Bill 194 - The new Enhancing Digital Security and Trust Act, 2024 and changes to Ontario's Freedom of Information and Protection of Privacy Act

May 14, 2024

Introduction

On May 13, 2024, the Government of Ontario tabled Bill 194, which introduced the *Enhancing Digital Security and Trust Act, 2024* (the EDST Act) and amendments to Ontario's long-standing public sector privacy law, the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Key takeaways

- Bill 194 will have a significant impact on institutions across the provincial and municipal public sectors, though it only proposes amendments to FIPPA and not MFIPPA.
- Bill 194 will align FIPPA with more modern privacy legislation and formalize the IPC's powers and create entirely new law that governs cyber security, artificial intelligence and children's privacy.
- The comment period for Bill 194 is open until June 11, 2024.

Analysis

The proposed EDST Act

The EDST Act will apply across the provincial and municipal public sectors, including to school boards, school authorities, children's aid societies, colleges, universities and hospitals.

Cybersecurity

The EDST Act will give the government the ability to enact regulations that require public sector entities to have cybersecurity programs that include elements relating to the assignment of internal responsibility, education awareness, incident response and program oversight. It will also give the Minister of Public and Business Service Delivery the ability to establish technical standards and issue cyber security directives. Standards and directives may be issued without notice and without consultation.

The EDST Act will give the government the ability to enact regulations requiring public sector entities to submit cyber security incident reports and set requirements for such reports. This contemplates a *bona fide* cyber incident reporting obligation, which is different than a privacy breach reporting obligation and most likely to be triggered at the outset of a cyber attack.

AI regulation

The EDST Act will introduce artificial intelligence (AI) regulation, imposing obligations that apply to the use of "artificial intelligence systems" in circumstances that will be prescribed by regulation. The definition of AI, likely to be much discussed, is as follows:

a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual.

For such systems:

- Public sector entities will be required to publish information about their use;
- Public sector entities will be required to develop and implement an accountability framework; and
- Public sector entities will be required to manage risks associated with their use of an AI system.

All these obligations will be detailed in regulation, which will also give government the ability to require the use of AI systems in accordance with regulation and prohibit the use of certain AI systems altogether. The EDST Act will also require the appointment of an individual to oversee the use of AI systems and meet other stipulated obligations.

Regulation of technology affecting minors

Finally, the EDST Act will also give the government the power to enact regulation governing the processing of minors' information by children's aid societies and school boards. These regulations will:

- Govern how "prescribed digital information" relating to minors is collected, used, and disclosed by children's aid societies and school boards;
- Require children's aid societies and school boards to file reports regarding their collection, use, and disclosure of prescribed digital information relating to minors
- Prohibit the collection, use, and disclosure of certain prescribed digital information relating to minors.

Regulations may also set technical standards respecting prescribed digital information and the making of digital technology available to individuals under age 18. "Prescribed

digital information" is not defined, but the government backgrounder states, "These protections would help prevent inappropriate data practices in our schools and ensure that applications support the health and well-being of all students. They would also help ensure digital tools for children are safer, such as by restricting software used in schools on school issued devices, like laptops, that do not meet certain standards."

Changes to FIPPA

Bill 194 introduces new breach reporting, privacy impact assessment (PIA), and information security requirements into FIPPA. It also formalizes the power of the Information and Privacy Commissioner of Ontario (the IPC) to investigate privacy compliance, granting the IPC new order making powers.

Breach reporting and notification requirements

Bill 194 will introduce privacy breach reporting and notification with the following features:

- **RROSH threshold** : Bill 194 uses the "real risk of significant harm" (RROSH) threshold for reporting and notification – that is, FIPPA institutions will be required to report to the IPC and notify affected individuals if there is reason to believe there is a RROSH in all the circumstances. This is the same standard featured in the federal and Alberta consumer privacy statutes for years and like that now embedded in other public sector privacy statutes – *i.e.*, it is aligned with the Canadian norm.
- **Reporting and notification together:** FIPPA institutions will be required to report and notify if the RROSH threshold is met.
- **Recordkeeping** : FIPPA institutions will be required to keep a record of every theft, loss or unauthorized use or disclosure of personal information that it reports the IPC (and not other privacy breaches, notably).

Bill 194 also introduces a requirement to file an annual report regarding the organization's breaches, similar to the requirement in Ontario's health privacy law. Entities will be required to submit an annual report to the IPC that summarizes the number of thefts, losses, or unauthorized uses or disclosures of personal information. All breaches, regardless of whether they meet the RROSH standard, are caught by this annual reporting requirement.

Privacy impact assessments

Bill 194 will introduce a requirement for institutions to conduct privacy impact assessments (PIAs) before collecting personal information "unless the regulations provide otherwise." Bill 194 stipulates that a PIA must include the following information:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.

3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended be collected.
5. The position titles of the officers, employees, consultants or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution...
8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 40 (5) and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,
    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.
10. Such other information as may be prescribed.

Bill 194 will require institutions to keep their PIAs current and implement any additional steps in the event that they make significant changes to the purposes for which they process personal information.

These provisions will arguably require institutions to assess existing systems and processes unless relief is granted by way of regulation.

Requirements regarding safeguards

Bill 194 will introduce an express requirement for institutions to implement reasonable safeguards to protect personal information from theft, loss, and unauthorized use or disclosure, and to protect against unauthorized copying, modification, or disposal. This will supplant the existing duty to secure records from unauthorized access that is set out in the FIPPA regulation, which the IPC has held varies based on "the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them."

New order making powers

Bill 194 will formalize the IPC's privacy compliance investigation powers, which it currently drives from its powers as a legislative officer (and which are immunized from judicial; review). Bill 194 will give the IPC the power to conduct complaint based and proactive reviews of an institution's information practices. After having conducted a review and having heard from the entity, the IPC will be able to issue compliance orders – including an order to "change [an] information practice." Finally, Bill 194 will provide for confidential "whistleblower" reports to be made directly to the IPC, barring the IPC from revealing the identity of a confidential informant.

Conclusion

Bill 194 will have a significant impact on institutions across the provincial and municipal public sectors, though it only proposes amendments to FIPPA and not MFIPPA. It will align FIPPA with more modern privacy legislation and formalize the IPC's powers and create entirely new law that governs cyber security, artificial intelligence and children's privacy.

Despite its significance, the substance of the EDST Act will be mainly left to regulation and directive. This structure will leave government with significant powers, which the current draft allows for exercise without notice or comment.

The government has invited comment on Bill 194. The comment period is open until June 11. Should you wish to discuss the Bill with a view to commenting or otherwise, please reach out.

Upcoming webinar on Bill 194 > May 23 | 12 p.m. - 1 p.m. ET

Join the members of our Ontario privacy and cybersecurity team on May 23 for an early look at this critical development – What might it mean? What are the key questions left to be resolved? What to do today? If you are not on our mailing lists and would like to register, **please click here** .

By

Daniel J. Michaluk, Marc Vani, Shane Morganstein, Eric S. Charleston

Expertise

Cybersecurity, Privacy & Data Protection, Artificial Intelligence (AI)

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749