SEPTEMBER 2021

IPC Comments on the Ontario Government's White Paper on *Modernizing Privacy in Ontario*

Patricia Kosseim
Commissioner

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Contents

A. INTRODUCTION

The Office of the Information and Privacy Commissioner of Ontario (IPC) is pleased to offer its views in response to the government's white paper, *Modernizing Privacy in Ontario*.[1] The purpose of our comments and recommendations is to support the creation of a modern regulatory framework based on strong governance of personal information in the private sector that leaves no Ontarian behind. Such a framework should also enable responsible and sustainable innovation, facilitate seamless oversight across sectors, and ensure harmonization with other jurisdictions.

I commend the government for proposing concrete provisions consistent with the principles-based, fair, well-balanced, pragmatic, flexible and proportionate approach our office called for in our response[2] to the government's first consultation document released last August, *Improving private sector privacy for Ontarians in a digital age*.[3] We strongly believe that Ontario should seize this opportunity to further the province's goal of equipping Ontarians "with the skills, rights and opportunities to fully participate, work and thrive in the digital world"[4] and to protect their privacy in a manner that aligns with local values, realities and culture. The white paper is a critical step in the journey of building a modern, privacy protective environment in Ontario that will give the public the confidence it needs to embrace innovation rather than shy away from it. Providing regulatory certainty and compliance support to Ontario businesses — particularly small and medium-size enterprises (SMEs) — is equally important for fuelling the data-driven economy at a time when Ontarians need it the most.

Harmonization was clearly an important consideration in the government's decision to base its legislative proposals on the federal *Digital Charter Implementation Act* ("Bill C-11"), expanding and improving upon it as needed and appropriate for Ontarians. In our view, this was a wise approach given the importance of achieving "substantially similar" status, which would exempt Ontario's organizations conducting commercial activity within the province from the federal regime[5], streamlining regulatory oversight and ensuring practical compatibility with other private sector privacy schemes in Canada and around the world.

Before commenting directly on the white paper's seven "Key Areas for Reform," we feel compelled to respond to the minister's statement[6] accompanying the white paper, suggesting that private sector reform in Ontario would be contingent on the fate of the federal Bill C-11. Since this statement, we now know Bill C-11 is destined to die on the order paper with the recent announcement of a fall federal election. Whether the same bill, a modified version, an entirely new bill, or no new bill at all will be tabled by the next federal government is unknown at this time. In view of this ongoing uncertainty, it is incumbent upon the Government of Ontario to press forward with its plans of enhancing Ontarians' privacy rights.

B. THE NEED FOR PROVINCIAL ACTION – WITH OR WITHOUT FEDERAL REFORM

As previously indicated, it is my office's view that privacy rights would be better protected with a provincial privacy law that is substantially similar to the federal law yet goes beyond the limits of the current *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), Bill C-11, or whatever reform bill may be introduced in the future.

Three Canadian provinces already have their own private sector privacy laws deemed substantially similar to *PIPEDA*. The choice for Ontario, as Canada's largest province, is whether to join – and even take a leadership role among – those provinces that have chosen to protect their citizens by filling the regulatory gaps left open by the federal framework.

Without a provincial approach to privacy in Ontario, millions of Ontarians will continue to be exposed to unregulated privacy and security risks, potentially undermining public trust and confidence in Ontario's data-driven economy.

In the discussion that follows, we explain how Ontarians and businesses operating in this province could benefit from a carefully crafted made-in-Ontario private sector privacy law — with or without federal law reform.

1) JURISDICTIONAL LIMITATIONS

Most significantly, a provincial private sector privacy law could provide protections in areas where the federal Parliament simply lacks the jurisdiction to act. In particular, the IPC was encouraged to see the government's proposal to cover the millions of employees of provincially regulated companies who have zero protections under federal privacy law.[7] As well, we were pleased to see that the provincial law being contemplated would cover unions, charitable organizations, and professional associations whose non-commercial activities have gone unregulated for far too long. A made-in-Ontario private sector privacy law could offer more comprehensive protections to Ontarians that go entirely beyond the reach of any federal law now or in the future.

I. EMPLOYEES

The privacy rights of employees of provincially regulated companies are not, and will never be, protected under federal privacy law given the distribution of powers between federal and provincial legislatures in our Constitution. Many experts have raised concerns about the increasing level of employee surveillance during the pandemic[8], which shows no signs of abating in a post-COVID recovery world. Professor Teresa Scassa has described some of the new technologies available to employers trying to track the productivity of their employees. These include technologies that monitor: websites visited; time spent on websites or in documents; location information through GPS; employees' computer

screens; incoming and outgoing email; keystrokes; social media activity and more. Even more invasive technologies, such as facial recognition and voice sentiment analysis, may soon be on the horizon as well. Many employers[9] are exploring requirements for employees to provide proof of vaccination as a condition of work, introducing additional risks to privacy and other human rights that will have to be lawfully justified, managed and mitigated according to the specific context and circumstances of employment.

Filling the gap on employee privacy would be a significant achievement given the current lack of protection that impacts millions of Ontarians on a daily basis as they strive to earn their livelihood.

II. NOT-FOR-PROFIT SECTOR

The significant volumes of data held by the not-for-profit sector in Ontario are not immune from privacy and security vulnerabilities,[10] yet they remain largely unprotected by federal privacy law, which is constitutionally constrained in this space. The pandemic has only exacerbated the cyber threats to the non-commercial sector. Like many other sectors, non-profit organizations have increasingly moved to remote work, resulting in greater exposure to privacy and security risks.[11] To further compound these risks, non-profits may have fewer resources to support privacy compliance activities. For example, one charity providing meal services recently experienced a breach and took five months to (voluntarily) notify the affected individuals because it required "a substantial amount of resources" from the charity's small team to assess the breach and respond accordingly.[12] Currently, no privacy law applies generally to Ontario non-profit organizations and no regulator has been given responsibility for this sector. Under a provincial private sector privacy law, the IPC would have the expanded mandate to support not-for-profits by advising them on their privacy and security challenges, educating them about risks, and encouraging up-front protections.

III. POLITICAL PARTIES

While the government's proposals were silent in this regard, the IPC recommends that the scope of application of an Ontario private sector privacy law include political parties, as is the case under British Columbia's private sector privacy law[13] and as is being proposed by Quebec's Bill 64.[14] Much has been said and written about the importance of covering political parties, including by Ontario's own independent officer responsible for election oversight who has called for political parties to be subject to privacy laws.[15] One need only turn to recent news items highlighting the alleged use of facial recognition technology by political parties to verify identities,[16] or the Cambridge Analytica scandal, to appreciate the need for political parties to be subject to privacy obligations. The potential misuse of personal information in election campaigns risks undermining not only the trust of citizens but the very core of democracy itself.

2) YOUTH AND CHILDREN

Despite widespread recognition that children and youth merit special privacy protection due to their inherent vulnerability, *PIPEDA* and Bill C-11 are largely silent on this subject. The province has an opportunity to fill this gap by enacting a law, with accompanying regulations or codes of practice that protect its most vulnerable citizens.

In 2019, 21% of polled Ontario students (7-12) reported spending five or more hours on social media per day.[17] Since the onset of the COVID-19 pandemic, studies have shown significant further increases in leisure screen time and use of social media among both children and youth.[18] Increased time online results in increased risks that children's personal information will be used, misused or even *abused* by others in ways that may be harmful to them, seriously undermining their sense of identity, self-confidence and well-being. As indicated in our previous submission, youth should be granted the freedom of experimentation and self-discovery at a young age without worrying about the permanent reputational impacts of information they post about themselves online.

Privacy risks to children and youth go beyond social media. Emerging smart toys are incorporating artificial intelligence (AI) capabilities that can collect data to personalize the user experience for children.[19] The use of these smart toys will continue to grow and children deserve protection from potentially intrusive technologies, particularly those designed to survey them, create gaming dependency or addiction or otherwise negatively influence their behaviour.

Given the provincial nexus with education, a provincial private sector privacy law could also go a long way in enhancing privacy protection for children in schools. While the IPC has jurisdiction in respect of school boards under the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), we do not have direct jurisdiction over the third party companies with whom they contract to provide information processing services, such as cloud-based data management services or the use of digital platforms for school-related purposes. As two recent findings from our office demonstrate, this means that when things go allegedly wrong with the third party service provider, we can only investigate part of the issue.[20]

3) OPERATIONAL EFFICIENCIES

In the absence of a substantially similar law in Ontario, *PIPEDA* applies to the full spectrum of Canadian business — from global internet giants, large multinationals, banks and telecommunications companies to small emerging companies and local family-owned businesses — all of which have different realities and pose different levels of privacy risk. This would be the same under Bill C-11 or any other federal reform bill.

The reality of Ontario's economic sector is that SMEs constitute 98% of all businesses in Ontario and 30% of the province's GDP.[21] Ontario's proposal goes a long way towards offering an alternative and more agile approach that would better fit the realities of

SMEs and their unique compliance challenges. The Ontario proposal would grant the IPC discretionary authority to develop compliance support tools, such as guidance and advisory services, and to approve the creation of sectoral codes of practice and certification programs. By reason of sheer geography, the IPC could play a consultative role at the regional and local level, closer to the eyes, ears and voices of the SME sector. By tailoring educational materials, codes and advisory services to better reflect the situation on the ground and by having discretion to focus on areas of greatest practical impact, the IPC could help guide SMEs through their post-COVID recovery efforts as they adopt more permanent solutions. The IPC could also help enable small innovative start-ups to thrive and mature responsibly, aligned with the province's Digital and Data Strategy.[22]

The Ontario proposal would also ensure a fair, contextual and robust enforcement regime that is more streamlined and efficient. Ontario could design a flexible and proportionate dispute resolution mechanism rather than the cumbersome, two-tiered enforcement regime proposed by Bill C-11. Ontarians have more than 30 years' experience with IPC's access and privacy dispute resolution mechanism that is heavily weighted towards early resolution and mediation.[23] Ontario courts are also familiar with the adjudicative processes of the IPC, having established a significant body of jurisprudence on matters of judicial review that have come before them over the past decades.

4) INTER-SECTORAL INTEGRATION

Ontario's proposal provides an opportunity to create a seamless data regulatory environment that is better integrated across sectors in a way that a federal law cannot practically achieve. The Ontario government can reduce red tape and regulatory burden by harmonizing its regulatory approach to innovative cross-sectoral initiatives and the exponential growth in public-private partnerships (P3) — from the "ed-tech" sector, to virtual health care services, to smart cities. In view of the increasing reliance of public institutions on third party service providers, and the rising number of data breaches occurring "somewhere" in the information processing chain, Ontario could devise a coordinated regulatory scheme that covers all the pieces of the puzzle within a single jurisdiction, rather than straddling between provincial laws (for public, health, child and youth sector components) and federal law (for private sector components).

