Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

June 24, 2024 ***VIA ELECTRONIC MAIL & ONLINE SUBMISSION***

Meghan Stenson, Clerk of Procedural Services
Procedural Services Branch
Whitney Block
Room 1405
99 Wellesley St. W
Toronto, ON M7A 1A2

Dear Meghan Stenson,

RE: Written Submission on Bill 194: *Strengthening Cyber Security and Building Trust in the Public Sector Act*, *2024*

I am writing regarding Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*, 2024, currently at Second Reading before the Legislative Assembly of Ontario. With the legislature in recess, I am providing my office's submission for distribution to the committee that will be charged with studying Bill 194 once members return on October 21, 2024.

Bill 194 is a crucial piece of legislation. If passed, Schedule 1 will establish cyber security and artificial intelligence (AI) system requirements for public sector entities and rules for the use of digital technologies affecting children and youth under eighteen. Schedule 2 amends the *Freedom of Information and Protection of Privacy Act* (FIPPA) to introduce new privacy protections and strengthen oversight.

As Ontario's Information and Privacy Commissioner, I am an independent Officer of the Legislature mandated to protect individuals' privacy and access to information rights. I commend the government for addressing the modern needs of Ontarians who face pervasive cybersecurity threats, escalating use of AI, and serious online privacy risks and harms, particularly our children and youth.

This bill rightly focuses on the critical areas affecting the well-being of Ontarians in an increasingly digitized world. It aligns with other global legislative reforms aimed at addressing rapid technological advancements and their broader societal impacts. We are at a critical moment in time, at a crossroads between risks and opportunities, where the decisions we make today will definitively shape our future for generations to come.

The IPC has worked actively to ensure Ontarians' privacy and access rights are considered and respected as we navigate this pivotal juncture. We have focused on preparing Ontarians for their digital future and, in collaboration with federal, provincial, and territorial counterparts, have called for stronger privacy safeguards and transparency. Recognizing the rise of AI, we have collaborated nationally and internationally on AI-related resolutions, policy positions, and law reform recommendations in public, health, and employment contexts.

Future-proofing Ontario's access and privacy laws has never been more important. Modern and effective laws are critical for heightening the level of accountability, transparency, and oversight needed to protect rights and maximize opportunities in a rapidly changing world. In the following

submission, I offer several recommendations to strengthen Bill 194 and fill important gaps in the government's current proposal. In summary, these recommended changes focus on three main themes:

1. Take a principles-based approach to govern novel areas of high-risk activity, such as artificial intelligence, that impact how Ontarians live, work and interact with public institutions. Such principles should be explicitly set out in law and reflect our collective commitment to fundamental human rights and the shared values that underpin our free and democratic society. These principles should establish the guardrails around the development and use of new technologies, ensuring that they serve to benefit society and support human flourishing.

2. Ensure greater transparency around how the government proposes to regulate cybersecurity, artificial intelligence, and digital technologies available to children and youth under 18. By engaging in public consultations and being more inclusive and transparent about its process of rulemaking, the government can create more effective regulations that are relevant to the needs and realities of different groups and communities. Ultimately, this would provide public institutions with clear, certain, and predictable rules they can better understand and apply in practice, and within which they can more safely and responsibly innovate.

3. Strengthen the accountability and independent oversight of public sector entities to ensure compliance with the proposed new rules. This includes ensuring recourse for any Ontarian who reasonably believes their privacy and human rights have been violated and protecting whistleblowers who speak out from reprisal. A system of oversight and enforcement that is coherent, streamlined and independent of government will build trust in public institutions that use technologies responsibly and ensure economic and social prosperity for all Ontarians.

SCHEDULE 1 OF BILL 194:
ENHANCING DIGITAL SECURITY AND TRUST ACT, 2024

The legislation, as drafted, would establish significant regulation-making powers in respect of cyber security, AI systems, and digital technologies affecting individuals under the age of 18. The IPC agrees that these areas of societal activity pose high risk to Ontarians' privacy and human rights and require urgent government intervention. However, as currently worded, Schedule 1 of Bill 194 lacks the statutory protections needed to protect with privacy and human rights, and fails to provide the level of transparency and accountability that are necessary to secure Ontarians' trust in how the government will effectively govern these high-risk areas.

The following recommendations aim to advance the underlying policy objectives of Schedule 1 by providing Ontarians with necessary assurances that their privacy and human rights matter, that clear and transparent principles exist to govern institutions' decisions and actions, and that an effective system of oversight ensures these are properly enforced.

A. General recommendations for Schedule 1

Schedule 1 should include a purpose clause

The proposed *Enhancing Digital Security and Trust Act* does not contain substantive statutory rules governing the collection, use, disclosure, and retention of personal information in the context of cyber security incidents, AI systems, or digital technologies affecting children and youth. It does not explicitly set out how such personal information will be protected and independently overseen, nor does it provide the level of transparency that Ontarians expect and deserve from their public institutions.

The preamble to the *Enhancing Digital Security and Trust Act* recognizes "the importance of protecting the privacy of the people of Ontario and the value of enhancing Ontario's privacy safeguards through increased transparency and independent oversight." However, a preamble alone does not have the force of law. It will not establish substantive individual or group rights, or define a public body's duties and obligations to protect these rights. Moreover, courts may be inconsistent in interpreting preambles, resulting in even less clarity or predictability for institutions and the public.

A purpose clause, on the other hand, can provide greater reassurance to Ontarians about how the legislation will be interpreted and establish clearer guardrails to protect Ontarians' privacy and human rights.[1] The IPC recommends including a purpose clause at the outset of the Act that would make more explicit the government's legislative intent and provide clear guiding principles on how the Act should be interpreted and applied.

[1] In her submission on Bill 194, Prof. Teresa Scassa also recommended that the government introduce a purpose clause into the legislation with clear articulated principles to guide the adoption and use of AI in the broader public service: "The purpose of this Part is to ensure that artificial intelligence systems adopted and used by public sector entities are developed, adopted, operated and maintained in manner that is transparent and accountable and that respects the privacy and human rights of Ontarians." .

Recommendation 1: Amend Schedule 1 to include the following purpose clause:

> ***[X] The purpose of this Act is to establish a governance framework for public sector entities in relation to cyber security activities, use of artificial intelligence systems and deployment of digital technologies affecting individuals under the age of eighteen, in accordance with the following principles:***
>
> ***(a) the privacy of individuals and groups must be protected, and the collection, use, retention, and disclosure of their personal information must be limited to that which is necessary and proportionate for the purpose;***
> ***(b) public sector entities must be transparent in fulfilling their obligations under this Act to the extent reasonable and appropriate, without jeopardizing the security and integrity of government information systems;***
> ***(c) artificial intelligence systems must be valid, reliable and safe, they must be designed to protect privacy and affirm human rights, and public sector entities that use them must be accountable and transparent;***
> ***(d) the creation and implementation of standards for digital technologies affecting individuals under age 18 must respect the rights of children and youth and be consistent with the values of personal autonomy, dignity, and individual self-determination; and***
> ***(e) compliance with the provisions of this Act and its regulations should be reviewed independently of government.***

The act should be subject to independent oversight and enforcement

Schedule 1 would see the government regulate a host of digital technologies that involve the collection, use, retention, and disclosure of Ontarians' personal information which falls squarely within the rest of the domain of the IPC. It vests exclusively in government the responsibility of overseeing public sector compliance with the rules and directives yet to be established, with no statutory provision for enforcement and no consequences in the event of non-compliance. This self-governing model is not what Ontarians would reasonably expect to regulate such high-risk areas of activity impacting their fundamental human rights. As with other public sector activities having such direct and consequential impact on Ontarians' lives, oversight and enforcement must be carried out independently of government.

We recommend therefore, that Schedule 1 be amended to include statutory language explicitly referencing the IPC's independent oversight and enforcement role, which continues in respect of any privacy and access rights that may be engaged through the types of cyber security, AI, and digital technology programs envisaged by the act.

Recommendation 2: Amend Schedule 1 to explicitly acknowledge the IPC's independent oversight role and responsibilities by adding the following clause:

> ***[X] The Information and Privacy Commissioner shall have all the powers, duties, and functions currently established by the Freedom of Information and Protection of Privacy Act, the Municipal Freedom of Information and Protection***

of Privacy Act, the Personal Health Information Protection Act, the Child, Youth and Family Services Act, and other legislation which assigns it powers, duties, and functions in relation to regulated public sector entities subject to this Act.

Regulation-making under the act should be subject to public consultations

Significant portions of the proposed legislation are being deferred to regulation. This includes substantive, values-based rules intended to govern the deployment and adoption of AI systems and digital technologies made available to children and youth. For the reasons discussed below, we strongly believe such higher-order rules and principles that reflect important societal values should be codified in the statute itself. To the extent that the government will still use regulations to flesh out more technical rules and requirements in greater detail then, at a minimum, these rules and regulations should be made transparent and subject to public consultation.

Further, the minister should be accountable for considering Ontarians' views and comments, particularly of those disadvantaged or marginalized groups or populations who otherwise tend to be absent from the rule-making process. The explicit requirement to hold public consultations before adopting regulations and to consider the diversity of Ontarians' views could be modelled after similar provisions that exist under current laws, such as section 74 of the *Personal Health Information Protection Act* (PHIPA). Therefore, we recommend that a mandatory public consultation mechanism be included in Schedule 1 of Bill 194 to ensure that the minister considers Ontarians' views and comments before adopting regulations on such consequential matters impacting their fundamental rights.

Recommendation 3: Amend Schedule 1 to require a prescribed public consultation process before adopting regulations under the act. Such a requirement should be modelled after section 74 of PHIPA.

The minister should consult with the IPC prior to making (or proposing) regulations or issuing directives that may impact privacy or access rights

Schedule 1 empowers the government to make regulations (either directly or through the Lieutenant Governor in Council) and issue directives in respect of cyber security programs, use of AI systems, and deployment of digital technologies affecting individuals under 18. Such regulations and directives will inevitably overlap with existing rules governing records and personal information within the custody or control of public sector entities under Ontario's access and privacy laws subject to the IPC's oversight. As such, public sector entities may face potentially duplicative, or worse, divergent, rules and directions.

