WeirFoulds LLP

# Bill 194 – How Public Sector Institutions Should Prepare For It

December 20, 2024

By James G. Kosa, Vipal Jain

Bill 194, which introduces cybersecurity and artificial intelligence (AI) requirements in Ontario's public sector, received Royal Assent on November 25, 2024. Now that this is the law, the question turns to compliance. How should public sector institutions move forward with Bill 194 compliance in mind? In this article, we explain how institutions can prepare to comply with this law.

Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act* was tabled by the Ontario government in May 2024. It amends Ontario's *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and introduces a new legislation called the *Enhancing Digital Security and Trust Act, 2024* (the "**EDSTA**"). A summary of the key provisions and highlights of Bill 194 are found in our previous article from May 31st, 2024. At a high level, the Bill establishes new requirements regarding cybersecurity and artificial intelligence in Ontario's public sector, expands the powers of the Information and Privacy Commissioner of Ontario ("**IPC**"), and enhances privacy protections including protections for minors.

Many of the provisions of Bill 194 are not yet in force. The EDSTA and most of the FIPPA amendments will come into force at a future date proclaimed by the Lieutenant Governor.

**Key Amendments: What Has Happened Since May?**

As a whole, the version of Bill 194 that went on to receive Royal Assent is substantively similar to the version that was introduced by the provincial government in May. The only significant amendment since its First Reading is to the definition of "public sector entities", which was edited under the EDSTA to now exclude "the Assembly". This means that the Bill 194 provisions regarding cybersecurity and AI systems do not apply to the Legislative Assembly of Ontario.

Notably, many of the concerns that were raised about the Bill, including concerns raised by IPC have not been addressed. For example, the IPC's written submissions about the Bill raised concerns that the Bill leaves critical rulemaking for future regulations and recommended having guardrails around the use of AI explicitly within the statute. The Bill does not reflect this, which creates uncertainty as to the scope of the impact on public sector institutions.

**Recommendations For Public Sector Entities to Get Ahead with Bill 194 Compliance**

Some of the changes proposed by Bill 194 are industry practice even though they were not previously required by law. Bill 194 introduces mandatory breach reporting, which already exists under other Canadian privacy laws such as the federal private sector privacy legislation. Other provisions of Bill 194 introduce new obligations which may require updating processes, policies and having appropriate tools in place:

1. **Mandatory Privacy Impact Assessments (PIAs)**

Bill 194 requires institutions to conduct PIAs before collecting personal information. The PIA must address for example, the legal authority for the intended collection, the types of personal information being collected, a clear rationale for why personal information is being collected and used, and a summary of any risks to the individual, among other things.

To prepare, institutions should develop a process for conducting PIAs that is tailored to their specific operational needs. Building and implementing a policy for conducting PIAs can be beneficial. A useful reference for this would be the OPC's Guide to the Privacy Impact Assessment Process.

While conducting PIAs has been common practice for many of our public sector clients, this is something our team can assist with.

2. **Enforcement**

Bill 194 strengthens IPC's role as a regulator. This includes granting it the power to review the information practices of an institution if a complaint has been received or if the IPC has reason to believe the institution has not complied with FIPPA. The IPC would have the power to order the institution to discontinue or change its information practices, return or destroy personal information collected, and implement a different information practice.

To prepare, institutions should strengthen their internal compliance processes. This entails reviewing and updating internal policies as necessary, ensuring roles and responsibilities associated with compliance are clear and having appropriate safeguards in place such as a robust protocol for identifying, assessing, and timely reporting breaches. Institutions should have a process in place to ensure that breaches that reach the threshold of "real risk of significant harm" are reported to affected parties and the IPC. Institutions should create an internal tracking system for all breaches and file an annual report to the IPC that includes both threshold and non-threshold breaches. It will be interesting to see how institutions operationalize the tracking of non-threshold breaches, given the challenges in interpreting the term.

3. **Use of AI systems**

Bill 194 requires institutions using AI systems (as prescribed by regulation) to disclose their use of AI systems to the public, develop and implement an accountability framework applicable to their use of the AI systems and take steps to manage risks associated with the use of AI systems.

To prepare, institutions using AI systems that are subject to these requirements will need to update their external policies/notices to provide information to the public about their use of AI systems. Institutions should implement risk management strategies to identify, assess and mitigate potential risks associated with AI systems. The extent of future regulations on AI will dictate the level of work required to prepare for these changes.

While many of our existing public sector clients are already preparing AI policies, this requirement goes a step further by mandating policies specific to the institution's use of particular AI systems as opposed to a general AI policy.

4. **Cybersecurity requirements**

Bill 194 authorizes the government to create regulations requiring public sector entities to develop and implement cyber security programs. The government may also set technical standards and issue directives related to cyber security; and require reports to be submitted to the Minister regarding incidents related to cyber security. The term "incident" remains undefined.

While many of these requirements are left to regulations, institutions can take proactive steps to ensure they have appropriate physical, technical, and administrative safeguards in place to reduce the risk of an incident. This includes implementing industry

standard measures such as encryption, access controls, and periodic assessments to evaluate the effectiveness of existing safeguards and adjust them as needed to address emerging risks.

Being overly prescriptive about security measures can present challenges, as industry standards evolve overtime to address emerging threats. It will be interesting to see how the government, through regulation, seeks to balance the need for clear minimum standards with the risk of imposing overly rigid requirements that could compel public sector institutions to adopt outdated or inadequate controls.

*We are currently helping our public sector clients with their compliance efforts. If you have any questions about Bill 194 or need assistance with compliance, please contact us.*

***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.***

For more information or inquiries:


## James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

## 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.