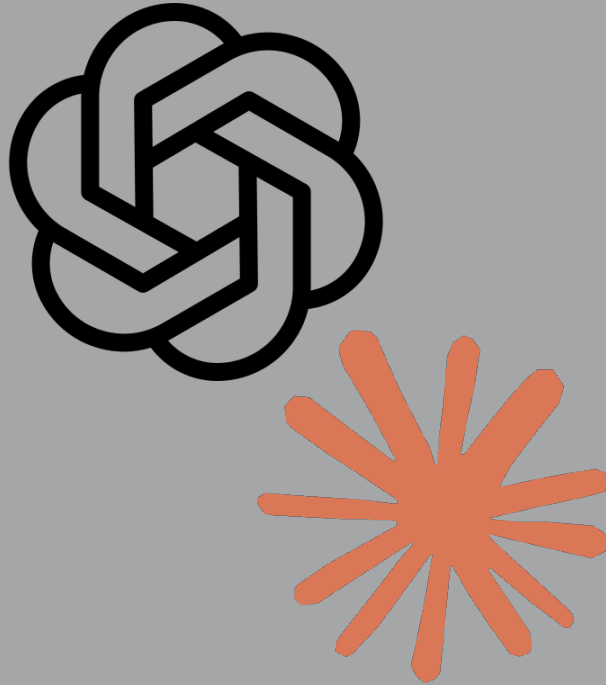
COMMON AI IN THE WORKPLACE

Common AI in the Workplace

Ecosystem Integration



Standalone Powerhouses



Meeting + Communication

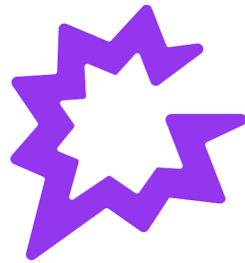


Common AI in the Workplace – Specialized Function

Knowledge Retrieval



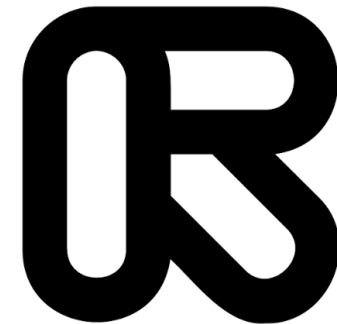
Revenue Intelligence



Customer Operations



HR Video Generation

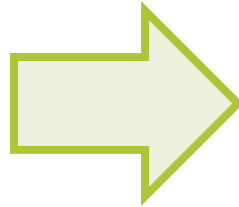


Using AI in the Workplace

Changing Output Verification Concerns

46.4%

**2023 Study on % of AI-Powered
Language model output factual errors**



20.3%

**2026 Study examined 2025 outputs and
found the new number closer to this %**

Using AI in the Workplace

Output Verification Error Consequences

- In *Moffatt v. Air Canada*, 2024 BCCRT 149, the British Columbia Civil Resolution Tribunal rejected the argument that a company is not responsible for its chatbot. The airline was held fully liable for negligent misrepresentation after its AI tool gave a customer false refund information.
- In *Zhang v. Chen*, 2024 BCSC 285, a Vancouver lawyer was ordered to personally pay court costs after her AI application hallucinated fake legal cases that were filed without human review.

➤ **Review is key when using AI as a tool in the workplace**



PRIVACY LEGISLATION & AI

Canada's Current Privacy Framework

Organizations have privacy obligations when they collect, use, or disclose personal information.

In British Columbia, key privacy statutes include:

- FIPPA — applies to public bodies.
- PIPA — applies to private-sector organizations.

Both statutes impose core obligations relating to personal information handling.

The four key considerations are:

- Consent
- Protection
- Accuracy
- Retention

Canada's Current Privacy Framework

Organizations must obtain meaningful consent for the collection and use of personal information.

Collection and use must be for purposes a reasonable person would consider appropriate.

Organizations must safeguard personal information in their custody or control.

Security measures must protect against risks such as:

- Unauthorized collection
- Unauthorized use
- Unauthorized disclosure
- Unauthorized disposal

Canada's Current Privacy Framework



Accuracy obligations apply when personal information may be used to make a decision affecting an individual.



Organizations must make reasonable efforts to ensure the information is accurate and complete.



Retention obligations apply when personal information is used to make a decision directly affecting an individual.