Under the same jurisdiction, an Ontario private sector privacy law could be carefully constructed so that its provisions either defer to (or prevail over) other existing privacy and access laws across its health, child and youth, and public sectors. In this way, Ontario could enable a consistent and coherent approach by integrating a new private sector privacy law and its other existing privacy and access statutes, all governed by a single privacy regulator, whose mandate would be carefully coordinated with the new data authority being proposed as part of its Digital and Data Strategy.[24] In this way, Ontario could simplify compliance requirements, increasing regulatory certainty for collaborating P3 organizations and streamlining Ontario's data regulatory environment overall.

5) HARMONIZED APPROACH

Another key consideration for an Ontario privacy law is how to regulate commercial activity involving trans-border data flows that have become part and parcel of the global economy. To respond to concerns that an Ontario private sector privacy law would only add to the complexity of the Canadian statutory landscape, a modern privacy regime could build in the appropriate mechanisms to reduce regulatory burdens for businesses having to comply with laws in multiple jurisdictions. This challenge already exists for countless other regulated activities by virtue of Canada's status as a federation and it can be overcome by intentional, creative and strategic design choices that promote cooperative federalism.

For example, *PIPEDA* explicitly recognizes provinces' legislative power to regulate the collection, use and disclosure of personal information within their respective borders. If a province chooses to adopt a "substantially similar" provincial law — as Quebec, British Columbia and Alberta have already done — businesses conducting commercial activity within that province are exempt from *PIPEDA* and have only to comply with the provincial law in question. For businesses that engage in commercial activity across borders that may trigger federal privacy law, the concept of "substantially similar status" helps ensure harmonization and interoperability between Canadian jurisdictions.[25] Similarly, when it comes to international data flows, the concept of "adequacy status" incentivizes harmonization and interoperability between Canadian laws and the European Union's General Data Protection Regulation (GDPR).[26]

Moreover, existing arrangements between Canadian data protection authorities already allow for cooperative enforcement measures that provide enhanced protection for their residents, greater predictability and certainty for businesses, and reduced regulatory burden. Ontario's private sector law could explicitly enable or authorize information-sharing arrangements among the IPC and other federal, provincial and territorial (FPT) privacy commissioners, as well as other relevant regulators, to promote consistency in approaches and cooperative enforcement. Under such arrangements, regulators could mutually recognize one another's jurisdiction, commit to respecting fundamental principles in common, agree on indicators for determining a lead jurisdiction, and engage to identify policy gaps and areas for further collaborative work.

Finally, in terms of enforcement, the IPC's order-making powers, including the power to issue administrative penalties under an Ontario private sector privacy law, could include consideration of any regulatory action already taken by other jurisdictions as a possible mitigating factor, ensuring a harmonized, fair and proportionate approach.

For all the above reasons, the IPC encourages the government to bring forward its own private sector privacy law, irrespective of federal privacy law reform. This legislative opportunity is worth pursuing in its own right for the benefit of all Ontarians, and not just as a fall-back plan to Bill C-11 or any successor bill — the future of which is highly uncertain.

C. COMMENTS ON THE GOVERNMENT'S PROPOSED AREAS FOR REFORM

We now address each of the seven topics the government has raised in its white paper under "Key Areas for Reform." We hope that our views will assist the government's deliberations and contribute to the constructive public debate the white paper is intended to elicit.

1. RIGHTS-BASED APPROACH

I. PREAMBLE

The IPC applauds the government's proposal to affirm privacy as a fundamental right in the preamble of an eventual Ontario privacy law. According to Teresa Scassa, Canada Research Chair in Information Law and Policy at the University of Ottawa, the inclusion of recitals in a preamble setting out the human rights basis for the protection of privacy would give legislative voice to the principles and human rights values that underlie data protection law in Canada and provide concrete direction for the interpretation of its provisions.[27] Although *PIPEDA* has been ruled as having quasi-constitutional status,[28] a recent decision[29] of the federal court reinforces the need to make the human rights approach more explicit if it is intended to "transform or alter the proper approach to statutory interpretation."[30]

In its white paper, the Ontario government commented that "a key factor in establishing public trust and confidence in the right to privacy will be the provision of genuine transparency requirements and strong, independent oversight for Ontarians." Yet, neither of these principles appears in the proposed preamble. Nor does the concept of demonstrable accountability. Transparency and accountability are arguably two of the most fundamental principles of a modern privacy law, deserving of at least the same prominence as principles of proportionality, fairness and appropriateness. Equally, most modern privacy laws around the world explicitly recognize "independence" of data protection authorities as a critical requirement for effective oversight.[31] An explicit reference to independent oversight would align with the overarching purposes set out in Ontario's *Personal Health Information Protection Act 2004* (*PHIPA*).

II. FAIR AND APPROPRIATE PURPOSES

The Ontario government has proposed an overarching provision that would set "principles-based boundaries" around permissible activities under the law. This provision would ensure that personal information may only be collected, used or disclosed for purposes that a reasonable person would consider fair and appropriate in the circumstances. We applaud the proposed application of the fair and appropriate clause to all collections, uses or disclosures of personal information, with or without consent. This provision will help transform what

could be interpreted as a mere symbol of compliance through paper trails documenting technical compliance[32] to more substantive protection of the privacy rights of Ontarians.

The principle of fairness is not included in the appropriate purposes provision in *PIPEDA* or Bill C-11, and we commend the government for considering the introduction of this important concept as an overarching condition. The European Data Protection Board (EDPB) defines fairness as "an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject."[33] This concept is critically important to protect individuals and groups from downstream discriminatory impacts of automated data processing and profiling, for example.

We also applaud the government for codifying a list of objective factors that must be considered when assessing what a reasonable person would consider to be a fair and appropriate purpose. These factors provide greater predictability and certainty for organizations having to apply the law and for regulators and courts having to interpret it.

In terms of the proposed factors themselves, we would offer three comments. First, when considering the volume, nature and sensitivity of the personal information, we would recommend including consideration of the context. For reasons on which we elaborate below, the sensitivity of the information may drastically change from one context to another.

Second, by assessing whether personal information is necessary to achieve the legitimate needs of the organization, one must also consider effectiveness. If the collection, use or disclosure of the personal information is not likely to be effective in meeting the legitimate needs of an organization, then it is not likely to be necessary either for achieving the same elusive ends. Conversely, even if the collection, use or disclosure of personal information is effective in achieving the legitimate needs of an organization, it might not be necessary to do so where, for example, less or other personal information will do. For greater certainty, we recommend that this proposed factor make explicit reference to both necessity and effectiveness as accompanying conditions to consider when determining what is fair and appropriate.[34]

Third, when assessing whether the benefit is proportionate to the individual's loss of privacy, it would be important to specify for whose benefit. We would recommend that benefit be considered beyond the organization's pure commercial profit to include benefits to the individual, to other individuals and to society more broadly.

III. "NO-GO ZONES"

Among the list of factors that must be considered in assessing what is a fair and appropriate purpose are the "legitimate needs" of an organization.[35] The white paper proposes a subparagraph of the fair and appropriate purpose clause in which it enumerates what would *not* be considered a legitimate need of an organization. If the government's intention is to prohibit these designated practices altogether (which we strongly believe it should), we recommend that it do so more clearly, directly and explicitly

by declaring these *not* to be fair and appropriate purposes, rather than indirectly by only having to consider them when assessing legitimate needs.

Among the list of prohibited purposes (otherwise known as "no-go zones") are purposes that are known or likely to cause significant harm to individuals or groups; contraventions of a law of Ontario or Canada; the monitoring or profiling of an individual under the age of 16 for the purposes of influencing the individual's behaviour or decisions; and any other prescribed purpose. With one qualification, we support the inclusion of these no-go zones in the law.

In particular, we query whether the prohibition against monitoring or profiling children and youth for the purposes of influencing their behaviour or decisions might be too broadly formulated. Given that an Ontario law would apply to not-for-profit organizations, among others, this prohibition might inadvertently preclude educational initiatives that actually benefit children and youth by promoting positive behavioural changes (for example, adopting healthier food choices or engaging in more physical activity), particularly in cases where parental consent has been obtained for such a purpose. Accordingly, we would recommend that the government consider qualifying this no-go zone to instances that may "*negatively* influence the individual's behaviour or decisions."

IV. DEFINITIONS OF PERSONAL INFORMATION AND SENSITIVE INFORMATION

The white paper has invited feedback on the definition of personal information. There is a long-standing body of law and jurisprudence that defines personal information as "information about an identifiable individual." Given the importance of a harmonized approach, we recommend that a new Ontario law remain consistent with this well-established definition as it already exists in many other privacy laws in Ontario, Canada and abroad.[36]

There are, however, three aspects of this definition that merit further attention. First, the concept of identifiability has become increasingly fluid, particularly when one takes into account the risks of re-identification. We elaborate on this issue further below in our discussion about de-identification.

Second, whether information is "about" an individual has also come under significant strain with the ability of emerging technologies to infer or predict information about individuals based on analyses of their online behaviour or profiling. Whether or not such information is accurate should not matter from a privacy perspective. To the extent it is associated with an individual or attributed to them by a human or algorithm, it should still be considered *about* them.

Third is the concept of the individual. While privacy laws have historically centred around the individual, there is increasing recognition of the potential privacy harms (and downstream discriminatory impacts) that new information technologies, particularly AI, can have on groups. While it may be too soon to suggest altering the classic definition of

personal information without further reflection on potential ramifications, the impacts on groups should be taken into consideration in other provisions of a modern privacy law, wherever relevant and appropriate.

The white paper also invites feedback on whether sensitive information should be defined in law either based on risk or on specific classes or categories of information. We would not recommend defining sensitivity in terms of an enumerated list of data types. Time and again, cases have shown that information which may seem banal at first (e.g. subscriber information) can rise to the level of "sensitive" depending on what that information together with other information is capable of revealing about the individual in the circumstances.[37] Conversely, information which is presumptively sensitive by its nature (e.g. financial information) may be considered less so depending on the particular context.[38] In our view, sensitivity of the information is certainly an appropriate factor to take into account when considering what constitutes a fair and appropriate purpose, whether consent should be express or implied, what level of security safeguards is warranted, and whether a data breach poses real risk of significant harm, etc. The higher protection afforded to sensitive information may also be relevant in assessing adequacy of an Ontario private sector privacy law under the GDPR.[39] However, when assessing sensitivity, the nature of the information should never, in our view, be decoupled from its context.