We recognize that section 14 of Schedule 1 proposes to resolve potential conflict as follows: "If a provision of this Act or the regulations made or directives issued under this Act conflicts with a provision of any other Act or regulation, the provision in the other Act or regulation prevails." However, we believe more should be done to minimize the likelihood of conflicting rules arising in the first place. The aim should be to avoid duplication and minimize the risk of confusion and inconsistency among public sector entities that could lead to inadvertent non-compliance and potentially frustrate the policy objectives of the bill.

We recommend that Schedule 1 be amended to require the minister to consult with the IPC before adopting or proposing regulations, or issuing directives that may impact access or privacy rights. This would be similar to existing provisions in other Ontario laws requiring this mandatory consultation step with the IPC and have the benefit of ensuring that consistent rules and directives are set for public sector entities. (See for example, sections 55.4(2)-55.4(3) of PHIPA that could be adapted accordingly).

Recommendation 4: Amend Schedule 1 to require the minister to consult with the IPC before proposing or adopting regulations, or issuing directives that may impact Ontarians' access or privacy rights. Such an amendment should be modelled after sections 55.4(2)-55.4(3) of PHIPA.

Ministerial directives should be transparent to the public

An essential objective of Schedule 1 is to enhance public trust in how public sector entities secure their information systems from cyber security risks and deploy digital technologies affecting children and youth. A key component of building trust is ensuring transparency of the directives promulgated by the minister so that Ontarians can understand general features of the regulatory framework and have confidence in its effectiveness.

Greater transparency can also have the positive downstream effect of increasing general public awareness and engagement. This could help Ontarians better understand the nature of the risks involved, ask more informed questions of public institutions they interact with, and become more knowledgeable participants in their own efforts to become digitally aware and protect their personal information online.

As drafted, the *Enhancing Digital Security and Trust Act* exempts ministerial directives from Part III of the *Legislation Act*, including the requirement to publish the directives on the e-laws website and in the *Ontario Gazette*. Schedule 1 does not otherwise require the government to publicly communicate ministerial directives to which public sector entities must conform. We recommend, therefore, that Schedule 1 be amended to require that these directives be made public so that Ontarians can better understand the kinds of actions that public sector entities are required to take and hold them accountable.

Recommendation 5: Amend Schedule 1 to require that the minister's directives be publicly promulgated. Specifically, add new sections following 4(3) and 11(3) of Schedule 1 to read as follows:

4(X) Every directive issued under section 4(1) of this Act,
(a) shall be made available to the public on request; and
(b) shall be publicly posted on at least one Government of Ontario website.

11(X) Every directive issued under section 4(1) of this Act,
(a) shall be made available to the public on request; and
(b) shall be publicly posted on at least one Government of Ontario website.

Schedule 1 should include a whistleblower provision

A compliance regime purporting to regulate high-risk activities, such as those proposed by Schedule 1 of Bill 194, sometimes depends on the courageous actions of individuals working within public sector entities to come forward with information or allegations of errors or omissions of their peers or superiors. For employees to feel sufficiently secure in bringing forward important information necessary for upholding the integrity of the compliance regime, including the prescribed reporting requirements, they need assurances of confidentiality and non-reprisal. We recommend, therefore, that Schedule 1 be amended to include explicit protection for whistleblowers.

Although section 10 of Schedule 2 of Bill 194 introduces a whistleblower provision, it would only apply to provincial institutions and only in respect of alleged contraventions of FIPPA and its regulations. Section 10 of Schedule 2 would not cover all the other public sector entities, including institutions under MFIPPA, children's aid societies, or school boards and would not apply to alleged contraventions of Schedule 1 or its regulations.

Recommendation 6: Amend schedule 1 to include explicit protections for whistleblowers.

Whistleblowing
[X] (1) Any person who has reasonable grounds to believe that a public service entity or any other person has contravened or is about to contravene this Act or the regulations, including a directive under this Act, may notify the Commissioner or an officer designated by the minister of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality
(2) The Commissioner or the officer designated by the minister must keep confidential the identity of a person who has notified them under subsection (1) and to whom an assurance of confidentiality has been provided.

Non-Retaliation
(3) No one shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage a person by reason that,

- ***(a) the person, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner or the officer designated by the minister that any other person has contravened or is about to contravene a provision of this Act or its regulations, including a directive;***
- ***(b) the person, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene a provision of this Act or its regulations, including a directive;***
- ***(c) the person, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of a provision of this Act or its regulations, including a directive; or***

(d) any person believes that the person will do anything described in clause (a), (b) or (c).

Penalty
(4) Every person who contravenes subsection (3) is guilty of an offence and on conviction is liable to a fine not exceeding $5,000.

B. Recommendations specific to the cyber security portion of Schedule 1

Public sector entities are increasingly being affected by a sharp rise in cyber security incidents, including ransomware attacks. According to the Canadian Centre for Cyber Security, malicious actors are increasingly targeting critical infrastructure and public services.[2] Institutions in the municipal, university, school, and hospital sectors are at particularly high risk of cybercrime, posing grave threats to Ontarians' most sensitive personal information,[3] potentially disrupting critical or life-saving public services,[4] and forcing the diversion of millions of taxpayer dollars to restore these services,[5] sometimes with limited success.[6]

Governments are rapidly moving to enhance the cyber security governance of public institutions and the protections afforded to their constituents.[7] The IPC supports the government's policy intent of building out a cyber security governance regime for Ontarians. However, we believe Schedule 1 can be improved in several respects, particularly regarding cyber security incidents involving personal information.

---

[2] Canadian Centre for Cyber Security. (2022). "National Cyber Threat Assessment 2023-2024." Available at: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.
[3] Canadian Internet Registration Authority. (2023). "Why are municipalities, schools, hospitals and universities still cybercriminals' biggest targets?" Available at: https://www.cira.ca/en/resources/news/cybersecurity/why-are-municipalities-schools-hospitals-and-universities-still-cybercriminals-biggest-targets/.
[4] Jacquelyn LeBel (2024). "More than 325K patient files stolen in cyberattack on 5 southwestern Ontario hospitals", *Global News.* Available at: https://globalnews.ca/news/10399865/patient-files-stolen-cyberattack-southwestern-ontario-hospitals/. Kevin Lamb. (2024). "Area medical clinics partially crippled by 'cyber-security incident'," *Orillia Matters*. Available at: https://www.orilliamatters.com/police-beat/area-medical-clinics-partially-crippled-by-cyber-security-incident-8438750. Hannah Neprash et al. (2023). "We tried to quantify how harmful hospital ransomware attacks are for patients. Here's what we found," *Stat*. Available at: https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/.
[5] The average cost for Canadian organizations to respond to ransomware incidents has risen to more than $1.1 million dollars (CAD) in 2023. See: Nathanial Dove. (2023). "Canadian firms paying 'significantly' more in ransomware attacks: data," *Global News*. Available at: https://globalnews.ca/news/10155151/companies-1-million-ransomware-attacks/.
[6] TELUS's 2022 Canadian Ransomware Study found that 15% of Canadian organizations that suffered a ransomware incident indicated that they were reinfected by the same ransomware attack after recovery.
[7] See, for example: Government of Canada. (2024). "Government of Canada's Enterprise Cyber Security Strategy." Available at: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html. White House. (2021). "Executive Order on Improving the Nation's Cybersecurity." Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. United Kingdom Cabinet Office. (2022). "Government Cyber Security Strategy: 2022 to 2030." Available at: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

Core elements of a cyber security program should be set out explicitly in statute

Securing Ontarians' personal information requires strong and robust cyber security programs. While cyber security programs may have particularities specific to each institution, they should all be required to have common core elements consistent with all programs. For example, Part 2 of the federal government's Bill C-26, the *Critical Cyber Systems Protection Act*, outlines a series of core elements that covered entities must include as part of the cyber security programs mandated by the bill, recognizing that these may be further amplified by way of regulation. These elements constitute best practices which were developed by a range of federal agencies, including Public Safety Canada.

Similar to the approach taken in federal Bill C-26, we recommend that Schedule 1 of Bill 194 be amended to explicitly require regulations to cover certain core elements that must be included in a cyber security program and that these compulsory core elements align with those to be required federally. Recognizing that it may take time for public sector entities to establish these cyber security programs, the government may also consider amending the legislation to include a specific time frame or a specific coming into force date for such programs.

Recommendation 7: Amend section 2(2) of Schedule 1 to ensure that any regulations governing cyber security programs of public sector entities require the inclusion of certain core elements consistently across all programs.

> *Regulations re programs*
>
> *(2) Without limiting the generality of clause (1) (b), a regulation made under that clause ~~may~~* ***shall*** *require that a public sector entity's program include,*
>
> > *[…]*
> >
> > ***(f) identification and management of any organizational cyber security risks, including risks associated with the public sector entity's supply chain and its use of third-party products and services;***
> > ***(g) measures to protect entity cyber systems from being compromised;***
> > ***(h) processes to detect any cyber security incidents affecting, or having the potential to affect, a public sector entity's cyber systems; and,***
> > ***(i) procedures to minimize the impact of cyber security incidents.***

IPC should be notified of cyber security incidents affecting personal information

Much of the substance of the cyber security regime proposed by Schedule 1 is being deferred to regulations. One such requirement to be set out in regulation is for public sector entities to submit reports to the minister (or a specified individual) regarding cyber security incidents. Such reports may require different content depending on various types of incidents. In general, the IPC supports this mandatory reporting requirement that will assist the minister to determine the nature, volume, and severity of incidents impacting public sector entities, assess how cyberthreats are evolving, and make informed resource-allocation decisions to address or mitigate such threats.

Cyber security incidents reported to the minister may involve Ontarians' personal information. Yet the IPC might not be alerted if the reporting entity underestimates the risk that personal information might have been involved. We would recommend therefore, that the minister informs the IPC of significant cyber security incidents reports that involve, or may involve, personal information. With this additional reporting requirement to the IPC in appropriate cases, Ontarians would build further trust that the government is properly considering and handling all aspects of cyber security incidents, including aspects impacting their privacy that might otherwise go unreported. Moreover, it would provide the IPC with a line of sight on possible trends and help ensure that the IPC's expertise can be leveraged in cyber incidents affecting Ontarians' personal information.