Organizations must retain that information for at least one year after use.



Retention supports the individual's ability to access the information.

Canada's Current Privacy Framework



Consent and protection are baseline obligations whenever personal information is used.



Accuracy and retention become especially important where personal information supports decisions about individuals.



AI-assisted decision-making therefore raises heightened compliance considerations under existing privacy laws.

Application of Current Privacy Laws to AI

Canada has not yet enacted AI-specific privacy legislation.

Existing privacy laws still apply to AI systems.

Organizations must comply with privacy laws when AI collects, uses, or discloses personal information.

Relevant laws include:

- PIPEDA
- B.C. PIPA
- B.C. FIPPA
- Québec Law 25

Application of Current Privacy Laws to AI



Canadian privacy regulators have confirmed that current privacy laws apply to AI.



G7 data protection authorities have also stated that current law applies to generative AI products and uses.



Canadian Privacy Commissioner Philippe Dufresne has emphasized that existing privacy laws continue to apply to new technologies, including generative AI.



AI-specific legal frameworks may develop, but current obligations remain in force.

Application of Current Privacy Laws to AI



The use of AI or automated decision-making does not reduce existing privacy rights.



Organizations must meet the same privacy obligations when personal information is processed by AI.



The legal obligations remain the same, but the compliance context changes.



AI systems may require new processes to ensure privacy obligations are properly implemented.

Application of Current Privacy Laws to AI

Organizations should proactively align AI practices with privacy commissioner guidance.

Key compliance priorities include:

- Consent and legal authority
- Appropriate safeguards
- Accuracy of personal information
- Retention of information used in decisions
- Transparency and accountability
- Early alignment can reduce risk and prepare organizations for future AI-specific legislation.



FUTURE REGULATORY/LEGISLATIVE DEVELOPMENTS

Canada's Attempt to Modernize Privacy and AI Law



Canada has attempted to modernize federal privacy law and introduce AI-specific legislation.



The key legislative proposal was Bill C-27, introduced in June 2022.



Bill C-27 did not pass and died on the Order Paper when Parliament was prorogued on January 6, 2025.



Despite this, Canada is expected to continue pursuing privacy and AI regulation.

Canada's Attempt to Modernize Privacy and AI Law

Bill C-27 would have introduced three statutes:

- Consumer Privacy Protection Act — CPPA
- Personal Information and Data Protection Tribunal Act — PIDPTA
- Artificial Intelligence and Data Act — AIDA

The CPPA would have replaced Part 1 of PIPEDA.

AIDA would have regulated AI systems used in international and interprovincial trade and commerce.

Both CPPA and AIDA were relevant where AI is used to make decisions with a significant impact on individuals

Canada's Attempt to Modernize Privacy and AI Law

The CPPA aimed to strengthen consumer privacy protections.

It also sought to support responsible innovation and data-driven commerce.

Key themes included:

- Individual control over personal information
- Transparency
- Accountability
- Meaningful consent
- In the AI context, the CPPA focused on explainability, accuracy, retention, and access

Canada's Attempt to Modernize Privacy and AI Law

The CPPA defined automated decision systems broadly.

Covered technologies included:

- Rules-based systems
- Predictive analytics
- Machine learning
- Neural networks

Organizations using personal information for decisions would need to:

- Retain relevant information
- Support access and explanation rights
- Ensure information is accurate, up to date, and complete

Canada's Attempt to Modernize Privacy and AI Law

- Organizations would need to provide information about how personal information is used.
- They would also need to explain how automated decision systems are used for predictions, recommendations, or decisions.
- For significant automated decisions, individuals could request an explanation of:
 - The type of personal information used
 - The source of that information
 - The principal factors leading to the outcome
- The goal is to help affected individuals understand how the AI-assisted decision was reached

Canada's Attempt to Modernize Privacy and AI Law

The CPPA would have expanded the Privacy Commissioner's powers.

The Commissioner could investigate, make binding decisions, issue compliance orders, and recommend administrative monetary penalties.

Maximum administrative penalties could reach the greater of:

- \$10 million; or
- 3% of global gross revenue.

Serious offences could result in fines up to the greater of:

- \$25 million; or
- 5% of global gross revenue

Canada's Attempt to Modernize Privacy and AI Law



AIDA would have applied to private-sector AI activity in international and interprovincial trade and commerce.