V. DATA PORTABILITY

The government's data portability proposal would grant individuals the right to transfer their personal information from one organization to another if both organizations are subject to a data mobility framework to be set out in regulations.

The touted benefits of data portability include enhancing an individual's control over their personal information and fostering competition by helping to address issues such as vendor lock-in and barriers to businesses' entry into market.[40]

Consistent with Bill C-11, the government has proposed the development of sector-specific standards and consistent technical requirements to facilitate moving data between organizations in that sector. The IPC supports the province's inclusion of a right of data portability in a private sector privacy framework to the extent it is interoperable with that of other jurisdictions and helps facilitate movement of data across borders. We also support a sectoral approach to the development of technical standards and requirements that would ensure an appropriate context-specific framework for porting data.

To date, some experts have indicated that the right to data portability has been underutilized in those jurisdictions that have introduced it, noting issues such as proper authentication of users; the appropriate handling of the personal information of third parties; legal risks and responsibilities if data is ported to a service provider with weak privacy or security protections; the safety of data while in transit and risks of onward transfers or other downstream uses of data.[41] Ontario can learn from the models and

implementation experience of other jurisdictions. A phased approach may also help to address the low levels of adoption experienced in other jurisdictions.[42]

The government is also seeking feedback on the appropriate scope of the portability provisions. In our view, Ontario's portability provisions should extend beyond only the information provided by the individual to the organization, to include other observed data about the individual (such as search history or location data). There are arguments both for and against extending the right of portability even further to include derived data as well, such as consumer profiles and behavioural predictions. We recognize that individuals may wish to port this type of personal information; at the same time, there are competing proprietary and confidentiality considerations that must be taken into consideration. The IPC looks forward to engaging with the government and other relevant stakeholders on these more granular aspects of a data portability framework, including the development of regulations and sector-specific technical standards.

VI. DISPOSAL AND DE-INDEXING

In its white paper, the government proposes a right to request disposal of personal information collected from the individual, subject to limited exceptions.

Our office supports the right of disposal, particularly where the information is provided by the individual or is observed about the individual. Should the right of disposal be extended to include all personal information that an organization holds about the individual regardless of its source or its derivation, more work will be needed to define countervailing considerations to the right of disposal, particularly where the charter rights of others may be engaged.[43] Whether minors' right to disposal of personal information is deserving of greater relative weight in the balance by virtue of their inherent vulnerability is also worth serious consideration.

Where an organization refuses an individual's request to destroy their personal information, we agree that the organization should be required to provide the individual with reasons for the refusal and information regarding available recourse. We are also pleased to see that the organization's disposal obligation would include responsibility for ensuring that any third party service providers that received the personal information in the course of providing a service to the organization must also destroy it.

A related but separate issue is the need to consider building in a requirement for de-indexing. De-indexing grants individuals the right to request that certain online content linked to their name be removed from the results returned by a search engine. Essentially, the information remains online but becomes more difficult for others to find. In our view, the right to request de-indexing is an important tool for individuals (particularly children and youth) to manage their online reputation and exert control over potentially embarrassing, inaccurate, outdated or irrelevant information.

Accordingly, we recommend adopting a de-indexing scheme, modelled after Quebec's Bill 64, itself inspired by the GDPR. Bill 64 proposes to grant individuals the right to request that hyperlinks attached to their name be de-indexed where dissemination contravenes the law or a court order or where dissemination causes serious injury to reputation or privacy that clearly outweighs the public's right to be informed or a person's freedom of expression, and the request does not exceed what is necessary for preventing the injury.[44] In balancing these latter interests, explicit criteria must be taken into account, including whether the person is a public figure or a minor; whether the information is up to date and accurate; the sensitivity of the information and the context in which the information is disseminated; as well as the time elapsed since the information was disseminated.

In our view, Bill 64 represents a thoughtful and well-balanced de-indexing scheme which the Government of Ontario should seriously consider in the context of its own private sector privacy law.

2. SAFE USE OF AUTOMATED DECISION-MAKING

The IPC is pleased to see the government's focus on establishing rules for the safe and trustworthy use of AI and automated decision-making.

In June 2021, the IPC set out its initial position on AI in its response[45] to the Ontario government's consultation on the *Trustworthy Artificial Intelligence (AI) Framework* intended for *government* use of artificial intelligence. Much of the underlying reasoning in our AI submission is equally applicable in the private sector context, and we recommend that the government review that submission in parallel with our comments below.

I. SCOPE OF THE PROHIBITION

The Ontario white paper defines automated decision-making as including any technology that "*assists* or replaces the judgement of human decision-makers" [46] (emphasis added). This proposed definition appears to be modelled on Bill C-11 and the Government of Canada's Directive on Automated Decision-Making.[47] It applies to a wide range of information analysis techniques[48], both where human decision-making is replaced, or assisted, by such a system. This would mean that decisions which are entirely automated, and human decisions which are merely assisted by an automated process would be treated equally. Accordingly, the prohibition against using automated decision systems to make decisions that may significantly affect an individual would apply to both.

By contrast, the equivalent prohibition at Article 22 of the GDPR refers to decisions based "solely on automated processing." By focusing on *solely* automated decisions, the GDPR approach creates an incentive for organizations to have a "human-in-the-loop." Having a "human-in-the-loop" helps ensure (at least where a decision produces legal effects

concerning an individual or significantly affects the individual) that a human decision-maker plays a non-trivial role in the outcome and takes accountability for it.

Human oversight is not a panacea that can address all algorithmic harms[49]; however, it is nonetheless an important accountability measure which should be encouraged. IIf the government's policy intent is to incentivize organizations to insert a human in the loop, it could consider narrowing the proposed prohibition against automated decision making to *solely* automated decisions as in the GDPR.

On the other hand, if the government's public policy intent is to increase transparency and individual control in respect of *any* decision that could significantly affect an individual, then any such decision, regardless of the means used to make it, should be subject to some or all of the conditions[50] proposed for automated decision systems.

Whichever the policy intent, a clear mapping should be made between that public policy intent and the proposed legislation, which takes into account whether and when fully automated processes should be regulated differently from the same process carried out with meaningful human involvement.

II. EXCEPTIONS TO THE PROHIBITION

The white paper proposes three exceptions to the prohibition against using automated means to make decisions that may significantly impact an individual: 1) such a decision must be necessary for entering into, or performing, a contract between the organization and the individual; 2) such a decision must be otherwise authorized by law; or, 3) the organization obtains the individual's express consent.

We are pleased to see the government's intention to address the significantly elevated privacy risks associated with AI. For instance, we agree with the proposal to require *explicit* consent where consent is relied upon as lawful grounds for automated decision-making. However, we are concerned that the other two exceptions may not actually offer any enhanced protection for individuals whose personal information is subject to automated decision-making relative to other types of processing.

For example, the necessity exception reads very similar to the first activity included in the list of business activities that would be authorized (without consent), yet it is not subject to the same critical guardrails that apply to those business activities (see our discussion below in respect of "*Business Activities*"). Likewise, the exception that would allow automated decision-making if *otherwise authorized by law*, would appear to allow organizations to use automated means to process personal information under any of the other authorized grounds that permit any other type of processing.

This begs the question: in what ways could an Ontario law enhance protections for individuals who may be significantly impacted by automated decision systems relative to protections that already exist in respect of other types of data processing? We recommend

that the exceptions to the prohibition against automated decision-making be tightened up accordingly in order to provide more meaningful protections for significantly impacted individuals. We also recommend consideration of further protections discussed below.

III. ACCOUNTABILITY, RISK ASSESSMENT AND REVIEW

Bias in an automated decision system is difficult to detect through analysis of a single decision. Rather, it will often require analyzing the outcomes of many decisions (as well as related inputs) before one can begin to identify trends. It would be inadequate, then, to rely entirely on complaints by individuals who are the subject of these decisions to identify biases in a deployed system. The assessment and detection of potential bias must begin before a system goes live and be monitored on an ongoing basis.

Where an organization makes automated decisions that would significantly affect the individual, it should be held to an up-front accountability requirement to assess the algorithmic impacts of its automated decision system. This assessment of algorithmic impacts could be part of an enhanced privacy impact assessment (PIA) (see discussion below). A due diligence process should be engaged early to establish that reasonable steps have been taken to identify and mitigate potential bias and to assess and affirm that potential benefits of the system are not outweighed by potential negative impacts to the affected individual or to a group. This should be supplemented by an ongoing review process, such as an evidence-based evaluation of actual impacts.

In keeping with a fair, well-balanced, pragmatic, flexible and proportionate approach, it would be reasonable to scale accountability and review requirements for automated decision systems. Scalability could be based on various risk factors such as the volume, nature and sensitivity of the information involved, reasonable expectations of the individual and the potential impacts on individuals or groups.

We recommend that this general due diligence requirement be elaborated upon by way of regulation and/or guidance to provide the flexibility needed to ensure that these various risk factors are appropriately taken into account in accordance with the context. For instance, in some situations, an assessment of the algorithmic impacts of an automated decision system might have to involve different business units across an organization to ensure that various perspectives are brought to bear on the assessment. In situations involving higher thresholds of risk, organizations may seek input from an external body of advisors or expert consultants. In cases involving higher risks still, consultation with the community or communities most likely to be impacted by the system and/or consultation with an independent review body, such as the IPC, might be required.

This pre-deployment assessment of automated decision systems does not remove the need for ongoing post-deployment review of decisions. As such, we support the white paper's inclusion of strong control mechanisms, such as the ability for individuals to comment on and contest a decision made about them, to request correction of the personal information used to render the decision and to have the decision reviewed.[51] We

recommend that organizations be required to inform individuals of these controls as part of the organization's obligation to respond to requests for an explanation of the automated decision system.[52]

IV. RECORD-KEEPING

The white paper invites comment on the issue of appropriate record-keeping requirements. We recommend that — at a minimum — effective record-keeping be required for any automated decisions that significantly affect individuals. This would include documentation of the risk assessment carried out in respect of the automated decision system adopted (see discussion above).

The white paper also raises the potential of "requiring organizations to log and trace the collection and use of personal information" in the context of automated decision-making. We acknowledge, as does the white paper, that requiring this in all cases could potentially place a substantial burden on organizations. However, we also note that, in the case of automated decisions which significantly affect the individual, the government proposes to (among other things) allow the individual to request the personal information used to render the decision. Without an associated record-keeping requirement, this right would be rendered moot. Therefore, we recommend that this particular record-keeping requirement be carefully considered in light of all of its related implications, both for and against.