Schedule 2 of Bill 194 would amend FIPPA by introducing a mandatory requirement for provincial public sector institutions to notify the IPC of privacy breaches that pose real risk of significant harm (including those arising from cyber security incidents). Service providers are already subject to a mandatory breach notification requirement under section 308(3) of the *Child, Youth and Family Services Act* (CYFSA). However, many other public sector entities under Schedule 1, including all MFIPPA institutions and school boards, have no obligation to report privacy breaches to the IPC. This would continue to be the case after Bill 194 is enacted. To remedy this gap, we recommend that the minister be required to report to the IPC significant cyber incidents involving, or potentially involving, personal information.

Recommendation 8: Amend Schedule 1 to require the minister to provide to the IPC copies of reports it receives from public sector institutions in cases of significant cyber incidents that involve, or may involve, personal information.

[X] The minister shall provide the Information and Privacy Commissioner with copies of reports the minister receives from public sector entities under section 2(1)(c), including reports produced by third parties at the request of public service entities, in respect of significant cyber incidents that involve, or may involve, personal information.

The minister should prepare an annual report on its cyber related responsibilities

The minister has significant regulatory responsibilities regarding cyber related activities covered by Schedule 1. These high-risk activities are of particular interest and concern to Ontarians whose lives may be significantly impacted by them. For Ontarians to have trust and confidence in the way of these activities are being governed, they must be provided with relevant information on the effectiveness of the regulatory regime and how it is being implemented. Accordingly, we recommend that Schedule 1 be amended to include a requirement for the minister to prepare an annual report regarding the cyber incident reports received from public sector entities in a given year. Such a report should inform the legislature and the public of how the minister is implementing his or her responsibilities, the general trends emerging over time, and the overall effectiveness of the regulatory regime. For example, the minister's annual report could include the number of cyber incidents reports received, the types of cyber incidents reported, the number of reports involving personal information shared with the Information and Privacy Commissioner, the general status and outcomes of such incidents, and any significant trends being observed year after year. Other specific elements of the report could be outlined in regulation to ensure that the appropriate level of information is publicly reported without

compromising the integrity of ongoing cyber security investigations or remedial measures underway to enhance the cyber security of public sector entities' systems.

Recommendation 9: Amend Schedule 1 to require the minister to issue an annual report on the number, types, and general outcomes of cyber related incidents reported, any emerging trends observed over time, and other information that may be prescribed in regulation.

C. Recommendations specific to the AI portion of Schedule 1

AI technologies hold the promise of significantly enhancing Ontarians' lives. Public sector use of AI can accelerate the delivery of government services, enhance government decision-making, improve public engagement, and help solve complex societal problems.

Despite their many promises, however, AI systems are not infallible. Setting up AI systems often depends on vast amounts of personal information that may be highly sensitive and may be inappropriately shared with others.[8] They sometimes return inaccurate results for reasons that are nearly impossible to explain and account for.[9] Automated decisions based on information or inferences resulting from AI systems may significantly impact people's lives.[10] They might perpetuate discrimination and bias against historically marginalized groups.[11]

Recognizing both the benefits and risks of AI systems, the IPC, together with the Ontario Human Rights Commission, called on the Ontario government to develop and adopt meaningful guardrails around the responsible use of AI systems. As it stands now, however, Schedule 1 does not include any of the guardrails we recommended in our Joint Statement of May 2023.[12] By deferring the substantive obligations of public sector entities to regulations, the

---

[8] Federal Trade Commission. (2021). "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others". Available at: https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

[9] Conor Dougherty (2015). "Google Photos Mistakenly Labels Black People 'Gorillas'". *The New York Times.* Available at: https://archive.nytimes.com/bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/.

[10] Frances Mao. (2023). "Robodebt: Illegal Australian welfare hunt drove people to despair". *BBC News*. Available at: https://www.bbc.com/news/world-australia-66130105. Anna Holligan. 2021. "Dutch Rutte government resigns over child welfare fraud scandal". *BBC News*. Available at: https://www.bbc.com/news/world-europe-55674146. Jeffrey Dastin. (2018). "Amazon scraps secret AI recruiting tool that showed bias against women". *Reuters*. Available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

[11] Ziad Obermeyer et. al. (2019). "Dissecting racial bias in an algorithm used to manage the health of populations". *Science*. Available at: https://www.science.org/doi/10.1126/science.aax2342. Mary Fetzer. (2023). "Trained AI models exhibit learned disability bias, IST researchers say". *PennState*. Available at: https://www.psu.edu/news/information-sciences-and-technology/story/trained-ai-models-exhibit-learned-disability-bias-ist/. Trishan Panch et. al. (2019). "Artificial intelligence and algorithmic bias: implications for health systems". *Journal of Global Health*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6875681/.

[12] IPC and OHRC. (2023). "Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies". Available at: https://www.ipc.on.ca/en/media-centre/news-releases/joint-statement-information-and-privacy-commissioner-ontario-and-ontario-human-rights-commission-use.

government has adopted an approach similar to that which the federal government initially took in its *Artificial Intelligence and Data Act* which received significant criticism, and ultimately caused the federal government to change its approach to regulating AI technologies. The Ontario government would be wise to heed this cautionary tale.

Fundamental AI principles and guardrails should codified in the statute

The AI-related provisions in Schedule 1 purport to regulate a highly dynamic technology that is still emerging and evolving. Given this, the government has chosen to defer much of its substantive rule-making to regulation. While this approach is understandable in a rapidly changing environment, it is nonetheless essential to establish a principles-based approach that aligns with societal norms and values. Doing so provides a degree of flexibility and agility to adapt rules to changing circumstances while also ensuring that those rules remain grounded within explicit statutory guardrails to protect Ontarians' fundamental human rights.

The IPC strongly recommends that the proposed legislation be amended to include explicit statutory language that sets out the basic parameters within which eventual regulations must be established. By codifying strong normative principles in the statute itself, the public can be assured that a robust, transparent, and principles-based approach will help enable the potential benefits of these powerful technologies while protecting individuals and groups from potential harms. There is growing corpus of laws, policies, and principles around the world to guide AI systems regulation (e.g. OECD AI Principles,[13] United Nations resolution A/78 on the ethics of AI,[14] the G7 Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System,[15] the European Union Ethics Guidelines for Trustworthy AI[16] cited by the European AI Act,[17] Canada's Guiding Principles for the use of AI in government[18] which are aligned with the Digital Nations shared approach to AI,[19] and Colorado's Consumer Protections for Artificial Intelligence[20]). The Ontario government has proposed its own set of principles for the ethical use of AI systems.[21]

As a result of these efforts, there are universal principles clearly emerging worldwide that Ontario could and should enshrine into its AI law. These are reflected in the IPC's and OHRC's

---

[13] OECD. (2024). "OECD AI Principles". Available at: https://oecd.ai/en/ai-principles.
[14] United Nations. (2021). "193 countries adopt first-ever global agreement on the Ethics of Artificial Intelligence". Available at: https://news.un.org/en/story/2021/11/1106612.
[15] G7. (2023). "Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System". Available at: https://www.mofa.go.jp/files/100573471.pdf.
[16] European Commission. (2019). "Ethics guidelines for trustworthy AI." Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[17] European Parliament (2024). "Artificial Intelligence Act. Consolidated Text". Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html.
[18] Government of Canada (2023). "Guiding Principles for the use of AI in government". Available at: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/principles.html.
[19] The Digital Nations is a collaborative forum of the world's leading digital governments composed of Canada, Denmark, Estonia, Israel, Mexico, New Zealand, Portugal, Republic of Korea, United Kingdom, and Uruguay. More information is available at: https://www.canada.ca/en/government/system/digital-government/digital-nations.html.
[20] Colorado General Assembly (2024). "Consumer Protections for Artificial Intelligence." Available at: https://leg.colorado.gov/bills/sb24-205.
[21] Government of Ontario. (2023). "Principles for Ethical Use of AI [Beta]." Available at: https://www.ontario.ca/page/principles-ethical-use-ai-beta.

joint statement of May 2023,[22] and are further discussed below. To ensure a harmonized approach with this growing international consensus, the government should amend Schedule 1 to include similar high-level principles and fundamental rules that public sector entities must follow when developing or deploying AI systems impacting Ontarians. By demonstrating its firm commitment to these principles, Ontario would show itself as a credible and influential leader serious about becoming a global hub for responsible AI capacity and development.

At a fundamental level, public sector entities developing or deploying AI systems must ensure that such systems are:

- ***Valid and reliable*:** Before AI technologies are adopted by public sector entities, the technologies should have to meet independent testing standards for validity and reliability, the details of which could be set out in regulation. Any tested technologies should demonstrably work as intended in the environments in which they will be used. All other statutory obligations should be predicated on this testing, undertaken before the deployment or use of an AI technology and on an ongoing basis afterwards.

- ***Safe*:** AI systems should be configured to support human life, physical and mental health, economic security, and the environment. They should be monitored and evaluated throughout their lifespan to confirm they continue to support these objectives and can withstand unexpected events or deliberate efforts that cause them to behave in harmful ways not intended or anticipated by the developers, operators, or users of these AI systems.

- ***Privacy protective*:** AI technologies should be developed or adopted using a privacy by design approach that anticipates and mitigates privacy risks to individuals and groups. This means, among other things, requiring clear lawful authority to collect, process, retain, and use personal data in relation to AI systems, including training date. Systems must build in measures to ensure the accuracy of AI outputs and protect all inferences about individuals resulting from these outputs that are about individuals as personal information. AI systems must also be designed to protect the security of personal information from unauthorized access or cyber security threats. Individuals should be informed of the intended use of AI technology to process their personal information and, where appropriate, have an opportunity to opt-out of an automated decision in preference for a human decision maker.

- ***Transparent*:** Public sector entities should adopt policies and practices that make visible, explainable, and understandable how AI technologies work. As part of this, public sector entities should retain sufficient technical information about the AI technologies they use so they can provide a full accounting of how decisions are reached. Individuals should be informed of decisions that have been made about them using AI. They should be told when they are interacting with an AI technology and when information presented to them has been generated by AI systems. The level of transparency by public sector entities may vary depending on whether it is directed to the public, individuals or groups directly impacted by AI systems, or regulators charged with overseeing them.

