WeirFoulds LLP

Privacy and AI: Key Takeaways From Ontario IPC's Investigation on the Use of AI Tools

April 30, 2024

By Vipal Jain and Natalie Bravo, Student-at-Law

Background

In our technology-driven world, the impact of artificial intelligence (AI) is undeniable. AI tools can simplify tasks, boost efficiency, and enable new possibilities that were previously out of reach.

On February 28, 2024, Ontario's Information and Privacy Commissioner (IPC) released a report (the Report)[1] adjudicated by the Commissioner, that provides guidance on IT contracting and the use of AI tools. The Report involves McMaster University's (McMaster) use of an exam-monitoring software that collects and analyzes personal information with AI to identify academic misconduct and inform decisions about academic integrity. This Report comes at a time when the Government of Ontario is developing Ontario's Trustworthy Artificial Intelligence Framework[2] to govern the safe and responsible use of AI.

Below we discuss the Report, including the Commissioner's findings and recommendations.

IPC Investigation and Findings

In January 2021, the IPC received a complaint from a McMaster student under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) regarding McMaster's use of Respondus exam proctoring software. The student anonymously raised concerns that the university was inappropriately collecting student information via the software and that it was unclear how Respondus collected, used, disclosed, or disposed of student data.

The Respondus software used by McMaster consists of two programs. Respondus LockDown Browser locks down most of a student's computer functions during tests. Respondus Monitor records audio and video of students through webcams. It flags suspected cheating during tests by scanning for biometric information and analyzing it through AI. The IPC's investigation found that McMaster infringed on students' privacy. While McMaster's collection of student personal information was necessary for the exam proctoring software to function, students were not given adequate notice about the purpose of collection. McMaster had published multiple files describing the software and data collection, but these files were not consolidated or easily accessible to students, thus McMaster did not provide adequate notice as required by law.

Further, the university's contractual arrangement with Respondus did not adequately protect personal information collected.

Additionally, Respondus did not have consent to use the students' audio and video recordings for system improvement purposes.

Recommendations

In the Report, the Commissioner notes McMaster's efforts in due diligence prior to adopting Respondus software, including carrying out a pilot project, completing a privacy impact assessment, examining the vendor's policies, among other things.[3] However, she recommended that McMaster adopt additional guardrails, given the potential of harm associated with AI. For example, McMaster did not fully consider the source of the training data, how Respondus may use the data for system improvement purposes, and the risk of biased outcomes. Based on the Report, below is a list of some recommendations to consider when adopting an AI tool:[4]

1. **Documents regarding the collection, use, and disclosure of personal information should be accessible and easy to understand.**

Any notices regarding the collection, use, and disclosure of personal information involving AI tools should be prepared and posted in a clear and comprehensive manner. Those affected should be able to understand how their personal information will be handled.

2. **Contracts with vendors should adequately protect personal information.**

Vendors should be restricted from using personal information for unauthorized purposes. This includes restricting vendors from using personal information for system improvement purposes, algorithm training purposes, and disclosing personal information to subcontractors for research purposes, without the consent of affected individuals.

3. **Additional guardrails should be in place to mitigate risks and govern the adoption of AI tools.**

AI can produce flawed output, and its algorithms could use data from unknown and inaccurate sources. Thus, an AI system's outputs can be difficult for an affected individual to understand or challenge. Respondus software, for example, looks for and flags academic misconduct, which if falsely detected, can have devasting consequences for a student. It is important to fully understand the risks with relying on AI and implement effective guardrails to mitigate such risks. The following guardrails should be considered:

- Conduct an algorithmic impact assessment (AIA) to assess and mitigate the potential risks and impacts associated with the deployment of an AI tool. In the Report, the Commissioner recommended conducting an AIA in addition to a privacy impact assessment.
- Meaningfully engage with affected parties, including those from vulnerable and historically marginalized groups and those with relevant expertise. This can help inform how the underlying algorithms of an AI tool work, and their potential adverse impact on communities.
- Provide opportunities for individuals to opt-out of using AI tools wherever possible. This can help accommodate individuals including those with serious apprehension about AI-enabled tools and the impact this can have on them and their personal information.
- Build an appropriate level of human oversight over the AI tool so that the accuracy of the data used by the tool can be verified, and any decision inferred or generated through AI can be validated.
- Ensure that any data used by the vendor to train its algorithms is obtained in compliance with applicable laws.

The Commissioner's guidance reminds us that while AI tools can offer significant benefits, without effective governance, they can pose heightened risks. Organizations should consider a thorough and thoughtful governance approach to help mitigate risks posed by AI.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

[1] Privacy Report, PI21-00001.

[2] Government of Ontario, "Ontario's Trustworthy Artificial Intelligence (AI) Framework", online: <https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework>.

[3] Privacy Report, PI21-00001 at para 138.

[4] Privacy Report, PI21-00001.

For more information or inquiries:

Vipal Jain

Toronto
416.619.6294

Email:
vjain@weirfoulds.com

Vipal's practice focuses on privacy and technology matters. She advises organizations across various sectors on matters relating to privacy law compliance, technology contracting, cybersecurity incidents and artificial intelligence.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035