V. RESTRICTIONS ON PROFILING

The white paper also asks whether any additional requirements or protections should be considered with respect to profiling. The white paper notes that "when profiling is the basis for a decision that significantly affects an individual, a false prediction carries a high risk of harm." However, an individual can be equally harmed by a *true* prediction that reveals previously unknown information, particularly with respect to sensitive attributes (such as genetic or behavioural characteristics).

Given the risks of harm associated with profiling, we would recommend that it be made clear that the resulting profiles of individuals also constitute personal information about those individuals, whether accurate or not. By explicitly clarifying this, profiles would be subject to the same protections as all other types of personal information, including access, correction, disposal, fairness and appropriateness.

3. ENHANCED CONSENT

Consent plays a central role in Canadian private sector privacy legislation, yet is nearly universally recognized as being in stark need of modernization. An updated consent framework would enable individuals to focus their attention on the most impactful information influencing their decisions while at the same time providing more practical

flexibility for organizations to innovate and compete. While, for reasons stated in our earlier submission,[53] we would still prefer a regime based on consent as a rule, subject to allowable exceptions, we nonetheless offer feedback on the government's proposed approach of placing consent and alternative grounds for processing personal information on equal footing.

I. VALID CONSENT

As a whole, we are supportive of the information elements that must be provided in plain language at or before the time of purported processing in order for consent to be considered valid. As per our earlier submission, we believe that consent will only be truly meaningful where it is reasonable to expect that the individual understands the nature, purpose and consequences of what is being asked.

We also support including among the list of information disclosures a requirement that the individual be informed of their right to give, refuse or withdraw consent. This relatively straightforward inclusion will help make consent more meaningful by ensuring that individuals are aware that they have true choice and that they may withdraw consent, subject to applicable legal or contractual requirements and reasonable notice.

Finally, and consistent with *PIPEDA* and Bill C-11, we recommend that any eventual Ontario law should clearly prohibit organizations from requiring, as a condition for the supply of a product or service, that an individual consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service. Similarly, organizations should be prohibited from obtaining consent by deceptive or duplicitous means.

II. FORM OF CONSENT

In regard to the form of consent, the white paper speaks of allowing organizations to rely on implied consent in certain circumstances taking into account the sensitivity of the personal information involved and the reasonable expectations of the individual. The IPC supports codification of these well-established conditions for implied consent.[54]

We would recommend clarifying more explicitly that the same information disclosure requirements apply for implied consent, as with express consent, including the requirement to inform individuals about their right to withdraw consent. Also, for implied consent to be valid, individuals must be provided with a timely and actionable means of expressing their objection to consent ("opt-out consent") and an ongoing ability to withdraw consent after the fact, subject once again to applicable legal or contractual requirements and reasonable notice.

III. BUSINESS ACTIVITIES

One of the most significant updates to the consent model featured in Ontario's proposals is the ability for organizations to collect and use personal information without consent for standard business activities subject to two important guardrails — that a reasonable person would expect such a collection or use for the activity, and the personal information is not collected or used for the purposes of influencing the individual's behaviour or decisions.

We agree that these two guardrails constitute reasonable limits on the processing of personal information without consent. In addition, it should be made explicitly clear that the collection and use of personal information for authorized business activities are still subject to the overarching requirement that they be done for purposes that a reasonable person would consider fair and appropriate in the circumstances. Establishing a link to the fair and appropriate purposes clause would provide the third necessary guardrail to ensure these business activities (most notably, the "exercise of due diligence to prevent or reduce the organization's commercial risk") are carried out responsibly and respectfully in the absence of consent.

Ontario's proposal related to business activities has noticeably removed from its list what in our view was one of the most concerning provisions in Bill C-11, namely "an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual." We strongly support the removal of this business activity from an eventual law.

We remain concerned, however, with the possibility of expanding the scope of permissible business activities by way of regulation at a later date. As a result of this provision, new business activities can be easily added without the important checks and balances that come with the process of legislative amendment. We recommend removing the possibility of prescribed activities from the list of business activities.

IV. DATA TRANSFERS TO SERVICE PROVIDERS FOR PROCESSING

Given the practical reality of how most companies operate and stay competitive in a modern business context, we would support the proposed authorization for organizations to transfer personal information to third party service providers without requiring consent of individuals in each case. With a few caveats that follow, we agree with Ontario's proposal to allow an organization to transfer an individual's personal information to a third party service provider for processing and to allow the service provider to use such information only for the same purpose for which it was transferred to it.

We would, however, recommend some necessary improvements. First, we would recommend that the language in these provisions use the term "transfer" more consistently in the context of third party processing, to distinguish these types of transactions from cases of outright disclosures. Second, we recommend that the organization which transfers

personal information to a service provider for processing only be allowed to do so if it maintains control over the information by ensuring, among other things, that the processing is carried out on its behalf and at its direction, and for the same lawfully authorized purpose for which the personal information was collected in the first place. Third, both the organization and its service provider(s) must be subject to clear accountability requirements which explicitly apportion responsibility between them[55] (please see section on Accountability below).

V. DISCLOSURES TO LAW ENFORCEMENT AGENCY

Provisions enabling disclosures to law enforcement without consent typically exist in Canadian privacy laws. However, in our view, Ontario's current framing of the proposed disclosures to law enforcement should be defined with greater precision to minimize the risk of unjustified incursions on constitutionally protected privacy rights.

As is, the proposal would permit organizations to disclose personal information to a law enforcement agency in Canada if 1) there are reasonable grounds to believe that an offence has been committed *and* 2) the disclosure would enable the law enforcement agency to determine whether to conduct such an investigation (emphasis added).

On the one hand, to be practical and in light of our experience interpreting similar provisions under public sector laws, we would recommend that the first condition of the provision be broadened to also permit disclosure where there are reasonable grounds to believe that a crime is being or is about to be committed.

On the other hand, we would recommend narrowing this provision in three ways. First, to avoid overbroad disclosures, we recommend that the second condition of the provision be narrowed to only allow disclosure of personal information to the extent it is reasonably believed to be *necessary* to enable the law enforcement agency to determine whether to conduct an investigation. Second, the terms "law enforcement agency" and "investigation" should be clearly and narrowly defined to prevent undue expansion of the provision. Third, we recommend that the provision be clarified to specify that such disclosure must be *at the initiative* of the organization rather than at the request of the law enforcement agency.[56] To deal with instances where disclosure is requested by a law enforcement agency, we recommend that a separate provision be included to require the law enforcement agency to identify their lawful authority and indicate the reason for their request before any such disclosure could be made. Sections 44 and 45 of Bill C-11 offer an example of this important distinction between disclosures requested by law enforcement, and disclosures made at the initiative of an organization, respectively.

Finally, and as will be explored further below under the Transparency section, we are of the view that any future Ontario law should include requirements for greater transparency in relation to these disclosures to law enforcement. Such transparency requirements would allow the public to have a better understanding of the prevalence of organizations

disclosing personal information to law enforcement, especially in circumstances of warrantless disclosures.

VI. INVESTIGATION OR LEGAL PROCEEDING

Under this provision, an organization may collect, use or disclose an individual's personal information if it is reasonable for the purposes of an investigation or legal proceeding. In our view, this provision is also too broad and should be appropriately scoped and circumscribed to avoid unwarranted privacy incursions.

We recommend that the terms "legal proceeding" and "investigation" be clearly defined. We also recommend that the proposed provision be teased out into two or more separate provisions so as to set out the specific conditions that attach to each case.

In the case of investigations, the legislation should specify what type of investigation is intended to be covered. Is it intended to cover investigations into a breach of an agreement or contravention of a law? Is it intended to cover investigations carried out by the organization itself, a designated third party investigative body, or another organization? The legislation should also significantly tighten the conditions attached to such collection, use or disclosure. Similar to Bill C-11, we would recommend including as conditions that the organization have reasonable grounds to believe that a breach of an agreement or contravention of a law has been, is being, or is about to be committed; that obtaining a person's consent would likely compromise the availability or accuracy of the information; and that the information is reasonable for the purpose of carrying out the investigation.

With respect to legal proceedings, we recommend that the provision be amended to clarify, also similar to Bill C-11, that disclosure of personal information can be made to comply with a subpoena, warrant, court order or similar requirement issued in a proceeding by a person having jurisdiction to compel the production of such information or to comply with a procedural rule relating to the production of such information in a proceeding. (See also section 41(1)(d) of *PHIPA* for similar wording).

VII. EMPLOYEE'S PERSONAL INFORMATION

The government's proposal includes new protections for the collection, use and disclosure of employee information. As indicated in our opening remarks, filling the gap on employee privacy would constitute a major and significant advancement of privacy rights in Ontario.

As currently proposed, however, we are concerned that the new provisions are overly broad and would allow an employer to collect, use and disclose any information about an employee as is reasonable for managing the employment relationship. Both *PIPEDA* and C-11 critically require that the collection, use and disclosure be necessary for establishing, managing or terminating the employment relationship and that employees be provided

with notice of the purported information practices. We strongly urge the government to introduce similar requirements of necessity and notice in an eventual Ontario law.

VIII. RESEARCH IN THE PUBLIC INTEREST

The proposed provision allowing research in the public interest is clear and enabling, yet also subject to a number of reasonable privacy protections. In our view, it represents an improvement over the equivalent provision that currently exists in *PIPEDA,* which we understand was significantly underutilized.

However, as currently proposed, the draft research provision would require that the research *relate to* the public interest. In our view, this condition should be further strengthened to only allow non-consensual use or disclosure of an individual's personal information where the research purpose is intended to *advance* the public interest.

IX. PUBLICLY AVAILABLE INFORMATION

The white paper proposes that an organization may collect and use an individual's personal information without consent if the personal information is publicly available and the collection is consistent with the purposes for which the personal information was made publicly available, the context and the reasonable expectations of the individual.

The fact that personal information may be accessible online does not mean that an individual has no reasonable expectation of privacy in it. Recent cases such as the Canadian privacy commissioners' investigation of Clearview AI[57] highlight the risk of organizations engaging in indiscriminate mass scraping of the internet and extracting personal information for the purpose of monetizing it — often leaving the affected individuals none the wiser and opening them up to privacy and other harms.