[22] IPC and OHRC. (2023). "Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies." Available at: https://www.ipc.on.ca/en/media-centre/news-releases/joint-statement-information-and-privacy-commissioner-ontario-and-ontario-human-rights-commission-use.

- ***Accountable*:** Public sector entities must develop a robust governance structure for the development, deployment, use, repurpose, or decommissioning of AI systems, with clearly defined roles and responsibilities. They should have to conduct algorithmic impact assessments including PIA's to identify the risks of algorithms and how to mitigate against such risks They should identify and document design and application choices they make in respect of their AI systems, and consequential decisions they make about groups or individuals made using AI outputs. Individuals must be able to challenge the accuracy of decisions made about them and seek recourse when they believe they have been negatively impacted by them. Public sector entities should be subject to review by an independent oversight body with authority to enforce these principles and require the organization to undertake remedial or corrective actions.

- ***Human rights affirming*:** AI technologies should be designed to be fair and equitable. They must respect and affirm human rights for individuals and communities. AI technologies should also be purposefully designed to address and redress historical discrimination and bias so that individuals and communities affected by AI systems do not experience ongoing discrimination based on equal application of logics of a given AI technology or its outputs.

Recommendation 10: Strengthen Schedule 1 by codifying clear statutory principles to serve as guardrails around the responsible use of AI systems by public sector entities. Codifying such guardrails, in addition to the purpose clause proposed under *Recommendation 1* would provide necessary assurances to earn and maintain Ontarians' trust in the use of AI systems. Details could be added through regulations or technical standards, allowing for a more flexible and agile regulatory approach.

A risk-based regulatory approach should be adopted

Several AI regulatory regimes emerging worldwide take a risk-based approach, whereby rules and obligations on organizations developing or deploying AI systems are more or less exacting, depending on the level of risk or potential harms to individuals and groups. As examples, the European Union AI Act,[23] Colorado's Consumer Protections for Artificial Intelligence,[24] the National Institute of Standards and Technology (NIST) AI Risk Management Framework,[25] and Canada's Artificial Intelligence and Data Act (AIDA)[26] in Bill C-27 collectively impose higher requirements and stronger oversight and enforcement measures, commensurate with higher levels of risk or potential harm.

Schedule 1 of Bill 194, insofar as it purports to regulate AI systems developed or adopted by public sector entities, should take a similar risk-based approach. Such an approach would

[23] European Parliament (2024). "Artificial Intelligence Act. Consolidated Text." Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html.
[24] Colorado General Assembly (2024). "Consumer Protections for Artificial Intelligence." Available at: https://leg.colorado.gov/bills/sb24-205.
[25] National Institute of Standards and Technology (2023). "AI Risk Management Framework." Available at: https://www.nist.gov/itl/ai-risk-management-framework.
[26] Government of Canada (2023). "The Artificial Intelligence and Data Act (AIDA)." Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

provide the level of flexibility needed to adopt and deploy AI systems, while providing the commensurate level of protection to individuals and groups in terms of safety and rights.

Recommendation 11: Amend Schedule 1 to explicitly adopt a risk-based framework. Such a framework should assess the potential impact and likelihood of harm associated with different AI systems, ensuring that AI systems with higher risk of unintended harm receive more stringent oversight than those classified as lower risk AI systems.

Certain statutory no-go zones should be specified

Notwithstanding recommendation 11, we believe there comes a clear threshold of risk, or certain harms, beyond which we should not venture as a society. Just as important as prescribing the purposes for which public sector entities may use AI systems within certain guardrails, is to prescribe the purposes for which they cannot use AI systems. Per s. 5(6) of Schedule 1, the government may establish certain prohibited uses of AI technologies through regulation. The IPC supports the creation of clear *no-go zones* that would prohibit public sector entities from using AI technologies in ways that are societally unacceptable or too high risk. We believe certain uses to be so universally rejected by Ontarians that they should be explicitly prohibited in statute today, with others to be prescribed by regulation over time.

Schedule 1 of Bill 194 should clearly and explicitly set out no-go zones for the deployment of AI systems by public sector entities. Article 5 of the EU *Artificial Intelligence Act* codifies a list of prohibited AI practices.[27] We recommend that Ontario consider banning a similar list of uses that would likewise be considered completely unacceptable to Ontarians and are highly unlikely to change over time given our unwavering commitment to human rights and to upholding fundamental principles of a free and democratic society.

Recommendation 12: Amend Schedule 1 of Bill 194 to include an explicit statutory list of prohibited uses of AI systems that may be supplemented by regulation. Banned uses of the technologies should be assessed against the foundational AI principles that the IPC proposes in Recommendation 10.

[27] Some examples of explicitly banned uses of AI technologies under the *EU Artificial Intelligence Act* include: 1) AI systems that deploy subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; 2) AI systems that classify individuals/persons for the purpose of producing social scores based on their social behaviour or known, inferred or predicted personal or personality characteristics, that can lead to detrimental or unfair treatment of individuals; 3) use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; or 4) AI systems used to assess the likelihood of a person committing a criminal offence, based solely on the profiling of that person or on assessing their personality traits and characteristics.
For more, see: EU Artificial Intelligence Act. (2024). "Article 5: Prohibited Items Artificial Intelligence Act". Available at: https://artificialintelligenceact.eu/article/5/.

Recommendations specific to digital technologies affecting individuals under 18

The third portion of Schedule 1 entitled *Digital Technology Affecting Individuals Under the Age of 18*, would establish a regulatory regime governing the digital information that school boards and children's aid societies may collect, use, retain or disclose relating to individuals under 18 and the types of digital technologies they may make available to children and youth.

As *Children and youth in a digital world* is one of my office's strategic priorities, I applaud the government for wanting to strengthen protections for children and youth. However, the proposed model of Schedule 1 has several flaws.

Privacy protections for children under Ontario's existing privacy laws should be strengthened

Most significantly, we remain very concerned with the overlap between this proposed regulatory regime under the supervision of the minister and my existing mandate over the *same regulated activity* under Ontario's access and privacy laws. This overlap has the potential to set up duplicative or divergent standards by the minister on one hand and my office on the other, sparking confusion, inconsistency, and uncertainty among regulated entities.[28] For example, regulations made under sections 9 and 10(a) under Schedule 1 prescribing how school boards and children's aid societies shall (or shall not) collect, use, retain or disclose digital information relating to children and youth under eighteen may run directly counter to decisions and guidance from my office under MFIPPA and Part X of CYFSA in respect of the exact same activities.

For these reasons, we strongly recommend that sections 9 and 10(a) be removed from Schedule 1 and that the additional privacy protections intended to be introduced by these provisions be more carefully thought through and integrated into FIPPA, MFIPPA and Part X of the CYFSA instead. This would have the benefit of strengthening protections and obligations that already exist respecting the collection, use, retention and disclosure of personal information, including of children and youth, ensuring a more coherent and consistent regime overall rather than introducing potentially conflicting rules. My office stands ready to consult on how this may best be achieved.

Recommendation 13: Remove sections 9 and 10(a) from Schedule 1 and strengthen instead relevant privacy provisions in FIPPA, MFIPPA and Part X of CYFSA to protect children and youth as part of a more consistent, coherent, and seamless privacy regulatory regime.

[28] Prof. Teresa Scassa, in her submission on Bill 194, has similarly warned that the legislation may lead to a situation where "the regulations could set requirements or standards that are lower than what is required under FIPPA or MFIPPA – creating an unnecessarily confusing and misleading system." She recommends that s. 9 (regulation setting by lieutenant governor in council) and 10 (minister regulations to require certain technical standards) should be moved into other legislation to avoid the risk of complicating the existing regulatory environment.

The application of ministerial regulations and directives regarding digital technologies made available for use by individuals under 18 should be broadened

Otherwise, we support the other provisions of Schedule 1, namely sections 10(b) and 11 that would introduce ministerial regulations prescribing technical standards and directives regarding digital technologies made available for use by individuals under age 18. The IPC recognizes that technical standards have the potential to improve the protections afforded to children and youth across the province when they are implemented in ways that are privacy protective and consistent with the values of personal autonomy, dignity, and individual self-determination, in accordance with the purpose clause we propose under Recommendation 1.

Moreover, technical standards that are adopted consistently across the board have the added benefit of enhancing the negotiating strength of school boards and children's aid societies vis a vis third-party digital platform. School boards and children's aid societies could point to such technical standards when negotiating with third parties to add in certain protections or remove certain features of their software applications to comply with Ontario laws.

However, as currently worded, the *Digital Technology Affecting Individuals Under Age 18* section of Schedule 1 captures only school boards and children's aids societies, leaving out other children and family service providers and public sector entities that could be reasonably expected to make technologies available to children under age 18. As examples, the proposed bill currently excludes public libraries, municipal childcare centres and day camps, and group homes. This will further add to the regulatory inconsistency and uncertainty by regulating some actors and not others. Moreover, it will create unfairness and inequities by providing some children and youth with more or less protections depending on which public sector entity they interact with.

For this reason, we recommend that the public sector entities subject to the minister's directives and regulations related to technical standards respecting digital technologies made available for use by individuals under age 18, be expanded to include all service providers within the meaning of the CYFSA, and all other municipal and provincial public sector institutions that could be reasonably expected to make such technologies available to children and youth.

Recommendation 14: Amend Schedule 1 of Bill 194 to expand the application of ministerial directives and regulations related to technical standards respecting digital technologies made available to individuals under the age of 18 so that these cover all service providers defined by the CYFSA, and all other public sector institutions that could be reasonably expected to make such digital technologies available to children and youth.

SCHEDULE 2 OF BILL 194: AMENDMENTS TO THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

The IPC is pleased to see some long overdue changes to FIPPA that would finally bring it in line with most other modern privacy laws and strengthen the privacy protections Ontarians want and deserve in a digital age. These include privacy impact assessments, mandatory breach reporting, and stronger enforcement. However, there are other critical gaps still to be filled. Before the ink dries on Schedule 2 of Bill 194, we strongly recommend certain amendments be made to avoid missing this opportunity to get it right.