It would apply not only to AI developers, but also to organizations that deploy or operate AI systems.



Organizations using third-party AI tools could still be within scope.



Relevant activities included using, managing, or processing data for an AI system

Canada's Attempt to Modernize Privacy and AI Law

- AIDA focused heavily on “high-impact” AI systems.
- Criteria would be set by future regulations.
- AI systems using personal information to make decisions about individuals may fall within this category.
- **Relevant risk factors include:**
 - Severity of potential harm
 - Scale of use
 - Human rights impacts
 - Ability to opt out
 - Impacts on vulnerable groups

Canada's Attempt to Modernize Privacy and AI Law



Organizations responsible for high-impact AI systems would need to identify, assess, and mitigate risks.



This includes risks of harm and biased output.



“Biased output” includes decisions, recommendations, or predictions that unjustifiably discriminate on protected grounds.



Organizations would also need records explaining mitigation measures and monitoring compliance

Canada's Attempt to Modernize Privacy and AI Law

- The Minister would have broad oversight and enforcement powers.
- **Powers included:**
 - Compelling records
 - Ordering audits
 - Requiring corrective measures
 - Suspending or stopping use of an AI system in urgent cases
- Organizations would need to notify the Minister where use of a high-impact AI system results in, or is likely to result in, material harm.
- Penalties could include significant fines, and individuals could face fines or imprisonment

Canada's Attempt to Modernize Privacy and AI Law

- Bill C-27 did not become law, but it shows the likely direction of Canadian privacy and AI regulation.
- **Future legislation is expected to focus on:**
 - Transparency
 - Accountability
 - Explainability
 - Accuracy
 - Retention
 - Bias mitigation
 - Regulatory oversight
- Organizations using AI should begin aligning with these principles now to prepare for future legal requirements

So where do we go next?

No comprehensive federal replacement yet

- As of June 11, 2026, the federal government has not introduced a new comprehensive private-sector privacy/AI bill to replace the old Bill C-27.

Canada's Attempt to Modernize Privacy and AI Law

Is a Replacement Bill Expected? Likely, but probably not a straight revival

- The federal government has signaled continued interest in:
 - modernizing privacy law;
 - regulating AI-related risks;
 - updating online safety rules.
- However, a future bill may not simply reintroduce the old Bill C-27 package.
- The former structure bundled together:
 - private-sector privacy reform;
 - a new privacy tribunal;
 - broad AI regulation.
- Given criticism of AIDA, the government may choose to separate privacy reform from AI regulation.

Recent Signals from the Federal Government

Policy activity continues:

- **April 2, 2026:** Government launched a review of the Privacy Act.
 - This relates to federal public-sector privacy, not private-sector PIPEDA reform.
- **June 4–5, 2026:** Government launched its AI for All strategy.
 - Included commitments to modernize privacy and online safety laws for an AI-driven world.
- **June 10, 2026:** Government introduced Bill C-34, the Safe Social Media Act.
 - Addresses social media services and certain AI chatbot services.
 - Narrower than a full replacement for Bill C-27/AIDA.