We are pleased to see that the government's proposal regarding publicly available personal information includes important requirements that the collection be consistent with the purpose and context in which the information was made publicly available and the reasonable expectations of the individual. However, to further enhance individual privacy in what could otherwise be open season on all personal information online, we invite the government to also consider criteria inspired by the definition of publicly available information recently adopted in the *Communications Security Establishment Act, S.C. 2019, c. 13, s. 76*, namely: information 1) that has been published or broadcast for public consumption, 2) is accessible to the public on the global information infrastructure or otherwise is available to the public on request, and 3) (most importantly) in which an individual has no reasonable expectation of privacy.

Also, in light of the government's policy objective of protecting vulnerable populations, especially children and youth, we recommend that the government seriously consider explicitly excluding from the definition of publicly available personal information any

personally identifiable information about youth or children that has been posted online (particularly on social media websites). In such cases, an organization seeking to use personal information of children or youth posted online would not have free rein to do so but would have to rely on another authorized ground, such as consent or research in the public interest.

4. DATA TRANSPARENCY FOR ONTARIANS

As set out in our October 2020 submission, the inclusion of transparency in a modern private sector privacy law will be one of its most important principles and is the critical lynchpin of its success. Transparency requirements can serve multiple and distinct purposes:

i. **For individuals**, they are an essential component of obtaining meaningful consent to the collection, use and disclosure of personal information;

ii. **For the broader public,** they afford an essential opportunity to understand and compare data management practices across competitors in an industry; and,

iii. **For regulators and oversight bodies**, they allow scrutiny of an organization's practices to ensure compliance and hold organizations to account.

With respect to the information disclosures that must be provided to individuals at the time of seeking meaningful consent, these disclosures must be relatively concise, timely and actionable, with greatest emphasis on the most impactful considerations that will likely inform individual choice and decision-making. On this topic, please see our comments above under "Valid Consent."

With respect to the second purpose mentioned above — dissemination of an organization's data management practices to allow the public to make comparisons across organizations — we support the white paper's proposal to require organizations to be transparent about their information management practices whether they are relying on consent or another authorized ground.

For this second purpose, we believe that the transparency requirements listed on pages 27-28 of the white paper represent a good baseline of generally *useful*, but not necessarily exhaustive, information to be provided to individuals. For example, while it is useful for the public to understand what data is being collected by the organization, there may be added value in describing the source of that information. Moreover, much work is currently underway to explore how such information could be provided in more effective ways.[58] As such, any proposed legislation should, at minimum, be designed to leave open both the list of general transparency requirements and the possible new approaches for achieving transparency in light of evolving research in this area.

Another beneficial addition to transparency requirements for the general public would be a provision requiring organizations to generate annual public reports outlining basic

statistics on the numbers, types and outcomes of law enforcement requests for access to personal information held by those organizations[59]. Privacy authorities internationally have been calling for this enhancement to transparency and accountability for some time, including through a resolution[60] at the 37th International Conference of Data Protection and Privacy Commissioners in 2015. These transparency reports are an important tool towards ensuring both that government and law enforcement agencies are acting responsibly and that organizations are exercising due diligence when receiving disclosure requests. The potential content of transparency reports and related disclosure policies is discussed in the IPC's 2018 *Disclosure of Personal Information to Law Enforcement* fact sheet[61] as well as the Government of Canada's *Transparency Reporting Guidelines.*[62]

Finally, the third purpose of transparency is to allow scrutiny of an organization's practices by privacy regulators and oversight bodies (in this case, the IPC) to ensure compliance, assess systemic risk factors and hold organizations to account for their obligations under a private sector privacy law. Examples of this type of transparency should include obligations of organizations to make their privacy policies, practices and procedures available to the IPC on request; to provide annual privacy breach statistics to the IPC on request; to report to the IPC in the event of a breach of security safeguards that poses real risk of significant harm; to show records of privacy impact assessments for data processing above a defined risk threshold (including any associated assessments of algorithmic impacts that significantly impact individuals); and to notify the IPC of an organization's intention to use or disclose personal information without consent for research in the public interest.

To be clear, such transparency obligations would not immunize non-compliant organizations. The IPC must still be able to act on the information it receives to work with the organization to resolve issues identified, and should such resolution not be possible (or in the case of egregious non-compliance), to take enforcement action.

I. ENHANCING ACCOUNTABILITY

In addition to the transparency requirements imposed on organizations to *demonstrate* accountability to regulators are the underlying accountability obligations themselves. Substantive accountability must play a central role in any modern privacy legislation that shifts away from a fully consent-based model. Enhanced accountability requirements serve as a counter-point to the increased flexibility organizations are granted to collect, use or disclose personal information without consent in a data-driven economy.

While the obligation for organizations to implement a scalable privacy management program is an important baseline requirement for an accountability 1.0 framework, a modern privacy law must strive for much stronger accountability measures in view of the increasing digital risks at play today and in the future.

At minimum, we would recommend imposing a mandatory obligation to conduct a privacy impact assessment (PIA) above a certain risk threshold, which should include an assessment of algorithmic impacts in the case of automated decision systems that

significantly affect individuals (see our comments above). This requirement would be consistent in principle with the GDPR.[63] To ensure an appropriate measure of flexibility, we would recommend that the required components of a PIA be prescribed by regulation or set out in guidance in order to ensure a systematic methodology for identifying, evaluating, mitigating and managing risks to data subjects.

We would not suggest that PIAs should be required for *all* collections, uses and disclosures of personal information as this might result in significant administrative costs that would unfairly burden organizations. However, where a collection, use or disclosure introduces significant risks above a certain threshold, PIA's should be required to avoid unfairly transferring the costs and related burdens onto individuals who would otherwise have to bear the brunt of ill-conceived initiatives.

II. ACCOUNTABILITY AND SERVICE PROVIDERS

A modern private sector privacy law must set out a clear and coherent regime for apportioning accountability among the multiple actors involved in complex data processing arrangements. Accordingly, we recommend that any proposed legislation clearly lay out the obligations of both transferring organizations and their service providers.[64] (See our comments above under Data Transfers to Service Providers for Processing.)

The organization that lawfully transfers personal information to a third party service provider to process it on its behalf should retain control over the personal information and ultimately remain accountable for it.[65] Among other obligations, the transferring organization should be required to ensure, through contractual or other means, that 1) the service provider can only process the data in accordance with the lawfully authorized purpose that the organization transferred it and 2) that the service provider will provide a level of privacy protection equivalent to that which the transferring organization is required to provide under the law. If the service provider is located outside the province, as many increasingly are, the transferring organization should be required to disclose this fact among its transparency obligations, along with a description of the related risks and implications. The transferring organization should also retain responsibility for responding to requests for access or disposal and for notifying individuals and/or reporting to the IPC in the event of a data breach.

For their part, service providers should be restricted from using or disclosing the personal information for any purpose other than the purpose for which the organization transferred it to them for processing. They should be required to provide the same level of protection as the transferring organization is obliged to provide under the law. Service providers should also generally be required to refer access or disposal requests to the organization, to immediately notify the organization in the event of a data breach and to collaborate with the organization in investigating, mitigating and containing such breach. Such general requirements should be set out in the legislation itself, supplemented by regulation and/

or guidance, as appropriate, to elaborate upon the more granular elements that should be addressed in any contractual arrangement between the organization and the service provider.

5. PROTECTING CHILDREN AND YOUTH

We applaud the government's proposal to address important issues such as substitute decision-makers and the minimum age thresholds for valid online consent in an Ontario private sector privacy law.

At the same time, we think a balanced approach would recognize that a youth's wishes may not always align with their parents'. For example, young teens may not agree with their parents' request to access or take down personal information they posted about themselves on social media sites as a means of expression. Conversely, teens may object to their parents' posting of photos or other personal information about them online. For these and other reasons, we would recommend that a private sector privacy law recognize the right of mature minors between the ages of 13 and 16 to object to their parental consent or parental requests on their behalf and that their objection should prevail.

Also, consistent with our views above, youth should have a broad right, even without parental consent, to have information they posted about themselves de-indexed, taken down, and in some cases deleted at source[66], subject to narrow exceptions. This is a proposal we advanced in our initial submission, recommending that minors deserve special consideration to support their freedom of experimentation and self-discovery and their ability to learn and change their minds at a young age without worrying about the permanent reputational impacts of information they post about themselves online.

Finally, the government has proposed to develop supplementary codes of practice that resemble those introduced in other jurisdictions. For example, the United Kingdom's Information Commissioner's Office has produced a strong code[67] in this regard, which "seeks to protect children within the digital world, not protect them from it."[68] The IPC supports the government's proposal and would be pleased to be involved in the development of a similar code of practice for Ontario to bring greater specificity to children's protection online.

6. A FAIR, PROPORTIONATE AND SUPPORTIVE REGULATORY REGIME

I. PROACTIVE SUPPORT

i. Codes of Practice and Certification Programs

Anecdotally, one of the most common stakeholder requests privacy regulators receive is "what do we have to do to be compliant with the legislation?" While we seek to be supportive through consultations, we see great potential for more detailed and proactive

delivery of guidance through the collaborative development of codes of practice and certification programs. Codes of practice can provide clear benefits for Ontarians (who receive greater transparency about the practices of an organization in an 'at-a-glance' format) and organizations (who receive a measure of regulatory certainty for their own practices and can more securely engage with service providers and partners who are certified against the code).

Of course, rigorous requirements would have to be established for regulatory approval of a code, any amendments thereto, and any third party certification program put in place to ensure ongoing monitoring of those organizations claiming adherence to it (as is the case under the GDPR[69] and Bill C-11[70]). To the extent compatible, a proposed Ontario law can also provide for reciprocal recognition of codes of practice and certification programs approved by the federal regulator and vice versa. Importantly, however, adherence to a code and certification program must not be allowed to fetter the discretion of the regulator. While compliance with a code of practice or obtaining certification will be relevant in assessing compliance with the law, they are not determinative of compliance with the law. The IPC must always have the residual authority to assess the application of the law to the specific facts and circumstances of individual complaints, any changes or deviations from an organization's practice or policy, and any novel, emerging risks.

ii. Flexible Regulatory Schemes

As noted in our prior submission, we would also encourage the government to consider adopting some of the agile and cutting-edge regulatory tools that are currently being tested in other jurisdictions.