Data minimization principles should be introduced

Data minimization is a foundational privacy principle common to most modern privacy legislation that serves as a safety valve against over-collection, use, and disclosure of personal information. PHIPA and Part X of the CYFSA both have a data minimization clause, as does FIPPA, but only in respect of Part III.1.[29] We adding a data minimization principle in Part III of FIPPA as well.

Data minimization requires a disciplined, *less is more* approach to the collection, use, and disclosure of personal information for legitimate government purposes. It typically takes the form of a general requirement for organizations to limit their collection, use, and disclosure of personal information to only that which is necessary to carry out its intended goal or purpose. It does not prevent organizations from carrying out their legitimate functions, but only serves to control the amount of personal information involved in the process.

Minimizing the amount of personal information collected, used, and disclosed to only what is necessary is a basic way of respecting individuals' privacy. It does so by tying it back to the institution's purpose and providing clarity on how the personal information may or may not be used. It serves to prevent, for example, overcollection and function creep. Data minimization is also an effective way of insulating institutions from the devastating impacts of privacy breaches. When less is collected in the first place, less can be lost or compromised as a result of a breach, reducing overall risks to privacy. Simply having less data to store and securely manage brings further benefits, such as reduced resourcing and related technical costs.

Data minimization reflects a universally accepted, modern data protection standard we strongly recommend adding such a clause to Part III of FIPPA through the proposed Schedule 2.

Recommendation 15: Amend Schedule 2 by introducing into Part III of FIPPA a data minimization principle similar to what already exists in PHIPA, Part X of CYFSA, and Part III.1 of FIPPA.

XXX(1) An institution shall not collect, use, or disclose personal information if other information will serve the purpose of the collection, use, or disclosure.

[29] Currently, data minimization under Part III.1 of FIPPA only applies to the activities of a small number of designated data integration units, whereas data minimization under section 30 of PHIPA and sections 283 and 287 of the CYFSA, applies more broadly under those acts.

(2) An institution shall not collect, use, or disclose more personal information than is reasonably necessary to meet the purpose of the collection, use, or disclosure, as the case may be.

(3) This section does not apply to personal information that an institution is required by law to collect, use, or disclose.

Privacy impact assessment requirements should be further strenghtened

If passed, Schedule 2 would amend FIPPA to require provincial institutions to conduct a privacy impact assessment (PIA) before collecting personal information and enable the IPC to receive copies of PIAs on request. This is a very positive development. PIAs are integral to *privacy by design*. They serve as an early warning system for privacy risks. They empower decision-makers to assess and anticipate serious risks up front so they can proactively resolve or mitigate the risks before deploying a new or amended program or initiative, avoiding costly breaches and loss of public trust.

However, under the proposed amendment, institutions would be allowed to begin collecting personal information *before* putting risk mitigation measures into place "if it is not possible to implement the [risk mitigation] steps". In such a case, they would have to do so "within a reasonable time". Under this proposed provision, Ontarians' sensitive personal information could be collected and exposed to a significant risk for an unknown period before the risk would be addressed. While we understand there may be a need for exceptions in certain circumstances, the proposed clause, as worded, is too permissive. We recommend that the ability to proceed with the collection of personal data before having privacy mitigation measures in place be limited to situations where the privacy risks of doing so are low.

Recommendation 16: Amend section 4(2) of Schedule 2 (proposing to introduce new provisions under section 38 of FIPPA) to circumscribe the conditions in which an institution may proceed to collect Ontarians' personal information before having implemented the steps needed to mitigate privacy risks identified pursuant to a PIA.

38 (4) The head of an institution shall ensure that the steps mentioned in paragraph 9 of subsection (3) are implemented:

(a) before collecting the personal information mentioned in that subsection; or
(b) if it is not possible to implement the steps before collecting the personal information ***and the privacy risks to individuals are low****, within a reasonable time after collecting the information*

Schedule 2 of Bill 194 would also require institutions to amend a PIA where there is any significant change to the purpose for which personal information is used or disclosed. Indeed, this requirement is critical to keep PIAs updated considering any significant changes to a program, initiative, or activity so that institutions have an accurate calculus of the risks involved.

However, PIAs should be updated whenever there is a significant change to any of the factors originally considered as part of the PIA, not just a change in the purpose for which personal information is used or disclosed. This would include any significant change to the institution's

legal authorities, the types or sources of personal information intended to be collected, the roles of individuals who will have access to the information, any of the planned limitations or restrictions, the period the personal information will be retained, or the safeguards or practices used to protect the personal information. Restricting the requirement to update PIAs only when there is a significant change to the purposes for which personal information is used or disclosed means that new privacy risks arising from any of these other significant changes would go unnoticed and unaddressed.

Recommendation 17: Amend section 4(2) of Schedule 2 to expand the situations in which PIAs must be updated under the proposed section 38(5) of FIPPA.

> *38 (5) Unless the regulations provide otherwise, before making any significant change to the ~~purpose for which personal information mentioned~~ **matters listed** in subsection (3) ~~is used or disclosed~~, the head of an institution shall,*
>
> > *(a) update the assessment prepared under subsection (3) to reflect the proposed change ~~and to set out the proposed intended use or disclosure~~; and*
> > *(b) implement any additional steps identified under paragraph 9 of subsection (3).*

Grounds for individual complaints should be expanded

Schedule 2 of Bill 194 would amend FIPPA to make explicit the right of individuals to bring privacy complaints to the IPC. This change is long overdue, and we are pleased to see this statutory gap finally get addressed. However, as currently proposed, Schedule 2 would appear to only grant the right to file a privacy complaint to individuals notified of a privacy breach. For example, if an individual learned of a potential violation of their privacy independently of a formal breach notification by the institution (e.g., an employee snooping case or other unauthorized access which the institution itself did not know or notify the individual about), the individual would have no right to complain. Likewise, if individuals had reason to believe an institution is inappropriately collecting or retaining their personal information, they could not file a complaint.

The grounds for individuals to file complaints with the IPC should be broadened to include any situation where an individual has reasonable grounds to believe that an institution has not complied with an obligation under Part III of FIPPA, whether or not they received a formal breach notification from an institution. This would align FIPPA more closely with the general right of individual complainants under both PHIPA and the CYFSA and other privacy statutes in Canada.

Recommendation 18: Amend section 6 of Schedule 2 to introduce broader grounds for individuals to bring privacy complaints under a new section 40.1(4.1) of FIPPA and make an ancillary change to the proposed new section 40.1(5) of FIPPA.

> ***Privacy Complaints***

40.1 ***(4.1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Part may make a complaint to the Commissioner.***

Privacy Complaints — time limit

*40.1 (5) A complaint mentioned in subsection (4**.1**) must be made in writing and filed with the Commissioner within one year after the subject-matter of the complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant, whichever is the shorter.*

Necessary investigative powers should be established

For the Commissioner to review privacy complaints or matters under FIPPA, Schedule 2 would grant certain investigative powers to the Commissioner. Specifically, Schedule 2 would enable the Commissioner to compel the production of information and records that are relevant to the subject matter under review and that are under the custody or control of an institution, and create a corresponding duty on the institution's officers, employees, consultants, and agents to cooperate and assist with the review.

This provision is a good first step but is insufficient to carry out an effective investigation in today's increasingly digital context. Privacy investigations typically involve complex information technologies (IT) and multiple parties that may or may not be institutions under FIPPA. For example, access to premises and onsite reviews of complex IT systems may be necessary to effectively determine the technological vulnerabilities that may have led to a privacy breach. Moreover, the ability to compel evidence under oath from persons other than the institution, including third party processors or persons reasonably suspected of malicious activity that resulted in a breach, is essential for the Commissioner to map out the entire data flow(s) and conduct a comprehensive investigation along the entire chain of actors involved.

These powers already exist under sections 60(1) and 59(2) of PHIPA, sections 320(1) and 319(2) of the CYFSA, and other privacy regimes across Canada. Notably, these powers also exist under section 52(4) of FIPPA as part of the access to information appeals inquiry process. While these powers are rarely used, they are essential escalation tools to streamline the efficiency of inquiries and investigations, particularly when the parties involved are resistant or uncooperative with the investigative process.

Recommendation 19: Amend section 7 of Schedule 2 by broadening the scope of investigative powers needed for the Commissioner to effectively carry out privacy reviews under the proposed section 49.0.1 of FIPPA.

Commissioner's review of information practices
49.0.1 (1) The Commissioner may conduct a review ***in respect of the compliance of any person with this Part*** ~~*of the information practices of an institution*~~ *if the Commissioner has received a complaint under subsection 40.1 (4.**1**) or has other reason to believe that the requirements of this Part are not being**, or will not be,** complied with.*

Powers of Commissioner
(6) The Commissioner may require the production of such information and records that are relevant to the subject matter of the review ~~and that are in the custody or under the control of an institution.~~

Evidence under Oath
(6.1) The Commissioner may summon and examine on oath any person who, in the Commissioner's opinion, may have information relating to a review under this Part, and for that purpose, the Commissioner may administer an oath.

Entry of Premises
(6.2) In a review under this Part, the Commissioner may at any reasonable time enter and inspect any premises without a warrant or court order, other than a dwelling, on satisfying any security requirements relating to the premises.

Evidence
(6.3) In a review under this Part, the Commissioner may receive and accept any evidence and other information that the Commissioner sees fit, whether on oath or by affidavit or otherwise and whether or not it is or would be admissible in a court of law.

Orders
*(7) ~~If, a~~**A**fter giving an opportunity to be heard to the head of the institution **and any other affected person, the Commissioner may make an order directing any person to perform a duty imposed by this Part and, if** the Commissioner determines that an information practice contravenes this Part, the Commissioner may order the head to do any of the following:*

1. *Discontinue the information practice.*
2. *Change the information practice as specified by the Commissioner.*
3. *Return, transfer or destroy personal information collected or retained under the information practice.*
4. *Implement a different information practice as specified by the Commissioner.*
5. *Make a recommendation in respect of how the information practice could be improved.*

Limit on certain orders
(8) The Commissioner may order under subsection (5) no more than what is reasonably necessary to achieve compliance with this Part.

