DEVELOPING, OFFERING AND USING GENERATIVE AI TECHNOLOGIES: CANADIAN PRIVACY REGULATORS WEIGH IN

Posted on January 3, 2024

Categories: Insights, Publications

Canada’s federal, provincial and territorial privacy authorities have co-published a document entitled Principles for responsible, trustworthy and privacy-protective generative AI technologies (the “Principles”), offering critical guidance for organizations that develop, provide and use generative artificial intelligence (“GenAI”) systems.

GenAI, a subset of machine learning, has gained popularity for its ability to generate diverse outputs such as text, images and audio in response to users’ prompts. However, its reliance on vast training datasets and user inputs, often including personal information, poses unique privacy challenges.

The Principles are drafted to apply to organizations that are subject to Canada’s public, private and health sector privacy laws. Though the considerations outlined in the Principles are framed as recommendations, many will be mandatory for organizations to comply with applicable privacy legislation.

This bulletin includes a high-level summary of those Principles that apply equally to organizations that develop, provide and use GenAI systems. However, organizations are advised to consult the Principles in full, as they contain additional recommendations, including some that may apply exclusively to developers, providers and/or users of GenAI systems.

Key Principles and Recommendations

According to Canada’s privacy regulators, ten key privacy principles that apply to the development, provision and use of GenAI systems are as follows:

1. Legal Authority and Consent:
An organization must have and document its legal authority for collecting, using, disclosing and deleting personal information in the course of training, developing, deploying, operating or decommissioning a GenAI system. Notably, the Principles assert that using GenAI to infer information about an identifiable individual constitutes a “collection” of personal information and therefore requires a valid legal authority, such as consent.

When relying on consent as its legal authority, an organization must ensure that such consent is specific, “valid”
and meaningful”, and not obtained through deceptive design patterns.

An organization that sources personal information from a third party in connection with a GenAI system must ensure that the third party has collected the personal information lawfully and has a legal authority to disclose the personal information.

2. **Appropriate Purposes:**
An organization must avoid any collection, use and disclosure of personal information for inappropriate purposes and consider whether the use of a GenAI system is appropriate for a specific application. This includes avoiding the development, putting into service, or use of a GenAI system that violates the “No-Go Zones” already identified by Canadian privacy regulators (such as for discriminatory profiling or generating content that otherwise infringes on fundamental rights), as well as potential emerging No-Go Zones identified in the Principles (such as the creation of content for malicious purposes, e.g., deep fakes).

3. **Necessity and Proportionality:**
An organization must establish the necessity and proportionality of using GenAI, and personal information within a GenAI system, to achieve the intended purpose(s). The Principles further advocate for the use of anonymized, synthetic or de-identified data, rather than personal information, in GenAI systems whenever possible.

4. **Openness and Transparency:**
An organization must be transparent about its collection, use and disclosure of personal information, as well as potential risks to individuals’ privacy, throughout the development, training and operation of a GenAI system for which the organization is responsible. This includes, for example, clearly stating the appropriate purpose(s) for such collection, use and disclosure of personal information and meaningfully identifying when system outputs that could have a significant impact on an individual or group are created by a GenAI tool. This information should be made readily available before, during and after use of the GenAI system.

5. **Accountability:**
A robust internal governance structure should be developed to ensure compliance with privacy legislation, including defined roles and responsibilities, policies and practices establishing clear expectations with respect to compliance with privacy obligations, a mechanism to receive and respond to privacy-related questions and complaints, and a commitment to regularly revisiting accountability measures (including bias testing and assessments) based on technological and regulatory developments. The Principles also recommend that an organization undertake privacy impact and/or algorithmic impact assessments to identify and mitigate potential or known impacts of a GenAI system (or its use) on privacy and other fundamental rights.

6. **Individual Access:**
The Principles emphasize individuals’ right to access and correct the personal information about them that is collected during the use of a GenAI system or that is contained within a GenAI model. Accordingly, an organization must ensure that procedures exist for individuals to exercise such rights.