The primary example of this is the "regulatory sandbox," a supervised, safe haven where organizations can experiment and test innovative products and services to ensure compliance with legislative and other requirements under the supervision of the privacy regulatory authority. We have seen this approach adopted by the **UK Information Commissioner's Office**[71], the **Norwegian Data Protection Authority**[72] (specifically for AI), and the **Ontario Energy Board**[73], among others. Again, the overall purpose would be to provide a modern and flexible means by which the regulator can support *privacy respectful and compliant* innovation by Ontario organizations in a secure and supervised environment.

iii. Providing Guidance and Advice

We would support a private sector privacy law that supplements enforcement measures with a range of supportive tools that foster and encourage regulatory compliance. Such tools include educational materials such as practical, transparent and comprehensive guidance and best practices, developed in consultation and collaboration with organizations and individuals. As noted by the government, the IPC has a long history of issuing guidance on the statutes we administer.[74] Other tools include advisory services in

respect of novel forms of data processing, and funding and publishing research in areas of emerging risk.

Like codes and certification programs, however, such tools cannot fetter the IPC's discretion in assessing compliance with the law. While guidance, advice, research and other resources will be important sources to consider, an individual complaint will still have to be assessed according to the application of the law to the specific facts and circumstances, any changes or deviations from an organization's practice or policy, and any novel, emerging risks. Also, in order to appropriately direct resources, focus on areas of highest systemic risk and provide generalizable value to organizations across a sector or industry, the IPC should have the discretion to determine which guidance, advice or research to undertake. In this regard, we would caution against the approach taken in Bill C-11[75] that requires the privacy commissioner to provide guidance at the request of an individual organization, which may create unfair competitive advantage in the marketplace and unduly drain public resources with little return on investment.

II. ENFORCEMENT REGIME

The IPC is broadly supportive of the enforcement framework being considered by the government for a made-in-Ontario private sector privacy law. In particular, the enforcement options address some of the most significant weaknesses in Bill C-11 and respond to many of the recommendations made by the IPC in its previous submission on private sector privacy legislation in Ontario.[76]

i. Investigative and Order-Making Powers

The modern privacy landscape requires a regulator with strong investigative and order-making powers. The IPC is pleased that the government recognizes this and is considering a legislative model that provides the IPC with the power to issue orders requiring organizations to comply with the law, cease contraventions of the law, make public the measures they have taken to fulfil their obligations, and destroy any personal information collected unlawfully.

The power to issue orders must be supported by robust yet flexible investigative powers. The IPC must have the power to commence an investigation in response to a complaint or on its own initiative. To ensure resources are appropriately directed at the most pressing issues, the IPC must also have the discretion to determine which matters should be investigated and to discontinue investigations. The IPC is pleased that the government has recognized the importance of providing the IPC with this discretion.

While the IPC is broadly supportive of the enforcement model under consideration by the government, we would recommend a few specific improvements. First, the power to issue orders should not be limited only in respect of "organizations," but also in respect of service providers to ensure they too comply with their relevant obligations under the

proposed act and its regulations (see our recommendations above, "Data transfers to service providers for processing").

Second, IPC orders relating to data mobility, disposal, de-indexing, access and correction rights should not be subject to appeal to the courts but rather judicial review. This would make the proposed law more practical, efficient and consistent with other statutes administered by the IPC[77] aand help ensure that IPC orders relating to these rights have a greater degree of certainty and finality.

ii. Administrative Monetary Penalties

Regulation of the private sector must recognize the economic value of personal information while also creating effective financial incentives to encourage compliance and ensure organizations do not profit from non-compliance. One tool to create such financial incentives is the use of administrative monetary penalties. The IPC supports introducing an administrative monetary penalty regime in an Ontario private sector privacy law. We further agree that administrative monetary penalties should be ordered by the IPC rather than by a separate administrative tribunal like that proposed in Bill C-11.

In our view, the proposed administrative monetary penalty provisions generally strike the right balance. They are similar to those in Ontario's *PHIPA* while adapted for the private sector context. The proposals also give appropriate discretion to the IPC to decide whether to issue an administrative monetary penalty and provide a list of factors for the IPC to consider.

While the IPC is broadly supportive of the model proposed by the government, we recommend several improvements. First, the draft provisions limit administrative monetary penalties to only "organizations." In our view, administrative monetary penalties should also apply to service providers in cases that warrant it. Given their important data processing responsibilities, we recommend that they too be covered in an eventual law (see our recommendations above, "Data transfers to service providers for processing").

Second, the administrative penalties provision, as proposed, would only apply to contraventions of the act. Ontario's private sector privacy law should consistently ensure that contraventions of regulations could equally result in administrative monetary penalties.[78]

Third, we recommend that the maximum amount of an administrative monetary penalty for an organization that is an individual be increased to $100,000. While $50,000 may be a significant penalty for many individuals, it is unlikely to meaningfully deter conduct that seeks to derive economic benefits far in excess of $50,000 in cases of significant non-compliance. On the other hand, the IPC agrees that the maximum amount proposed for an organization that is not an individual is appropriate, recognizing that the amounts listed are maximums, and the determination of the actual amount of an administrative monetary penalty will be based on the particular facts and circumstances of each case.

Fourth, the factors to consider when deciding whether to issue an administrative monetary penalty should be expanded to take into account whether a penalty or fine

has already been imposed under other privacy and access legislation in relation to the same facts and circumstances. This will help ensure the interoperability of Ontario and other Canadian privacy and access legislation such that organizations are not overly (or unfairly) penalized monetarily.

iii. Offences

The IPC strongly agrees that an Ontario private sector privacy law should include a regime for statutory offences. This enforcement tool is an important instrument to sanction egregious contraventions while also deterring them from occurring in the first place.

We generally agree with the example offences proposed in the white paper, including where an organization re-identifies personal information that has been de-identified; seeks retribution against a whistleblower; fails to report a breach of security safeguards to the IPC; fails to maintain a record of every breach of security safeguards; fails to retain information subject to an IPC inquiry; or fails to abide by an IPC compliance order. In addition to these, we would recommend the inclusion of the following offences:

- Willfully collecting, using or disclosing personal information in contravention of the law;[79]
- Willfully making a false statement to mislead or attempt to mislead the commissioner in performing his or her functions under the law;[80]
- Making a request for access, correction, portability, disposal or de-indexing or relating to automated decision systems under false pretenses;[81]
- Altering, concealing or destroying personal information or causing a person to do so with the intent of denying a right under the law; [82] and
- Dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging a person who (a) disclosed a privacy breach to the commissioner; (b) did something required under the act or its regulations; (c) or refused to do something the act or its regulations prohibits.[83]

Including these will ensure that some of the worst contraventions of Ontario's private sector privacy legislation constitute punishable offences, consistent with their treatment under other Ontario privacy laws, such as *PHIPA*.

We also note that the offence provisions provided in the white paper apply only to organizations. Consistent with Ontario's other privacy laws[84], the offence provisions should extend beyond organizations and apply to any person. Further, we recommend that the maximum fine for individuals found guilty of an offence be lower relative to the proposed fines applicable to non-individuals.

iv. Power to Order Compensation

One question raised in the white paper is whether the IPC should have the ability to order that individuals be compensated in the event of a privacy breach. In our view, where individuals have been affected by a breach, there could be a simplified process for obtaining a base level of compensation that reflects the overall nature of the risks created by the contravention. In that regard, the IPC could have the ability to issue an order requiring that discrete amounts in financial compensation be paid. For example, the IPC could order that credit monitoring services and identity theft protection be provided to individuals affected by a privacy breach or that the costs of cancelling or prematurely terminating a contractual relationship with the organization be waived.

Through its early resolution processes and interest-based mediation efforts, the IPC could bring the parties to a mutually satisfactory resolution which may include a one-time modest financial award to each affected individual, obviating the need for an investigation and possible order.

However, while the IPC may be uniquely positioned to assess the general nature of a breach, broad risks created for affected individuals and appropriate mitigation measures, we are not uniquely placed to assess individual damages. Individual claims for damages would best be addressed through the courts.

Accordingly, individual claims for compensation should be addressed by ensuring the availability of a private right of action for damages where the IPC finds a contravention of the law or where a person has been convicted of an offence under the law.[85]

7. SUPPORT FOR ONTARIO INNOVATORS

I. DE-IDENTIFIED INFORMATION

i. Permitted Use of De-Identified Information

As noted in the white paper, the de-identification scheme being proposed is consistent with that proposed by the IPC in its earlier submission to the government's private sector privacy consultation. Generally speaking, the scheme defines a threshold at which information is considered "de-identified" — still subject to privacy legislation but afforded greater flexibility for its use in certain defined situations. It also defines "anonymized information," which would be outside the four corners of the law.

ii. Definition of De-identified Information

The identifiability of information can be understood as being along a spectrum. In a binary model, this spectrum is divided into "personal information," which is identifiable, and "non-

personal information," which is not. There is, however, no statutory bright line between these two states. Fuzzy interpretations of identifiability by organizations result in either risky information management practices flying completely under the radar or, conversely, reticence risk impeding fair competition and healthy innovation. Attempts to help organizations distinguish between these two states of information have been undertaken through guidance, regulation, codes of practice and/or the courts.

Ontario has proposed a three-state model: personal information, de-identified information and anonymized information. Although "personal information" is not defined in the white paper, presumably it would take on the universally accepted meaning of "information about an identifiable individual" (see our earlier comments under "Definitions of Personal Information and Sensitive Personal Information"). The proposal defines "de-identified information" as "information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information." The proposed definition of "anonymized information" would be "information [that] has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person."

Because an organization's obligations would differ with respect to each of those three states, it is critical that the states be well-defined. To that end, we recommend that the middle state of "de-identified information" be defined as follows:

> "**De-identified information**" means information that does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual, but still presents a residual risk, however minimal, of re-identifying an individual."

The addition of a threshold — namely "reasonably foreseeable circumstances" — allows for appropriate governance mechanisms (physical, technical and administrative) to be put in place, either internal or external to an organization, to effectively and securely segregate de-identified data from any other information that may be combined and used to re-identify an individual.

The insertion of the final clause referring to "residual risk, however minimal, of re-identifying an individual" is intended to better differentiate de-identified information from anonymized information, helping organizations more clearly determine when information remains subject to the law or falls outside the law and enabling a more consistent approach to de-identification across sectors[86] and jurisdictions.[87]

As for anonymized data, many might argue that this state of data is illusory and that personal information could never be truly anonymous anymore.[88] While this is increasingly true in light of evolving information technologies and the pervasive amount of personal information widely available online, there remain some forms of statistical data that are aggregated at sufficiently high level to permit its further use and public release without any risk of re-identification.[89] Moreover, providing for anonymized data leaves open the

possibility for some emerging privacy-enhancing technologies (e.g., synthetic data) to eventually attain or re-attain this state of anonymization, allowing it to be more liberally used for innovative purposes while posing effectively zero risk to individuals.[90]

iii. Application

We strongly support bringing de-identified information within the scope of a private-sector privacy legislation. However, we would emphasize that it is important to do so explicitly. We recommend that this be done within the application section of the proposed law.

