Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

Submitted to: Ministry of Public and Business Service Delivery

Submitted by: Ontario Bar Association

Date: June 10, 2024

ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

L'ASSOCIATION DU BARREAU DE L'ONTARIO
Une division de l'Association du Barreau canadien

Table of Contents

Executive Summary 3
Ontario Bar Association 3
Comments & Recommendations 4
Details Left to Regulations 4
Comments on the Enhancing Digital Security and Trust Act, 2024 4
Comments on Freedom of Information and Protection of Privacy Act Amendments 5

Executive Summary

The Ontario Bar Association ("**OBA**") welcomes the opportunity to make a submission on *Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* ("***Bill 194***"). We commend the government for taking action on Artificial Intelligence ("**AI**"). The adoption and use of AI are inevitable, and it is important to put necessary safeguards in place to protect the public and clarify the ground rules for its use. We have provided a short submission on this Bill and look forward to the opportunity to comment on the corresponding regulations where many details will surface.

Ontario Bar Association

Established in 1907, the OBA is the largest and most diverse volunteer lawyer association in Ontario, with close to 16,000 members, practicing in every area of law in every region of the province. Each year, through the work of our 40 practice sections, the OBA provides advice to assist legislators and other key decision-makers in the interests of both the profession and the public and we deliver over 325 in-person and online professional development programs to an audience of over 20,000 lawyers, judges, students, and professors.

This submission was prepared and reviewed by members of the OBA's Business Law, Child & Youth Law, Municipal Law, and Privacy and Access to Information Law sections. Members of these sections include barristers and solicitors in public and private practice in large, medium, and small firms, and in-house counsel across every region in Ontario.

Comments & Recommendations

Details Left to Regulations

The OBA has previously commented on the increased tendency to defer significant details of new Bills to future regulations. There are principled and practical concerns with this approach. Firstly, it removes the oversight and debate that occurs when a Bill is moved through the Legislature. Virtually all the substance of *Bill 194* will come out through Lieutenant Governor in Council regulations, Minister's regulations, and Minister's directives. While we recognize that regulatory authority is necessary to remain agile and responsive to evolving technology, the breadth of details left to future regulations, which will pass outside of the Legislature, is significant. Secondly, this approach makes it difficult to provide useful feedback during the current consultation period, as we do not know what the future regulations and directives will prescribe. We strongly urge the government to alter this trend by putting more substantive details in the legislation, and only leaving provisions that require flexibility to the regulations.

Comments on the *Enhancing Digital Security and Trust Act, 2024*

Bill 194 in its current form essentially creates a set of minimum standards for the use of AI by public institutions. The legislation and the accompanying regulations must ensure that the goal of creating a standardized set of rules accounts for the differences between public institutions. Public institutions vary significantly in size and the volume of documents they deal with, and *Bill 194* should recognize and account for these differences in its requirements.

Bill 194 should avoid restricting public lawyers on the tools they can use compared to private lawyers. Many public institutions engage with, contract with, or retain private sector entities and lawyers. If a public institution contracts with private sector employees, for example by using external counsel using AI, would the institution need to impose restrictions on external counsel? Will public sector lawyers need to work differently, or

have more limits on the use of AI than their private sector counterparts? These are questions that will need to be considered when implementing *Bill 194* and the expected future legislation on AI use in private institutions. The government must also ensure that the definition of AI is not overly broad in scope. Commonly used tools could potentially be captured by a broad definition of AI, including things as mundane as predictive typing in emails. The scope of AI captured by this regime can be broader than what this legislation is designed for, and the government should take care in avoiding unintended consequences that would come with an overly broad definition of AI.

Reporting requirements on the use of AI must also include a necessary carveout for privileged information, and sensitive and confidential information. This type of information should be outside of the scope of disclosure requirements.

Comments on *Freedom of Information and Protection of Privacy Act* Amendments

The risk mitigation provision proposed for subsection 38(4) requires an institution to take steps (i) to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and (ii) to mitigate the risks to individuals in the event of such an occurrence. These steps are required to be taken (a) before collecting the personal information, or (b) if it is not possible to implement the steps before collecting the personal information, within a reasonable time after collecting the information. The use of the term "within a reasonable time" is ambiguous and should be clarified. What could be considered a reasonable time can vary between different organizations and purposes, so a standard timeline may not be optimal, but clarity would be helpful to avoid interpretation disputes.

The requirement to prepare a written assessment on the use of personal information should apply prospectively, and not retroactively. Though retroactive application is not explicitly mentioned, we note that it would be difficult or impossible for institutions to

apply this requirement to existing databases and records that can include hundreds of thousands of documents. Any obligation to make assessments on existing information that has been collected for decades would impose unreasonable administrative burdens on institutions. Additionally, adequate time needs to be given to institutions to comply with the requirements. The *Accessibility for Ontarians with Disabilities Act* can be used as an example, where new requirements were implemented but deferred to provide institutions the time necessary to come into compliance with the Act.

Subsection 40.1, the breach of privacy safeguards and the time limit for complaints, incorporates discoverability into the limitation period. Complaints must be filed with the Commissioner within one year after they come to the attention of the complainant or should reasonably have come to the attention of the complainant, whichever is shorter. For institutions, they are required to notify an individual of any theft, loss, or unauthorized use of personal information if it is reasonable in the circumstances to believe that there is a real risk of significant harm. These two provisions read together can create uncertainty, as the substantial harm is the basis of the disclosure obligation. An institution's data could be breached, but substantial harm may not materialize until a later time – it is unclear whether the shorter of the date the substantial harm was known or ought to have been known would apply in these cases.

In terms of what constitutes a "real risk of significant harm", subsection 40.1(7) includes factors like the sensitivity of information, the probability that the personal information has been or will be misused, the availability of steps an individual could take to reduce the risk of harm occurring and mitigate the harm. The inclusion of steps an individual could take to reduce the risk of harm or mitigate harm is circular. These factors are used to assess whether an institution needs to disclose a breach to an affected individual, but an individual would not be able to mitigate the risk of harm when they are not made aware of it.

Consideration should also be given to how these provisions will interact with the *Limitations Act* if an individual wants to pursue a tort action for damages. There may be a need for an ultimate limitation period like the one in place in the *Limitations Act*. An ultimate limitation period would provide clarity for both the individual and institution in knowing when an issue has expired.

The whistleblowing provision in section 57.1 is well-intentioned but needs additional tweaking to effect the policy goal of providing protections and guarantees to whistleblowers. The provision currently says that any person with reasonable grounds to believe an institution has or is about to contravene the Act may notify the Commissioner and request that their identity be kept confidential. Replacing the term "reasonable grounds" with "reasonable belief" (in good faith) would be better language to protect whistleblowers. There is also a disconnect between an individual requesting that their information be kept confidential, and the Commissioner providing an assurance to that end. Assurances should be automatic to avoid discouraging individuals from whistleblowing out of fear that their request will be subsequently denied. Lastly, the Ministry should turn its mind to how individuals could be identified without their explicit personal details being made public. It is possible to identify an individual by the information disclosed, if it is only known by a small number of individuals. The Commissioner should be required to keep whistleblower information confidential, including indirect ways of attribution, and this information should not be compellable by the Commissioner.

We appreciate the government's intention in providing guidance on the use of AI in public institutions and look forward to seeing the regulations that will provide the details on the regime.

***

The OBA would be pleased to discuss this further and answer any questions that you may have.