What this means for organizations

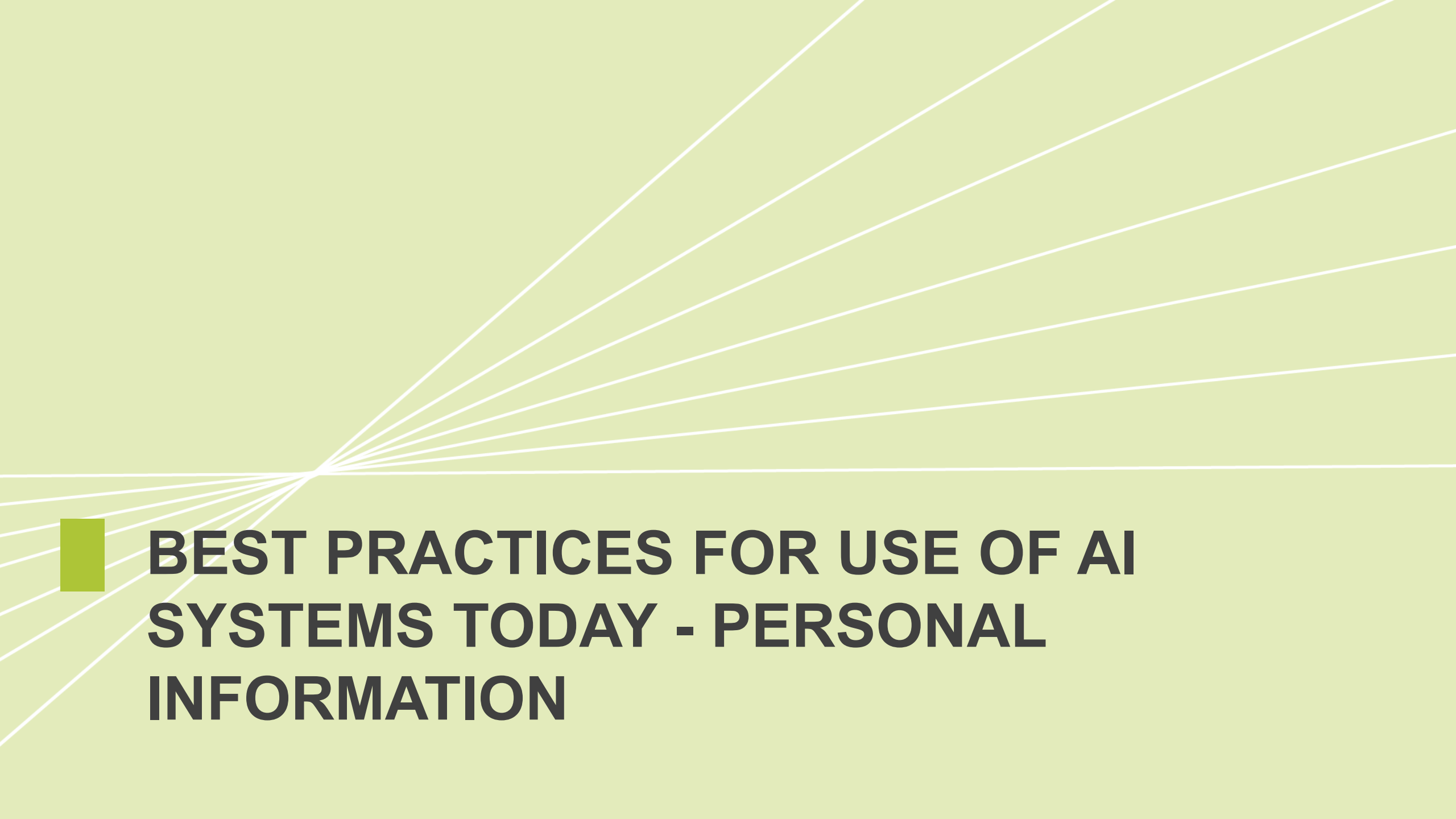
No new CPPA/AIDA-style federal regime is currently in force.

PIPEDA remains the key federal private-sector privacy law for now.

Organizations should still prepare for reform because federal activity suggests change is likely.

Watch for:

- a new private-sector privacy modernization bill;
- narrower AI-specific legislation or regulation;
- online safety rules affecting platforms, social media, and AI chatbots.



BEST PRACTICES FOR USE OF AI SYSTEMS TODAY - PERSONAL INFORMATION

Best Practices

With the death of Bill C-27, should organizations care about the use of personal information in AI Systems?

- Organizations should still care because Bill C-27 was not the source of all privacy obligations.
- It would have added AI-specific rules, but organizations using personal information in AI systems are already subject to existing privacy laws.

Best Practices – Good place to start

Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies, issued on December 7, 2023.

- Joint guidance issued by Canada's federal, provincial, and territorial privacy commissioners.
- Explains how existing Canadian privacy laws apply to generative AI.
- Applies to organizations developing, providing, or using generative AI systems.
- Not legislation, but an important regulatory roadmap.

Best Practices - Why the Guidance Matters



Confirms that organizations remain responsible for privacy compliance when using generative AI.



Helps translate existing privacy principles into AI-specific practices.



Signals the likely direction of future AI-specific laws.



Many recommendations may already be required under existing privacy legislation.



Early alignment helps organizations manage risk and prepare for future regulation.

Best Practices - Core Principles: Legal Basis and Purpose

Legal Authority and Consent

- Have legal authority for collecting, using, disclosing, and deleting personal information.
- Ensure consent is meaningful and specific where relied on.