7. **Limiting Collection, Use, and Disclosure:**
An organization must limit the collection, use and disclosure of personal information to what is necessary to fulfill an appropriate, identified purpose. The Principles stress that publicly accessible personal information (including personal information published online) cannot be collected or used indiscriminately, including in connection with a GenAI system. Appropriate retention schedules must also be developed for personal information contained within a GenAI system’s training data, system prompts and outputs.

8. **Accuracy:**
Personal information used in connection with GenAI systems must be as accurate, complete and up-to-date as is necessary for the purpose(s) for which it is to be used. This obligation includes, without limitation, identifying and informing users of a GenAI system about any known issues or limitations regarding the accuracy of the system’s outputs, and taking reasonable steps to ensure that outputs from a GenAI system are as accurate as necessary for their intended purpose, particularly when the outputs will be used to make (or assist in making) decisions about one or more individuals, will be used in high-risk contexts, or will be released publicly.

9. **Safeguards:**
Safeguards must be implemented to protect personal information collected or used throughout the lifecycle of a GenAI system from risks of security breaches or inappropriate use. Such safeguards must be commensurate to the sensitivity of the personal information and take into account risks specific to GenAI systems, such as prompt injection attacks, model inversion attacks and jailbreaking.

10. **Considering the Impact on Vulnerable Groups:**
When developing or deploying a GenAI system, an organization should identify and prevent risks to vulnerable groups, including children and groups that have historically experienced discrimination or bias. GenAI systems should be fair and free from biases that could lead to discriminatory outcomes. For developers, this obligation includes ensuring that training data sets do not replicate or amplify existing biases or introduce new biases. Users of GenAI systems must oversee and review the systems’ outputs and monitor for potential adverse effects, particularly when such outputs are used as part of an administrative decision-making process or in highly impactful contexts (e.g., employment, healthcare, access to finance, etc.).

**Other Recent Developments in Canada’s Proposed Regulation of Artificial Intelligence**

The release of the Principles reflects a global movement calling for the safe and responsible development and use of artificial intelligence (“AI”).
Canada and the United States (among other countries) have endorsed the Guidelines for secure AI system development[1] which recommend that the design, development, deployment and operation of AI systems be done in a secure and transparent manner. This international collaboration demonstrates a unified approach by a number of governmental agencies to mitigating the potential risks associated with AI technologies.

In another significant step towards responsible AI adoption, several leading organizations, including CGI and IBM, have signed on to Canada’s Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. This voluntary commitment by major players in the GenAI space underlines the growing consensus on the importance of safe and ethical AI development and management.

Finally, significant legislative reform regarding international and interprovincial trade and commerce in AI systems is potentially on the horizon. If passed, Bill C-27, which is still under committee consideration in Canada’s House of Commons, would (among other proposed changes), introduce the Artificial Intelligence and Data Act (the “AIDA”).[2] The AIDA would codify some of the Principles with respect to certain regulated activities involving AI systems, including obligations related to risks assessments and transparency.

Key Takeaways for Businesses

Given the complex and evolving nature of GenAI, it is essential that organizations involved in the development, provision or use of GenAI:

- Conduct thorough assessments of their current and future GenAI systems and use cases for compliance with the recommendations outlined in the Principles;
- Develop and implement robust data governance policies and procedures that align with the requirements of privacy legislation and the Principles;
- Implement clear and comprehensive consent mechanisms for the collection, use and disclosure of personal information in connection with GenAI systems, unless another legal basis exists for such processing of personal information;
- Engage in continuous monitoring and updating of GenAI systems to address any emerging privacy concerns or biases;
- Foster a culture of privacy-protective and ethical GenAI use, ensuring that all stakeholders understand their responsibilities (for example, by undertaking regular role-specific training); and
- Collaborate with legal experts to ensure their AI initiatives otherwise align with privacy legislation, the Principles and any additional guidance and investigation findings that may be released by Canadian privacy regulators in the future.
If you have any questions about the Principles, or the application of Canada’s existing and proposed privacy legislation to the development, provision or use of GenAI technologies, a member of McMillan’s Privacy & Data Protection Group would be happy to assist you.

[2] See our previous bulletin on Bill C-27: ‘Privacy Reform is on the Table Once More’.

By Kristen Pennington, Robert C. Piasentin, Robbie Grant, Stephen Johnson (Student-at-Law)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2024