Procedure
*(9) The Statutory Powers Procedure Act does not apply to a review conducted under **this Part**, ~~section~~ **and the Commissioner may establish the rules of procedure that the Commissioner considers necessary**.*

Enable the Commissioner to disclosure information as necessary

Currently, FIPPA binds the Commissioner to one of the most restrictive confidentiality clauses of any Canadian privacy statute. FIPPA does not include any statutory exceptions to the

Commissioner's obligation not to disclose information that comes to their knowledge in the performance of their powers, duties, and functions under this or any other act.

Schedule 2 of Bill 194 would change that by allowing the Commissioner to share information with their federal, provincial, and territorial counterparts to coordinate activities, including enforcement and policy development, to ensure that personal information is protected as consistently as possible across jurisdictions. This is a very welcome amendment which my office fully supports.

Schedule 2 would also allow the Commissioner to share information if the disclosure is permitted for a prescribed purpose. It is not yet known what those exceptions will be or when such exceptions might be adopted by resolution. Section 68(3) of PHIPA and section 328(3) of the CYFSA, on the other hand, have more explicit statutory provisions that allow the Commissioner to disclose information that comes to their knowledge in the performance of their functions if required for the purpose of exercising those functions.

Such circumstances may include having to share certain information with the parties, and sometimes third parties, to investigate or establish the grounds for findings, recommendations, and orders. It may be necessary to disclose information to a court in the context of a judicial review or other legal proceedings. The Commissioner may have to disclose information to other government institutions that require necessary information to mitigate the impacts of a privacy breach or a major cyber security incident for example or to the Attorney General for the prosecution of an offence under the Act. Most significantly, the Commissioner may need to disclose information in the public interest for the purposes of public education, accountability, and transparency. With additional powers to investigate privacy complaints, including high-profile privacy breaches affecting hundreds of thousands of individuals, Ontarians will expect to know the general status and outcome of investigations.

Recommendation 20: Amend section 9 of Schedule 2 to remove any ambiguity around the Commissioner's ability to share information necessary to carry out their powers, duties, and functions under the current section 55(1) of FIPPA.

> *55 (1) The Commissioner or any person acting on behalf of or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act, unless* ***the disclosure is required for the purpose of exercising those powers, duties or functions or*** *the disclosure is permitted for a prescribed purpose.*

In the alternative, if Bill 194 is passed in its current form, we would urge the government to expedite the development of the regulation addressing exceptions to Commissioner's confidentiality obligation so that it comes into force upon the act's proclamation.

A recipient rule should be included

Public institutions increasingly outsource certain functions to third party vendors to help carry out their statutory mandates. Such scenarios often involve the processing of personal information by external organizations that are not institutions covered by FIPPA.

A *recipient rule* would help ensure that when institutions share Ontarians' personal information with any third-party recipient, the recipient cannot use it for other, unrelated purposes, such as mining the data for their own commercial benefit or enrichment. A recipient rule would also create a legal obligation for third parties to notify institutions in the event of a privacy breach. While institutions may include such restrictions and obligations in their contractual arrangements with third parties, this is not always done consistently, and such terms or conditions are not always easy to negotiate or straightforward to enforce. Imposing a direct statutory obligation on recipients to restrict the uses to which they may put the personal information and to notify the institution in the event of a breach would help institutions strengthen or fill gaps in their third-party agreements.

Introducing a *recipient rule* under FIPPA would also align with a similar obligation that already exists under section 49 of PHIPA. Such a provision would specify that when an institution discloses personal information to a recipient organization (that is not an institution), the recipient can only use or disclose the information for the purposes for which it was originally disclosed, or as permitted or required by law, and must notify the institution in the event of a breach.

Recommendation 21: Amend Schedule 2 to add a provision into Part III of FIPPA that imposes restrictions on third party recipients of personal information as follows.

> ***XXX(1) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, a person who is not an institution and to whom an institution discloses personal information, shall not use or disclose:***
>
> > ***(a) the information for any purpose other than the purpose for which the institution was authorized to disclose the information under this Act or the purpose of carrying out a statutory or legal duty; and***
> > ***(b) more of the information than is reasonably necessary to meet the purpose of the use or disclosure, as the case may be.***
>
> ***(2) If personal information that was disclosed by an institution to a recipient under subsection (1) has been stolen, lost, or used or disclosed without authority, the recipient shall notify the institution from which it received the personal information.***
>
> ***(3) The notification mentioned in subsection (2) must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the recipient determines that the theft, loss or unauthorized use or disclosure has occurred.***

Children's personal information should be deemed as sensitive

We commend the government for recognizing the need to protect children's personal information in an increasingly digital world. While Bill 194 proposes some means of enhancing those protections in Schedule 1 (as discussed above), it misses out on the critical and timely opportunity to do so in Schedule 2 by amending FIPPA to this effect.

As children and youth are increasingly exposed to digital technology and daily online activity, the risks that children's personal information will be used in ways that may lead to harm are also on the rise. My office has consistently called for the recognition that children and youth's personal information constitutes sensitive information and requires special considerations, protections, and safeguards.

Therefore, we recommend that Schedule 2 introduce a provision deeming children and youth's personal information as *sensitive personal information*. Further, we recommend that institutions' obligations to conduct privacy impact assessments and to establish the necessary administrative, technical, and security safeguards be modified commensurately with this increased level of sensitivity.

Recommendation 22: Amend Schedule 2 of Bill 194 to introduce a new section 2(5) under FIPPA that would deem the personal information of children and youth as being sensitive information.

> ***2 (5) In this Act and the regulations, personal information relating to children and youth shall be deemed to be sensitive.***

Recommendation 23: Amend sections 4(2) and 5 of Schedule 2 in Bill 194 that propose to add new sections 38(3) and 40(5) to FIPPA, as follows.

> *38(3) Unless the regulations provide otherwise, before collecting personal information, the head of an institution shall ensure that a written assessment is prepared that contains the following information respecting any personal information that the institution intends to collect:*
>
> […]
>
> *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**, taking into account the sensitivity of the information,** in the event of a theft, loss or unauthorized use or disclosure of the personal information.*
>
> […]
>
> *40(5) The head of an institution shall take steps that are reasonable in the circumstances**, including having regard to the sensitivity of personal information,** to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the personal information are protected against unauthorized copying, modification, or disposal.*

Whistleblowers should be protected from employer reprisal

Schedule 2 of Bill 194 introduces important whistleblowing provisions. Any person who has reasonable grounds to believe that an institution has contravened or is about to contravene

FIPPA would be able to notify my office and request that their identity be kept confidential. Establishing a legislative framework to enable public sector employees to speak up about wrongdoing, risk, or negligence reflects the basic tenets of a modern privacy law and is critically important to ensure effective institutional governance.

In some cases, however, employees may feel apprehensive to report wrongdoing or potential wrongdoing due to fear of employer reprisal. As drafted, Schedule 2 would not protect from retaliation an individual who reported (or who an institution thinks will report) a breach to the IPC. In many cases, the institution will be able to deduce the identity of the individual, even if the Commissioner does not disclose it. This protection from retaliation, which exists under section 70 of PHIPA and section 330 of the CYFSA, is critical for protecting an individual's right to come forward both legally and practically. We recommend therefore, that an equivalent protection be included in FIPPA.

Further, the ability to notify the IPC and request that one's identity be kept confidential should be available to whistleblowers who have concerns about *any person* who has contravened, or is about to contravene FIPPA, not just institutions and data integration units.

Recommendation 24: Amend section 10 of Schedule 1 to expand the scope of whistleblower protections and introduce a new non-retaliation provision into section 57.1.

Whistleblowing

57.1 (1) Any person who has reasonable grounds to believe that ~~an institution, a ministry data integration unit under Part III.1, or a multi-sector data integration unit under Part III.1~~ ***~~or~~ a person*** *has contravened or is about to contravene this Act or the regulations may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.*

Confidentiality
(2) The Commissioner must keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

(3) No one shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage a person by reason that,

(a) the person, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that any other person has contravened or is about to contravene a provision of this Act or its regulations;
(b) the person, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene a provision of this Act or its regulations;
(c) the person, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of a provision of this Act or its regulations; or
(d) any person believes that the person will do anything described in clause (a), (b) or (c).

Further, the IPC recommends amending Schedule 2 of Bill 194 to introduce a corresponding provision under section 61(1) of FIPPA that would make it an offence to retaliate against a whistleblower in contravention of the prohibition above (similar to that which already exists in PHIPA and the CYFSA):

Recommendation 25: Amend Schedule 2 of Bill 194 to introduce a new provision under FIPPA that would make it an offence for anyone to retaliate against a whistleblower:

61 (1) No person shall,
...
(g) contravene subsection 57.1(3)

Expansion of ServiceOntario's powers should be removed from FIPPA

The IPC supports modernizing government services and implementing digital technologies to streamline and improve how Ontarians interact with government services, provided this is done securely and respects individual privacy rights.

If passed, section 15 of Schedule 2 would amend section 65.1 of FIPPA to expand the definition of *customer service information*, and enable ServiceOntario to collect, use, and retain this additional personal information. This is personal information about Ontarians who rely on ServiceOntario to obtain and renew their health cards, driver's licenses, Ontario Photo ID cards, and other critical identity documents. The proposed new powers would be for purposes beyond those currently permitted under ServiceOntario's enabling statute and regulation: the *Ministry of Government Services Act* and Ontario Reg. 475/07.

FIPPA's core purpose is to protect Ontarians' personal information held by the government. We are concerned that the government is proposing to use FIPPA to broadly expand ServiceOntario's ability to collect, use, and retain personal information as part of an optional service delivery channel without clearly demonstrating the need for these additional authorities. In addition, the authority for SeviceOntario to retain and use personal information should not be set out in FIPPA which is a privacy protection statute. Instead, the expansion of any lawful authority or purpose of ServiceOntario should be more appropriately and transparently addressed under its own enabling legislation and regulation.