Appropriate Purposes

- Use personal information only for appropriate purposes.
- Ensure generative AI is suitable for the specific application.

Necessity and Proportionality

- Use generative AI and personal information only where necessary and proportionate.
- Use anonymized, synthetic, or de-identified data where possible.

Best Practices - Core Principles: Transparency and Accountability

Openness

- Be transparent about what personal information is collected, used, and disclosed.
- Explain why the information is needed.
- Disclose when generative AI is used in decision-making.

Accountability

- Organizations remain responsible for privacy compliance.
- Establish governance structures, policies, assessments, and complaint processes.
- Maintain records to demonstrate compliance.

Best Practices - Individual Rights and Data Limits

Individual Access

- Enable individuals to access and correct their personal information.
- Support access rights where information appears in AI models or outputs.

Limiting Collection, Use, and Disclosure

- Limit personal information to what is necessary.
- Avoid function creep and indiscriminate collection.
- Set retention schedules for training data, prompts, and outputs.

Best Practices - Core Principles: Accuracy and Safeguards

Accuracy

- Ensure personal information used in AI is accurate, complete, and up to date.
- Take reasonable steps to confirm AI outputs are accurate for the intended purpose.

Safeguards

- Protect personal information based on sensitivity.
- Address AI-specific risks, including:
 - Prompt injection
 - Model inversion
 - Jailbreaking

Best Practices



Later AI/Privacy Developments After the 2023 Guidance



Canadian and international privacy regulators have continued to address AI after the 2023 generative AI guidance.



Later developments reinforce that AI remains a live privacy compliance issue.

Best Practices

Key post-guidance developments:

- G7 Statement on Trustworthy AI — October 11, 2024
- G7 Statement on AI and Children — October 11, 2024
- OPC's AI, Privacy, and Your Business guidance — May 6, 2025
- Privacy Commissioner's statement to Parliament on AI — February 2, 2026

The G7 Data Protection and Privacy Authorities are the privacy regulators of the G7 jurisdictions. They issue coordinated guidance and statements on emerging privacy issues, including how existing data protection laws apply to artificial intelligence and generative AI.

G7 Statement on Trustworthy AI

- Issued by the G7 Data Protection and Privacy Authorities on October 11, 2024.

Best Practices

Confirms that AI creates significant challenges for:

- Privacy
 - Data protection
 - Fundamental rights and freedoms
-
- Reiterates that current privacy and data protection laws apply to generative AI.
 - Emphasizes that privacy and data protection should be embedded into AI development, deployment, and governance.
 - Calls for cooperation between privacy regulators and other regulators to address AI's cross-cutting risks.

Best Practices

Why the Trustworthy AI Statement Matters

- Shows that privacy regulators see AI governance as part of their existing mandate.
- Reinforces that organizations should not wait for AI-specific legislation.

Highlights common AI privacy risks, including:

- Processing of personal data
- Bias and discrimination
- Deepfakes and disinformation
- Impacts on human rights

Supports the view that privacy principles such as fairness, accountability, transparency, and security are central to AI governance.

Best Practices - Key Business Guidance from the OPC

Organizations developing or using generative AI should:

- Label when generative AI is used in content creation or decision-making.
- Establish legal authority for collecting and using personal information.
- Ensure consent is valid and meaningful where relied on.
- Be open about how information is used and the privacy risks involved.
- Make AI tools explainable to users.
- Develop safeguards for privacy rights.
- Limit sharing of personal, sensitive, or confidential information.
- Build privacy by design into AI tools

Best Practices - Overall Takeaway

Bill C-27 died, but AI/privacy regulation did not disappear.

Regulators continue to issue AI-specific statements, guidance, and policy positions.

The consistent message is:

- Existing privacy laws apply now.
- AI systems must protect personal information.
- Organizations remain accountable for AI-related privacy risks.
- Future regulation is likely to build on current privacy principles.
- Organizations should align AI practices with privacy regulator guidance now, rather than waiting for new legislation.

Application to BC: More Privacy Law



The Advance Notice Mandate: While Ontario has an AI-specific law, British Columbia and Alberta utilize existing Personal Information Protection Acts (PIPA) to enforce similar boundaries.



The Purpose Statement: Under PIPA frameworks, employers may collect and use candidate data only if they provide advance notice detailing the exact purposes of that collection.