For clarity and ease of interpretation, this section might also enumerate the sections that continue to apply to de-identified data and those that do not. At minimum (and subject to any necessary targeted exceptions), we would recommend de-identified data remain subject to those provisions relating to organizational accountability, fair and appropriate purposes, safeguards, openness and transparency, and challenging compliance. The provisions which we recommend apply to de-identified information should also be subject to appropriate-level enforcement measures in cases of non-compliance.

We would also recommend that an Ontario law should incentivize organizations to de-identify data as much as possible. For example, when de-identification is used as a safeguarding measure, this could be a due diligence consideration or a mitigation factor when assessing compliance and applying the enforcement measures more generally. Moreover, the law should clarify that organizations are permitted to use or disclose de-identified data in any circumstance in which it is authorized to use or disclose the original personal information from which the de-identified data was generated.

With respect to the proposed provision calling for proportionate technical and administrative measures to be applied to de-identified data, we are comfortable with the risk-based approach that takes into account the purpose for which the information is de-identified and the sensitivity of the personal information. For further clarity, we would recommend adding consideration of the context as well as the risks of re-identification.

We strongly support creating a prohibition against using or attempting to use de-identified information for the purpose of re-identifying an individual (subject to narrow exceptions), as well as the related offence for knowingly contravening such a prohibition.

Finally, we would recommend clarifying transparency requirements for the use of de-identified *and* anonymized information. As currently proposed, organizations would be required to provide a "general account" of their use of de-identified information. In our view, simply stating that information will be "de-identified and used for internal research and development" or "for socially beneficial purposes" would not likely meet the policy intent of achieving meaningful transparency. Individuals whose personal information will be de-identified to advance these other purposes have a right to know what these purposes are, particularly where there are residual risks of re-identification. Much like investors who avoid putting their money in investment funds that are not aligned with their ethical values,

individuals should have visibility into what will be done with their personal information and at least have the option, wherever possible, of avoiding organizations that engage in what they believe to be objectionable practices. What additional detail would be required to satisfy this level of transparency could likely be established through guidance.

A similar argument in favour of general transparency requirements could be made in respect of anonymized information that is derived from individuals' personal information at source. However, this question requires further reflection since, admittedly, there is less, if any, privacy interest remaining in anonymized information. Moreover, the proposed definition of anonymized information — as information to which the act would not apply — would have to be brought back within the scope of the act for the sole purpose of the transparency requirement.

To support "transparency to the regulator," we also recommend that organizations be obliged to maintain records of their de-identification process. This could be part of a PIA to be made available to the regulator on request. Particularly above a certain risk threshold, where the original data from which the de-identified information has been derived is sensitive or the intended use can significantly affect individuals, an organization should clearly document the steps it has taken to de-identify the data, the basis on which it assesses those steps to be sufficiently effective and the grounds on which it reasonably believes the purposes of the research or innovation are fair and appropriate. This transparency requirement would create important visibility for regulators and due diligence for organizations.

II. POTENTIAL OTHER MEANS OF SUPPORTING INNOVATORS

With respect to the final question regarding safeguards or governance models to enable sharing of de-identified information for socially beneficial purposes, this is an area we continue to study and on which we intend to further develop our position and recommendations.

Interestingly, commentators, such as Wu et al.[91], have noted that a focus on permitting innovative use of personal information already held by the organization will inevitably favour larger organizations that hold large datasets. This can create a situation in which "a few special organizations, due to their data monopolies and technical resources, are able to decide which problems are solved and how." However, as new data governance models arise that permit data sharing, "less-resourced innovators — including individual researchers, citizen developers, local communities, and small-and-medium-sized enterprises — can access sufficient data to fuel AI and data analytics, reframe problems and solve them in new ways." [92]

Innovative governance models intended to promote greater, more equitable and more timely access to government data by all sectors of Ontario's economy are also expected to emerge as part of the government's Digital and Data Strategy.[93] While efforts to promote broader data sharing are certainly laudable and should continue to be encouraged, we

recommend that appropriate governance models, with effective, independent oversight mechanisms, be seriously considered, designed and implemented at the earliest possible time given all of the important privacy, security, fairness and equity implications at play. Ontario is uniquely-positioned to design a coordinated, cross-sectoral governance model that will bring forth the intended benefits of open data for the province, with the commensurate privacy and security protections in place.

D. CONCLUSION

Many important measures were not raised in the government's white paper, including mandatory breach notification, definition and application provisions, provisions setting out what happens in the event of a conflict for organizations regulated by other statutes, retention of personal information and transitory provisions. Further, where measures are raised, detailed drafting language was sometimes not provided. It is our assumption that these and other standard and critical provisions would be featured in an eventual bill, should the government decide to proceed, and we look forward to engaging in more detailed discussion as the legislative process continues.

At the end of the day, it continues to be our view that Ontario should proceed with a made-in-Ontario private sector privacy law whether or not *PIPEDA* reform eventually happens federally. Doing so will ensure a more timely response to the ever-increasing risks Ontarians are facing as they increase their digital activities in all aspects of their lives. It will also introduce a much-needed human rights-based approach to privacy, privacy protections for employees, enhanced focus on youth and children and coverage of a far broader spectrum of organizations that currently hold significant amounts of personal information without any general privacy obligations. This will also enable government to craft an Ontario-focused law that takes into account the needs of local businesses struggling to survive post-pandemic and looking for opportunities to compete, grow and thrive in a data-driven economy. And most importantly, it will allow Ontario to design a world-leading data governance model that supports respectful and sustainable innovation, in a manner that protects the privacy of Ontarians and earns their trust and confidence for the future.

Thank you for the opportunity to respond to the government's proposals. We hope the comments above will contribute to the public discourse and assist the government in making its decisions and choices. Our office stands ready and committed to work together with the government to advance this important initiative in the interest of all Ontarians.

ENDNOTES

1 Ontario government. "**Modernizing Privacy In Ontario**" (June 17, 2021)

2 Office of the Information and Privacy Commissioner of Ontario, "**Submission to the Ontario Government's discussion paper, Improving private sector privacy for Ontarians in a digital age**" (October 16, 2020) retrieved on July 9, 2021.

3 Ontario government, "**Ontario Private Sector Privacy Reform: Improving private sector privacy for Ontarians in a digital age**" (13 August 2020), retrieved on August 8, 2021.

4 Ontario government. "**Modernizing Privacy In Ontario**" (June 17, 2021)

5 See section 26(2)(b) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

6 Lisa Thompson, Minister of Government and Consumer Services "**Statement - Strengthening Privacy Protections for Ontario's Digital Future**" (June 17, 2021), retrieved on July 12, 2021.

7 According to Statistics Canada, Key Small Business Statistics Report 2020, the small-medium sized enterprise (SME) sector accounted for 86.4% (or 4.2 million) of Ontario's private sector employees.

8 Professor Teresa Scassa, "**Privacy in the Precision Economy: The Rise of AI-Enabled Workplace Surveillance during the Pandemic**" (June 8, 2021), retrieved on June 30, 2021, Vass Bednar, "**Your boss is watching you while you work**" (August 18, 2020), retrieved on June 30, 2021; ; Darrell M. West, "**How employers use technology to surveil employees**", The Brookings Institute (January 5, 2021), retrieved on August 27, 2021.

9 KPMG Business Outlook Poll, "**Sixty-two per cent of businesses plan to mandate employee vaccines**" (August 19, 2021), retrieved on August 23, 2021. See also: Canadian Lawyer, "**Workplaces showing trend toward mandating COVID vaccinations for employees**" (August 20, 2021), retrieved on August 23, 2021, and Canadian Lawyer, "**Can employers require new hires to show proof of vaccination?**" (May 17, 2021), retrieved on June 30, 2021.

10 ZDNet, "**One of New York's largest nonprofits suffers data breach**" (May 31, 2019), Insurance Business America, "**Non-profits are a target for data breach**" (April 16, 2019), Charity Village, "**Minimizing the risk of a data breach: a guide for non-profit organizations**" (March 8, 2017), all retrieved August 12, 2021.

11 Lawyers Daily, "**Critical privacy, security risks for charities, not-for-profits**" (June 10, 2021) retrieved on July 10, 2021.

12 CBC News, "**Data theft from Meals on Wheels reveals gap in provincial privacy legislation, expert says**" (July 11, 2021) retrieved on July 12, 2021.

13 *Personal Information Protection Act, S.B.C. 2003, c. 63*

14 National Assembly of Quebec, ***Bill 64, An Act to modernize legislative provisions as regards the protection of personal information*** (June 12, 2020) s. 81, retrieved on August 1, 2020.

15 Elections Ontario, "**Realizing Change and Planning for the Future"**, 2018-2019 Annual Report

16 Globe and Mail, **"Liberals face possible federal, provincial privacy probes for use of facial recognition technology" (June 24, 2021)**, retrieved on July 19, 2021.

17 Figures are drawn from the Ontario Student Drug Use and Health Survey and are based on students in grades 7-12 unless otherwise indicated. Boak, A., Elton-Marshall, T., Mann, R. E., and Hamilton, H. A. (2020) **The Mental Health and Well-being of Ontario Students, 1977-2019**: Detailed findings from the Ontario Student Drug Use and Health Survey. Toronto, ON: Centre for Addiction and Mental Health.

18 International Journal of Behavioral Nutrition and Physical Activity "**Impact of the COVID-19 virus outbreak on movement and play behaviours of Canadian children and youth: a national survey**" (July 6, 2020) retrieved August 12, 2021.

19 Kathryn Rattigan, "**Smart Toys and How they May be Invading our Privacy**" (July 15, 2021)

20 Office of the Information and Privacy Commissioner of Ontario, **MC18-48** and **MC17-52**.

21 Ontario Chamber of Commerce, "**Ontario Economic Report 2020"**

22 Ontario government, "**Ontario's Digital and Data Strategy**" (April 30, 2021), retrieved August 12, 2021.

23 See **IPC Annual Report 2021** which shows, consistent with past years, that the vast majority of public sector and health sector files get resolved by way of early resolution and mediation.

24 Ontario government, "**Ontario's Digital and Data Strategy**" (April 30, 2021), retrieved August 12, 2021.

25 *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*, s. 26(2)(b)

26 *EU General Data Protection Regulation*, Article 45, and European Commission, "**Adequacy Decisions**".