Furthermore, the proposed changes under section 15 of Schedule 2 would broaden the definition of customer service information that ServiceOntario can collect, use, and retain without the correlative protection of a data minimization principle. As per Recommendation 15 above, a data minimization principle is critical to restrict the collection and use of personal information if other information can serve the purpose and limit the collection and use of personal information to no more than necessary to meet its legitimate purpose.

Recommendation 26: Amend Schedule 2 of Bill 194 to remove Section 15. If the government wishes to expand ServiceOntario's authority, it should do so by amending ServiceOntario's enabling statute and regulation rather than by way of amendments to FIPPA. Any expansion of ServiceOntario's authority to collect personal information of Ontarians, even under its own enabling legislation, should be clearly circumscribed by a data minimization

principle to guard against the potential of creating a centralized repository of Ontarians' government-held personal information.

A mandatory statutory review period to ensure the Act stays current over time should be included

FIPPA came into force back in 1988, nearly 40 years ago, when phones were still mostly landlines, records were almost exclusively paper-based, and Google was just a glimmer of an idea. Since then, there has been a titanic shift in how organizations process personal information owing to an onrush of digital technologies now available to them. Technological inventions have accelerated at an exponential rate giving us vast amounts of digital storage and computing power, high-speed internet, connected mobile devices and wearables, social media platforms and, of course, artificial intelligence systems.

Despite this sea of change, FIPPA has never undergone any significant review until now. To avoid finding ourselves in this same situation in the future, Ontario laws and policies cannot be left to lag so far behind technology. We recommend that a statutory review clause be added to FIPPA to ensure that it gets reviewed on a regular basis and evolves over time to stay current with modern reality.

Recommendation 27: Amend Schedule 2 of Bill 194 to introduce a mandatory statutory review period to ensure FIPPA is reviewed by the Legislature minimally every five (5) years.

Equivalent amendments to MFIPPA should be introduced

While my office welcomes FIPPA amendments to bring the act closer to a 21st-century standard, we are concerned that Bill 194 is not simultaneously advancing equivalent amendments to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Amending FIPPA but not MFIPPA would significantly disrupt the harmony, consistency, and uniformity around how personal information is collected, used, retained and disclosed across Ontario's provincial and municipal institutions. This misalignment would create unnecessary confusion and uncertainty for Ontario's public sector organizations. Meanwhile, Ontarians would be left disappointed and wondering why they are afforded different privacy protections from the province than from, for example, their city, town, school, or public library.

Moreover, establishing clear rules for privacy breach reporting under provincial privacy law but not under its municipal counterpart risks muddying the waters at a critical time when institutions need to be educated about their new obligations. New expectations will have to be made crystal clear upon implementation of the bill. Having to explain which public institutions are and are not subject to these new provisions will unduly complicate matters. Allowing municipal institutions to skip out on reporting breaches when other provincial institutions must do so is no insignificant matter. In each of the last two years, two-thirds of all privacy breaches and complaints reported to the IPC have been from MFIPPA institutions, and those were just the ones we know of under

a voluntary reporting scheme. Municipalities and municipal institutions like schools and libraries continue to be major targets for cyber attacks.[30]

Reforming FIPPA without making equivalent changes to MFIPPA also creates a discrepancy in the IPC's statutory powers to investigate breaches. It could complicate reviews of cases where both municipal and provincial institutions are involved, causing significant issues and delays. We would be hindered in our ability to examine data flows across institutions. For example, when investigating privacy complaints related to Ontario's transit systems (involving both Metrolinx and the TTC) or policing (involving both Ontario Provincial Police and municipal police services). For these reasons, we strongly recommend that equivalent amendments in Schedule 2 in respect of FIPPA, be made to MFIPPA as well.

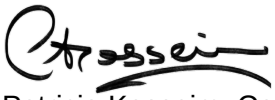
Recommendation 28: The IPC strongly recommends that the government hasten its plans to introduce equivalent changes to MFIPPA, as it has for FIPPA, to ensure that Ontarians are afforded the same privacy protections whether they are engaging with provincial or municipal public sector organizations.

Conclusion

In closing, I wish to reiterate our support for Bill 194, with the changes recommended above. My office remains committed to working with the government and the legislature to strengthen the current legislative proposals for the benefit of all Ontarians.

In the spirit of openness and transparency, this letter and attachments will be posted on the IPC's website in both English and French.

Sincerely,



Patricia Kosseim, Commissioner

Cc: Todd J. McCarthy, Minister, Public and Business Service Delivery and Procurement
Renu Kulendran, Deputy Minister, Public and Business Service Delivery and Procurement
John Roberts, Associate Deputy Minister, Public and Business Service Delivery and Procurement
Melissa Kittmer, Assistant Deputy Minister, Public and Business Service Delivery and Procurement
Mohammad Qureshi, Corporate Chief Information Officer, Public and Business Service Delivery and Procurement
Daniela Spagnolo, Chief Information Security Officer, Public and Business Service Delivery and Procurement
Michelle Stock, Chief of Staff, Public and Business Service Delivery and Procurement

Attachments

[30] Financial Post. "Southern Ontario school board acknowledges 'cyber incident'," Dec 2023. Available at: https://financialpost.com/technology/southern-ontario-school-board-acknowledges-cyber-incident.
CBC. "Hamilton library computers, other services remain down, 3 months after ransomware attack," May 2024. Available at: https://www.cbc.ca/news/canada/hamilton/library-cyber-impact-continues-1.7203740.

APPENDIX

Recommendation 1: Amend Schedule 1 to include the following purpose clause [note: IPC proposed legislative language appears in **bold text**]:

> ***[X] The purpose of this Act is to establish a governance framework for public sector entities in relation to cyber security activities, use of artificial intelligence systems and deployment of digital technologies affecting individuals under the age of eighteen, in accordance with the following principles:***
>
> ***(a) the privacy of individuals and groups must be protected, and the collection, use, retention, and disclosure of their personal information must be limited to that which is necessary and proportionate for the purpose;***
>
> ***(b) public sector entities must be transparent in fulfilling their obligations under this Act to the extent reasonable and appropriate, without jeopardizing the security and integrity of government information systems;***
>
> ***(c) artificial intelligence systems must be valid, reliable and safe, they must be designed to protect privacy and affirm human rights, and public sector entities that use them must be accountable and transparent;***
>
> ***(d) the creation and implementation of standards for digital technologies affecting individuals under age 18 must respect the rights of children and youth and be consistent with the values of personal autonomy, dignity, and individual self-determination; and***
>
> ***(e) compliance with the provisions of this Act and its regulations should be reviewed independently of government.***

Recommendation 2: Amend Schedule 1 to explicitly acknowledge the IPC's independent oversight role and responsibilities by adding the following clause:

> ***[X] The Information and Privacy Commissioner shall have all the powers, duties, and functions currently established by the Freedom of Information and Protection of Privacy Act, the Municipal Freedom of Information and Protection of Privacy Act, the Personal Health Information Protection Act, the Child, Youth and Family Services Act, and other legislation which assigns it powers, duties, and functions in relation to regulated public sector entities subject to this Act.***

Recommendation 3: Amend Schedule 1 to require a prescribed public consultation process before adopting regulations under the act. Such a requirement should be modelled after section 74 of PHIPA.

Recommendation 4: Amend Schedule 1 to require the minister to consult with the IPC before proposing or adopting regulations, or issuing directives that may impact Ontarians' access or privacy rights. Such an amendment should be modelled after sections 55.4(2)-55.4(3) of PHIPA.
.

Recommendation 5: Amend Schedule 1 to require that the minister's directives be publicly promulgated. Specifically, add new sections following 4(3) and 11(3) of Schedule 1 to read as follows:

> ***4(X) Every directive issued under section 4(1) of this Act,***
>
> ***(a) shall be made available to the public on request; and***
>
> ***(b) shall be publicly posted on at least one Government of Ontario website.***
>
> ***11(X) Every directive issued under section 4(1) of this Act,***

(a) ***shall be made available to the public on request; and***
(b) ***shall be publicly posted on at least one Government of Ontario website.***

Recommendation 6: Amend schedule 1 to include explicit protections for whistleblowers.

Whistleblowing
[X] (1) Any person who has reasonable grounds to believe that a public service entity or any other person has contravened or is about to contravene this Act or the regulations, including a directive under this Act, may notify the Commissioner or an officer designated by the minister of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality
(2) The Commissioner or the officer designated by the minister must keep confidential the identity of a person who has notified them under subsection (1) and to whom an assurance of confidentiality has been provided.

Non-Retaliation
(3) No one shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage a person by reason that,

(a) ***the person, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner or the officer designated by the minister that any other person has contravened or is about to contravene a provision of this Act or its regulations, including a directive;***
(b) ***the person, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene a provision of this Act or its regulations, including a directive;***
(c) ***the person, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of a provision of this Act or its regulations, including a directive; or***
(d) ***any person believes that the person will do anything described in clause (a), (b) or (c).***

Penalty
(4) Every person who contravenes subsection (3) is guilty of an offence and on conviction is liable to a fine not exceeding $5,000.

Recommendation 7: Amend section 2(2) of Schedule 1 to ensure that any regulations governing cyber security programs of public sector entities require the inclusion of certain core elements consistently across all programs.

Regulations re programs

(2) Without limiting the generality of clause (1) (b), a regulation made under that clause ~~may~~ ***shall*** *require that a public sector entity's program include,*

[…]
(f) identification and management of any organizational cyber security risks, including risks associated with the public sector entity's supply chain and its use of third-party products and services;
(g) measures to protect entity cyber systems from being compromised;
(h) processes to detect any cyber security incidents affecting, or having the potential to affect, a public sector entity's cyber systems; and,
(i) procedures to minimize the impact of cyber security incidents.

Recommendation 8: Amend Schedule 1 to require the minister to provide to the IPC copies of reports it receives from public sector institutions in cases of significant cyber incidents that involve, or may involve, personal information.

> ***[X] The minister shall provide the Information and Privacy Commissioner with copies of reports the minister receives from public sector entities under section 2(1)(c), including reports produced by third parties at the request of public service entities, in respect of significant cyber incidents that involve, or may involve, personal information.***

Recommendation 9: Amend Schedule 1 to require the minister to issue an annual report on the number, types, and general outcomes of cyber related incidents reported, any emerging trends observed over time, and other information that may be prescribed in regulation.