The Outsourcing & Service Provider Rule (Alberta PIPA): If you upload a candidate's resume, cover letter, or video file into an AI platform, you are handing personal data to a third-party provider. Alberta law explicitly requires you to inform the candidate if that service provider operates outside Canada and what specific tasks they have been authorized to perform.



The Consent Shift: If an employer's third-party AI vendor uses candidate resumes to train their own underlying commercial models, the standard "employment notice exception" vanishes. You must obtain explicit, proactive consent from the job seeker.



AI IN HIRING + EMPLOYMENT

AI in Hiring + Employment

Hiring Changes: Ontario Job Posting Disclosure

As of January 1, 2026, changes to the *Employment Standards Act* came into effect.

Section 8.1: Any employer with **25 or more** employees **must explicitly disclose** if **AI** is used in the **hiring process**.

AI	Hiring Process
Definition (O. Reg 476/24): “Machine-based systems inferring from inputs to generate outputs.”	Defined as covering the stages of: • Screening [Keyword Filters] • Assessing [Video/Skills Tech] • Selecting [Ranking Algorithms]

AI in Hiring + Employment

Challenges in Hiring & Recruiting¹

Hiring Manager Friction	64% of Canadian HR managers state that AI-generated resumes create massive verification challenges.
Workload Inflation	89% of HR leaders report that their recruiting team's workload has grown drastically due to AI-driven applicant volume.
Extended Delays	61% of Canadian HR departments report a measurable increase in their overall time-to-hire.

1. From Robert Half's Article "AI's Impact on Hiring": <https://www.roberthalf.com/ca/en/insights/ai-hiring-impact>

The AI Arms Race in Hiring

Candidate AI (Mass Resume Optimization)

└─> Floods HR Systems with Inauthentic Profiles

└─> Employer AI (Automated Filtering)

└─> Triggers Strict Mandatory Legal Disclosures

- Candidates – in an era of mass employer AI use, have begun using generative AI to perfectly align their resumes.
 - Tailored Resumes
 - Keyword optimization
- To counter this, Canadian employers are actively reversing the tech trend by introducing extra in-person interviews and supervised skills assessments to separate real talent from AI generation.

AI in Hiring + Employment – Human Rights

AI models do not generate data from thin air; they learn from existing human datasets and inevitably replicate and amplify past human inequalities.

Bias is not just text-based. A 2023 Bloomberg article on visual tools like Stable Diffusion reveals severe stereotyping, such as routinely depicting CEOs as white men, dark-skinned individuals as criminals, and rarely showing women as judges, doctors, or lawyers.

- [Generative AI Takes Stereotypes and Bias From Bad to Worse](#)

A 2020 study conducted by the Stanford Computational Policy Lab found that speech recognition software still struggles to accurately process accented or non-native speech. Relying on automated AI tools to evaluate timed video interviews can easily trigger a Human Rights complaint on the ground of place of origin.

- [Racial disparities in automated speech recognition | PNAS](#)

AI in Hiring + Employment – Job Loss

- “While AI is often associated with concerns about widespread job loss, early evidence from Canada since the mass availability of generative AI tools like ChatGPT suggests a more nuanced reality, highlighting a labour market evolving amid a confluence of technological, demographic and economic factors.”
 - StatsCan: Canadian employment trends in the era of generative artificial intelligence: Early evidence - <https://www150.statcan.gc.ca/n1/pub/36-28-0001/2026001/article/00003-eng.htm>

AI in Hiring + Employment – Constructive Dismissal



If an employer unilaterally utilizes AI in a way that fundamentally alters, reduces, or strips an incumbent employee's core job duties and responsibilities, the employee may legally claim they have been constructively dismissed.



A successful constructive dismissal claim is treated as a wrongful dismissal without cause, requiring the employer to pay statutory termination notice, severance, or common law reasonable notice.



Update employment contracts to include explicit language reserving the right to unilaterally modify an employee's duties over time.

AI in Hiring + Employment – Labour Agreements



Unionized employers face strict boundaries.



Canadian Unions have taken to the International Labour Conference to speak on AI transforming the workplace – Canadian Labour Congress: “Canada’s unions take concerns over AI and labour rights to global stage” (June 2026)



Collective agreements and statutes like the *Labour Relations Code* s. 54 set notice at 60 days in BC and union consultation before implementing any technological changes that alter working conditions for a significant number of workers.