27 Teresa Scassa, "**A Human Rights-Based Approach to Data Protection in Canada**," in Dubois, E. and Martin-Bariteau, F. (eds.), Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa, ON: University of Ottawa Press (2020).

28 *Nammo v. Transunion of Canada Inc.*, 2010 FC 1284 at paragraphs 74 and 75; *Bertucci v. Royal Bank of Canada*, 2016 FC 332 at para 34

29 ***Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723*.**

30 ***Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723***, at para 30, cited by Professor Teresa Scassa **"First Step Along the Path to a Right to Be Forgotten in Canada?" (July 9, 2021), retrieved on July 12, 2021**

31 See, for example, Global Privacy Assembly, "**Policy Strategy Working Group 1: Global frameworks and standards**" (October 2020), retrieved July 12, 2021, which found that 8 of 10 global privacy frameworks "make specific reference to independence requirements" of privacy authorities.

32 Washington University Law Review, **"Privacy Law's False Promise"** (December 2019), retrieved July 9, 2021.

33 European Data Protection Board, "**Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"** (November 2019)

34 **R v Oakes, [1986] 1 SCR 103; see also Office of the Privacy Commissioner of Canada, "A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century" (November 2010), retrieved August 23, 2021.**

35 Subparagraph (4) of the Fair and Appropriate Purposes provision, entitled "legitimate needs"

36 **Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, s. 2(1)**, **Alberta Personal Information Protection Act s.1(1)(k)**, **Regulation (EU) 2016/679, General Data Protection Regulation**.

37 **R. v. Spencer, 2014 SCC 43 (CanLII), [2014] 2 SCR 212**)

38 **Royal Bank of Canada v. Trang, 2016 SCC 50, [2016] 2 S.C.R. 412**

39 Office of the Privacy Commissioner of Canada, "**OPC updates guidance regarding sensitive information**" (August 13, 2021) retrieved August 18, 2021.

40 Covington "**Five Key Themes from the FTC's Data Portability Workshop"**, (September 30, 2020)

41 U.S. Federal Trade Commission, "**Data To Go: The FTC's Workshop on Data Portability**" (September 2020), retrieved July 28, 2021 and its summary, **"Data To Go: The FTC's Workshop on Data Portability"** (November 2020)

42 Future of Privacy Forum, "**FPF Testifies at FTC Data Portability Workshop**" September 23, 2020, and European Commission, **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition -two years of application of the General Data Protection Regulation** June 24, 2020.

43 For further discussion see: Office of the Information and Privacy Commissioner of Ontario, "**Submission to the Ontario Government's discussion paper, Improving private sector privacy for Ontarians in a digital age**" (October 16, 2020) retrieved on July 9, 2021.

44 National Assembly of Quebec, "**Bill 64, An Act to modernize legislative provisions as regards the protection of personal information**" see s. 113 of the Bill creating s. 28.1

45 Information and Privacy Commissioner of Ontario, "**IPC Comments on the Ontario Government's Consultation on Ontario's *Trustworthy Artificial Intelligence (AI) Framework***" (June 2021), retrieved July 27, 2021.

46 "Automated decision system" means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets;

47 Government of Canada, "**Directive on Automated Decision-Making" (**April 2021), retrieved July 27, 2021.

48 Including regression analysis which is a relatively straightforward and common statistical practice.

49 Ben Green and Amba Kak. Slate, "***The False Comfort of Human Oversight as an Antidote to A.I. Harm***" (June 15, 2021), retrieved July 27, 2021.

50 These include the ability to request access to the personal information used to render the decision (and request it be corrected), to request the reasons and principle factors that led to the decision, the ability to comment on or contest the decision, and the ability to request review of the decision.

51 See subsection 2 ('Same') on page 14 of the white paper. Note that these are largely analogous to those described in Recital 71 and Articles 13(2)(f) and 22(3) of the *EU General Data Protection Regulation.*.

52 See subsection 3 ('Automated Decision Making') on page 10 of the white paper.

53 Office of the Information and Privacy Commissioner of Ontario, "**Submission to the Ontario Government's discussion paper, Improving private sector privacy for Ontarians in a digital age**" page 11 (October 16, 2020) retrieved on July 10, 2021.

54 As confirmed by the Supreme Court of Canada in ***Royal Bank of Canada v. Trang*, 2016 SCC 50, [2016] 2 S.C.R. 412.**

55 *EU General Data Protection Regulation*, Articles 24, 28, and 29.

56 **R. v. Spencer, 2014 SCC 43, [2014] 2 SCR 212**, and **R. v. Orlandis-Habsburgo, 2017 ONCA 649**.

57 "**Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta**" (February 2, 2021), retrieved July 13, 2021.

58 For some time researchers have been exploring the concept of visual displays of privacy information. Perhaps the first well-known effort was the "Privacy Nutrition Label" developed in 2009 by a team from Carnegie Mellon University (**http://cups.cs.cmu.edu/privacyLabel/**). More recently, we have seen efforts such as the IoT [Internet of Things] Security and Privacy Label (**https://iotsecurityprivacy.org/**) and the Digital Trust for Places and Routines iconography (**https://dtpr.helpfulplaces.com/**), and quite prominently Apple's December 2020 launch of Privacy Labels for

App Store apps (**https://developer.apple.com/app-store/app-privacy-details/**). In each case, the intention is to provide individuals with basic necessary information in an easily understood format.

While (excepting Apple's Privacy Labels) none of these efforts have reached a level of broad adoption, as an initial transparency mechanism to provide an "at-a-glance" understanding of an organization's practices this approach shows some promise.

59 For example, number of requests received; number of requests resulting in disclosure; number of required disclosures (for instance, in response to a court order), number of persons whose information was disclosed; etc.

60 Global Privacy Assembly. **Resolution on Transparency Reporting** (October 27, 2015), retrieved July 27, 2021.

61 Information and Privacy Commissioner of Ontario. "**Disclosure of Personal Information to Law Enforcement**." (November 2018)

62 Government of Canada. "***Transparency Reporting Guidelines***." (June 2015), retrieved August 23, 2021.

63 Article 35.1: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

Article 35.3(a): "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."

64 Here, "transferring organization" and "service provider" are roughly equivalent to "controller" and "processor" in the GDPR. Chapter IV of the GDPR entirely sets out the controller/processor relationship, including specific obligations for the controller (Article 24) and the processor (Article 28).

65 For example, in Bill C-11, this is done in section 7(2): Personal information is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.

66 We note that Google has recently taken a first step towards this, announcing its intention to introduce a policy permitting anyone under the age of 18 (or their parents or guardians) to request de-indexing of their images. See Google, "**Giving kids and teens a safer experience online**" (August 10, 2021) retrieved on August 16, 2021.

67 **Section 123 of the Data Protection Act 2018** states that "the Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children." Under section 125(1) "when a code is prepared under section … 123…(a) the Commissioner must submit the final version to the Secretary of State, and (b) the Secretary of State must lay the code before Parliament."

68 United Kingdom Information Commissioner's Office, "**Age appropriate design: a code of practice for online services**" (September 2, 2020) retrieved August 16, 2021.

69 *EU General Data Protection Regulation*, Article 41(1).

70 Bill C-11, ss. 76(3) and 77(1).

71 UK Information Commissioner's Office, "**Sandbox beta phase discussion paper"** (January 30, 2019), retrieved July 27, 2021.

72 Norwegian Data Protection Authority, **"Sandbox for responsible artificial intelligence"** Retrieved July 27, 2021.

73 Ontario Energy Board **"OEB Innovation Sandbox"** Retrieved July 27, 2021.

74 Office of the Information and Privacy Commissioner of Ontario, **"Guidance"**.

75 Bill C-11, s. 109(e).

76 Office of the Information and Privacy Commissioner of Ontario, **"Submission to the Ontario Government's discussion paper, Improving private sector privacy for Ontarians in a digital age"** (October 16, 2020) retrieved on July 10, 2021.

77 *PHIPA* s. 62 and *Child, Youth and Family Services Act*, 2017, S.O. 2017, c. 14, Sched. 1, s. 322 [*CYFSA*]

78 The draft provisions are inconsistent in this regard. Subsection (1) of the draft administrative monetary penalty provisions does not refer to contraventions of the regulations under the Act. Other draft provisions, however, do refer to both the "Act" and "its regulations".

79 See *PHIPA*, s. 72(1)(a). A similar offence is included in Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5, s. 59(1)(a).

80 See *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 61(1)(e) [*FIPPA*]; *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, s. 48(1)(e) [*MFIPPA*]; and *PHIPA*, s. 72(1)(h).

81 See *FIPPA*, s. 61(1)(c); *MFIPPA*, s. 48(1)(c); and *PHIPA*, s. 72(1)(b).

82 See *FIPPA*, s. 61(1)(c.1); and *MFIPPA*, s. 48(1)(c.1). A similar offence is included in *PHIPA*, s. 71(1)(d).

83 This offence should be included if not already captured by the whistleblowing offence referenced in the white paper. For similar offences, see *PHIPA*, ss. 70 and 72(1)(j); Bill c-11, ss. 124 (1) and 125 and the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, ss. 27.1 (1) and 28.

84 See *FIPPA*, s. 61; *MFIPPA*, s. 48; and *PHIPA*, s. 72; and *CYFSA*.

85 Similar to s. 65 of *PHIPA*.

86 Our proposed definition is similar to, and compatible with, that found in Ontario's *Personal Health Information Protection Act.*

87 See, for example, *EU General Data Protection Regulation* Recital 26: "The principles of data protection should … not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

88 See, for example, Rocher et al. **"Estimating the success of re-identifications in incomplete datasets using generative models"** Nature Communications 10, Article no. 3069 (July 23, 2019) retrieved August 16, 2021.

89 See, for example, Case Study #6 in the Canadian Anonymization Network's March 2021 report, **"Practices for Generating Non-Identifiable Data"** retrieved July 27, 2021.

90 See, for example, El Emam, Mosquera, and Bass: **"Evaluating Identity Disclosure Risk in Fully Synthetic Health Data"**, Journal of Medical Internet Research, 22(11), 2020.

91 Wu et al. Data & Policy, **"How data governance technologies can democratize data sharing for community well-being"** (July 2021), retrieved July 27, 2021.

92 Ibid.

93 Government of Ontario, **"Building a Digital Ontario"** (April 30, 2021); Government of Ontario **"Ontario Appoints Special Advisor on Data Authority"** (August 6, 2021), retrieved August 16, 2021.

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333

www.ipc.on.ca
info@ipc.on.ca

September 2021