Recommendation 10: Strengthen Schedule 1 by codifying clear statutory principles to serve as guardrails around the responsible use of AI systems by public sector entities. Codifying such guardrails, in addition to the purpose clause proposed under *Recommendation 1* would provide necessary assurances to earn and maintain Ontarians' trust in the use of AI systems. Details could be added through regulations or technical standards, allowing for a more flexible and agile regulatory approach.

Recommendation 11: Amend Schedule 1 to explicitly adopt a risk-based framework. Such a framework should assess the potential impact and likelihood of harm associated with different AI systems, ensuring that AI systems with higher risk of unintended harm receive more stringent oversight than those classified as lower risk AI systems.

Recommendation 12: Amend Schedule 1 of Bill 194 to include an explicit statutory list of prohibited uses of AI systems that may be supplemented by regulation. Banned uses of the technologies should be assessed against the foundational AI principles that the IPC proposes in Recommendation 10.

Recommendation 13: Remove sections 9 and 10(a) from Schedule 1 and strengthen instead relevant privacy provisions in FIPPA, MFIPPA and Part X of CYFSA to protect children and youth as part of a more consistent, coherent, and seamless privacy regulatory regime.

Recommendation 14: Amend Schedule 1 of Bill 194 to expand the application of ministerial directives and regulations related to technical standards respecting digital technologies made available to individuals under the age of 18 so that these cover all service providers defined by the CYFSA, and all other public sector institutions that could be reasonably expected to make such digital technologies available to children and youth.

Recommendation 15: Amend Schedule 2 by introducing into Part III of FIPPA a data minimization principle similar to what already exists in PHIPA, Part X of CYFSA, and Part III.1 of FIPPA:

> ***XXX(1) An institution shall not collect, use, or disclose personal information if other information will serve the purpose of the collection, use, or disclosure.***
>
> ***(2) An institution shall not collect, use, or disclose more personal information than is reasonably necessary to meet the purpose of the collection, use, or disclosure, as the case may be.***
>
> ***(3) This section does not apply to personal information that an institution is required by law to collect, use, or disclose.***

Recommendation 16: Amend section 4(2) of Schedule 2 (proposing to introduce new provisions under section 38 of FIPPA) to circumscribe the conditions in which an institution may proceed to collect Ontarians' personal information before having implemented the steps needed to mitigate privacy risks identified pursuant to a PIA:

> *38 (4) The head of an institution shall ensure that the steps mentioned in paragraph 9 of subsection (3) are implemented:*
>
> > *(a) before collecting the personal information mentioned in that subsection; or*
> > *(b) if it is not possible to implement the steps before collecting the personal information* ***and the privacy risks to individuals are low****, within a reasonable time after collecting the information.*

Recommendation 17: Amend section 4(2) of Schedule 2 to expand the situations in which PIAs must be updated under the proposed section 38(5) of FIPPA.

> *38 (5) Unless the regulations provide otherwise, before making any significant change to the ~~purpose for which personal information mentioned~~* ***matters listed*** *in subsection (3) ~~is used or disclosed~~, the head of an institution shall,*
>
> > *(a) update the assessment prepared under subsection (3) to reflect the proposed change ~~and to set out the proposed intended use or disclosure~~; and*
> *(b) implement any additional steps identified under paragraph 9 of subsection (3).*

Recommendation 18: Amend section 6 of Schedule 2 to introduce broader grounds for individuals to bring privacy complaints under a new section 40.1(4.1) of FIPPA and make an ancillary change to the proposed new section 40.1(5) of FIPPA.

> ***Privacy Complaints***
>
> *40.1* ***(4.1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Part may make a complaint to the Commissioner.***
>
> *Privacy Complaints — time limit*

*40.1 (5) A complaint mentioned in subsection (4**.1**) must be made in writing and filed with the Commissioner within one year after the subject-matter of the complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant, whichever is the shorter.*

Recommendation 19: Amend section 7 of Schedule 2 by broadening the scope of investigative powers needed for the Commissioner to effectively carry out privacy reviews under the proposed section 49.0.1 of FIPPA.

Commissioner's review of information practices
49.0.1 (1) The Commissioner may conduct a review ***in respect of the compliance of any person with this Part*** ~~*of the information practices of an institution*~~ *if the Commissioner has received a complaint under subsection 40.1 (4.**1**) or has other reason to believe that the requirements of this Part are not being**, or will not be,** complied with.*

[…]

Powers of Commissioner
(6) The Commissioner may require the production of such information and records that are relevant to the subject matter of the review ~~*and that are in the custody or under the control of an institution.*~~

Evidence under Oath
(6.1) The Commissioner may summon and examine on oath any person who, in the Commissioner's opinion, may have information relating to a review under this Part, and for that purpose, the Commissioner may administer an oath.

Entry of Premises
(6.2) In a review under this Part, the Commissioner may at any reasonable time enter and inspect any premises without a warrant or court order, other than a dwelling, on satisfying any security requirements relating to the premises.

Evidence
(6.3) In a review under this Part, the Commissioner may receive and accept any evidence and other information that the Commissioner sees fit, whether on oath or by affidavit or otherwise and whether or not it is or would be admissible in a court of law.

Orders
(7) ~~*If, a*~~***A****fter giving an opportunity to be heard to the head of the institution* ***and any other affected person, the Commissioner may make an order directing any person to perform a duty imposed by this Part and, if*** *the Commissioner determines that an information practice contravenes this Part, the Commissioner may order the head to do any of the following:*

1. *Discontinue the information practice.*
2. *Change the information practice as specified by the Commissioner.*
3. *Return, transfer or destroy personal information collected or retained under the information practice.*
4. *Implement a different information practice as specified by the Commissioner.*

5. Make a recommendation in respect of how the information practice could be improved.

Limit on certain orders
(8) The Commissioner may order under subsection (5) no more than what is reasonably necessary to achieve compliance with this Part.

Procedure
(9) The Statutory Powers Procedure Act does not apply to a review conducted under ***this Part****, ~~section~~* ***and the Commissioner may establish the rules of procedure that the Commissioner considers necessary****.*

Recommendation 20: Amend section 9 of Schedule 2 to remove any ambiguity around the Commissioner's ability to share information necessary to carry out their powers, duties, and functions under the current section 55(1) of FIPPA.

55 (1) The Commissioner or any person acting on behalf of or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act, unless ***the disclosure is required for the purpose of exercising those powers, duties or functions or*** *the disclosure is permitted for a prescribed purpose.*

Recommendation 21: Amend Schedule 2 to add a provision into Part III of FIPPA that imposes restrictions on third party recipients of personal information as follows:

XXX(1) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, a person who is not an institution and to whom an institution discloses personal information, shall not use or disclose:

(a) the information for any purpose other than the purpose for which the institution was authorized to disclose the information under this Act or the purpose of carrying out a statutory or legal duty; and
(b) more of the information than is reasonably necessary to meet the purpose of the use or disclosure, as the case may be.

(2) If personal information that was disclosed by an institution to a recipient under subsection (1) has been stolen, lost, or used or disclosed without authority, the recipient shall notify the institution from which it received the personal information.

(3) The notification mentioned in subsection (2) must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the recipient determines that the theft, loss or unauthorized use or disclosure has occurred.

Recommendation 22: Amend Schedule 2 of Bill 194 to introduce a new section 2(5) under FIPPA that would deem the personal information of children and youth as being sensitive information:

2 (5) In this Act and the regulations, personal information relating to children and youth shall be deemed to be sensitive.

Recommendation 23: Amend sections 4(2) and 5 of Schedule 2 in Bill 194 that propose to add new sections 38(3) and 40(5) to FIPPA, as follows:

38(3) Unless the regulations provide otherwise, before collecting personal information, the head of an institution shall ensure that a written assessment is prepared that contains the following information respecting any personal information that the institution intends to collect:

[…]

*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**, taking into account the sensitivity of the information,** in the event of a theft, loss or unauthorized use or disclosure of the personal information.*

[…]

*40(5) The head of an institution shall take steps that are reasonable in the circumstances**, including having regard to the sensitivity of personal information,** to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the personal information are protected against unauthorized copying, modification, or disposal.*

Recommendation 24: Amend section 10 of Schedule 1 to expand the scope of whistleblower protections and introduce a new whistleblower non-retaliation provision into section 57.1:

Whistleblowing

*57.1 (1) Any person who has reasonable grounds to believe that ~~an institution, a ministry data integration unit under Part III.1, or a multi-sector data integration unit under Part III.1~~ **a person** has contravened or is about to contravene this Act or the regulations may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.*

Confidentiality

(2) The Commissioner must keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

(3) No one shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage a person by reason that,

(a) the person, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that any other person has contravened or is about to contravene a provision of this Act or its regulations;

(b) the person, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene a provision of this Act or its regulations;
(c) the person, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of a provision of this Act or its regulations; or
(d) any person believes that the person will do anything described in clause (a), (b) or (c).

Recommendation 25: Amend Schedule 2 of Bill 194 to introduce a new provision under FIPPA that would make it an offence for anyone to retaliate against a whistleblower:

61 (1) No person shall,
...
(g) contravene subsection 57.1(3)

Recommendation 26: Amend Schedule 2 of Bill 194 to remove Section 15. If the government wishes to expand ServiceOntario's authority, it should do so by amending ServiceOntario's enabling statute and regulation rather than by way of amendments to FIPPA. Any expansion of ServiceOntario's authority to collect personal information of Ontarians, even under its own enabling legislation, should be clearly circumscribed by a data minimization principle to guard against the potential of creating a centralized repository of Ontarians' government-held personal information.

Recommendation 27: Amend Schedule 2 of Bill 194 to introduce a mandatory statutory review period to ensure FIPPA is reviewed by the Legislature minimally every five (5) years.

Recommendation 28: The IPC strongly recommends that the government hasten its plans to introduce equivalent changes to MFIPPA, as it has for FIPPA, to ensure that Ontarians are afforded the same privacy protections whether they are engaging with provincial or municipal public sector organizations.