Collective Agreements may contain terms limiting the loss of employment due to AI.



TAKEAWAYS

Designing AI Policy

As AI may be used in all aspects of the business, an effective AI policy should be drafted for general application.

Requires input from all parts of the business, including IT, legal, human resources, and sales.

Organizations must establish a clear internal corporate message on technology adoption, explicitly defining whether generative AI use is:

- actively encouraged,
- simply permitted for specific tasks,
- restricted based on department-specific needs, or
- advance approval is required before adoption.

Scope of Policy



The policy must cover all employees, independent contractors, and third-party vendors who interact with or implement AI tools for company purposes.



Delineate between **Personal AI use** and **Work-use**.



Compliance standards must apply to all work-related activities without regard to location, capture AI use during or outside normal hours, and include AI use of company equipment, personal devices, or third-party hardware.



Because different teams handle varying levels of risk, the core policy should consider specialized, business unit-specific extensions to AI programs or the need for separate protocols for high-exposure groups like finance or HR departments.

Controlling Use and Access

-  Policies should distinguish between AI tools such as Generative AI use and Algorithmic AI, as the latter may be more central to the business.
-  Blanket AI bans simply will not work, as technology continues to advance.
-  Employers should maintain an actively managed register of approved AI tools, outlining which departments and jobs are authorized to utilize each platform.
-  Prior to using an approved tool for an unlisted task, or utilizing an unlisted tool for any work-related purpose, users must secure express, written advance consent from a supervisor, manager, or designated department head.
-  Critical thought must be applied to all machine outputs. Every piece of AI-generated content must be rigorously fact-checked, sense-checked, and cross-referenced with trusted sources before being relied upon or distributed.

Safeguarding Corporate Assets



AI outputs face legal ownership hurdles, as corporate copyright and patent protections typically require direct human authorship or contribution.



Employees must be barred from inputting corporate trade secrets, confidential business data, or proprietary information into public or unvetted AI prompts, as doing so can result in inadvertent disclosure to third parties.



Inputting data licensed from third parties into an AI model can violate commercial use restrictions, potentially exposing the employer to breach of contract liabilities.



Before publishing or distributing any work product generated or assisted by AI tools, employees may secure manager approval.

Disclosure of AI Use

Need to Disclose in Canada

- Before publishing or distributing any work product generated or assisted by AI tools, employees should include a clear public disclosure or disclaimer stating that the content was AI-generated.
- Not a rule in Canada *yet*.

Other Jurisdictions

- *Federal Trade Commission (FTC)* – Section 5
- *EU AI Act* – Article 50
- Both highlight the importance of transparency and disclosure in AI in advertising and endorsements.

Accountability in AI Use

- To ensure traceability, employees should be required to document their business AI usage in an internal register or **Data Asset Inventory**, which is recommended by Practical Law Canada: “Generative AI in the Workplace Policy” (page 23) and tracks:
 - the tool name,
 - the specific purpose,
 - input sources,
 - underlying logic models, and
 - the research used to verify accuracy.
- Tools like: ChatGPT Enterprise/Claude for Business/Gemini Workspace integrate this function inherently

Making Use of Paid LLM Programs

Feature	ChatGPT – Free	ChatGPT Enterprise
Data Use	Personal accounts operate under consumer policies	Business data is not used to train OpenAI models by default
Security Controls	Standard account security	Enterprise-grade security, encryption, compliance controls, and advanced governance features
User Management	Individual account only	Centralized user management, role-based permissions
Admin Console	No	Full administrative dashboard and usage insights
Custom GPTs	Yes - Restrictions	Available with enterprise controls and governance policies



Policy pulled from:
<https://openai.com/enterprise-privacy/>

Real World Effects of Paid vs Free AI

Courts varied on if AI-generated advice and prompts could be privileged, finding that it depended on the:

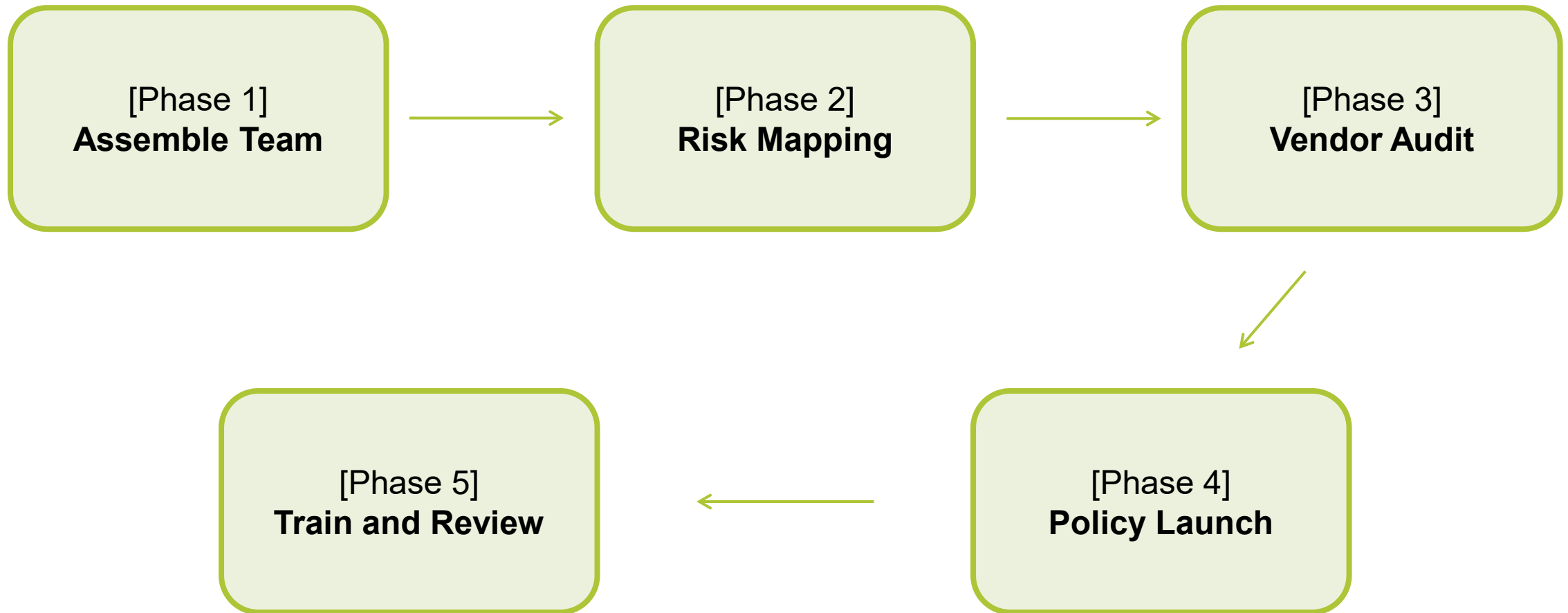
- type of program used,
- area of law covered,
- status of litigant, and
- **privacy policy of the tool**, where the consumer-version of Claude was found to have been equal to making a third-party disclosure.

United States Decisions:

United States v. Heppner, No. 1:25-cr-00503-JSR, 2026 U.S. Dist. LEXIS 32697 (S.D.N.Y. Feb. 17, 2026)

Warner v. Gilbarco, Inc., No. 2:24-cv-12333, 2026 WL 373043 (E.D. Mich. Feb. 10, 2026), reported at 820 F. Supp. 3d 629

Takeaways – Implementation Strategy





ANY QUESTIONS?

THANK YOU



Contact



Michael Watt

Partner

T: 604-484-1733

mwatt@ahbl.ca



Loren Mallett

Partner

T: 604 484 1750

lmallett@ahbl.ca



Jeffrey Zhang

Articling Student

T: 604 643 2486

jzhang@ahbl.ca

DISCLAIMER

*This presentation is for educational purposes only.
Please seek legal advice if you have a particular
situation. Use of these materials does not create a
solicitor client relationship.*

OFFICES

Vancouver

TD Tower
2700 – 700 West Georgia Street
Vancouver, BC V7Y 1B8
Canada

T: 604 484 1700

Toronto

Bay Adelaide Centre
2740 – 22 Adelaide Street West,
Toronto, ON M5H 4E3
Canada

T: 416 639 9060

Kelowna

Regus Landmark
1100 – 1631 Dickson Avenue
Kelowna, BC V1Y 0B5
Canada

T: 604 484 1700

LEARN MORE AT AHBL.CA

FOLLOW US ON SOCIAL MEDIA:



YOUR **PERSPECTIVE** OUR **FOCUS**™