ONTARIO NONPROFIT NETWORK

September 8, 2021

The Hon. Ross Romano
Minister of Government and Consumer Services
Government of Ontario
By email: Ross.Romano@ontario.ca

Response to *Modernizing Privacy in Ontario*
***Empowering Ontarians and Enabling the Digital Economy* (White Paper)**

Dear Minister Romano,

We are writing to provide feedback on the Modernizing Privacy in Ontario White Paper to assist the Government in developing modern legislation that can be realistically implemented by nonprofits to protect the privacy of Ontarians.

ONN is the independent nonprofit network for the 58,000 nonprofits in Ontario, focused on policy, advocacy and services to strengthen Ontario's nonprofit sector as a key pillar of our society and economy. We work to create a public policy environment that allows our network of diverse nonprofit organizations across Ontario to work together on issues affecting our communities and channel the voices of our network to governments, funders, and other stakeholders.

ONN partners with Powered By Data to convene the Data Policy Coalition, made up of more than 30 nonprofit organizations, representing service providers, advocacy groups, and funders within the nonprofit sector. We are working together to enhance the nonprofit sector's access and responsible, ethical use of government-held administrative data to improve service delivery, program evaluation, and evidence-based planning for Ontarians.

We strongly support the Government of Ontario's vision to make Ontario the world's most advanced digital jurisdiction, and commend you on this important legislative initiative which will no doubt be a cornerstone of that vision. Furthermore, we agree with the Government's premise that to achieve this vision, the scope of privacy legislation should be comprehensive and provide Ontarians with not only the rights, but also the skills and opportunities to fully participate in a digital world. Please find below our key recommendations followed by a section-by-section discussion of the White Paper.

Key Recommendations

The following summarize, in our view, the highest priority recommendations made below:

- We recommend that if legislation requires data to be portable across organizations, that government funders correspondingly streamline their required databases and data storage formats. Similarly, adequate time must be given to implement data portability.
- We recommend that requirements be implemented for the design of automated decision-making to ensure that they are "non-discriminatory by design."
- We recommend that the excluded category of "collection of employee information" include placement students and volunteers as well.
- We recommend that the Government create standard plain-language privacy policy, procedure, and practice templates, as well as consider creating a plain-language privacy policy builder similar to Community Legal Education Ontario's Ontario's Not-for-Profit Act bylaw builder.
- We strongly support the proposal to equip the Information and Privacy Commissioner of Ontario with more resources, powers, and strong penalties, as well as the mandate to create codes of practice and take an education first approach to regulation.
- We recommend that the requirement for parental consent be waived in cases where doing so may deter a youth from accessing crisis, abuse, or other similar services.
- We support the creation of a clear framework and best practices for the use of de-identified and anonymous data and recommend safeguards to ensure data collected for nonprofit purposes cannot be inappropriately transferred to for-profit entities for their private benefit.

Rights-Based Approach to Privacy

ONN agrees that "with rapid advances in technology that vastly expand the ability of organizations to collect, use, and share personal information, new rules and rights are needed to protect Ontarians from potentially unfair practices and maintain a high level of trust and confidence in the digital economy." However, it must also be acknowledged that many small to medium size organizations have limited understanding and capacity to manage the information that is collected by software designed by, and stored on databases belonging to, multinational corporations. A made in Ontario privacy solution should recognize that in practice small organizations, whether for-profit or nonprofit, have little control over these platforms relative to the tech giants who own them.

1) Does the proposed preamble in this section include the right principles, reasons and values to guide the interpretation of a potential privacy bill?

The principles, reasons, and values set out in the proposed preamble to guide the interpretation of the privacy legislation are appropriate. However, it is also important to acknowledge that personal

information is often collected in the course of public service delivery and used both for the benefit of the individual as well as for the sake of important public policy objectives such as evidence-based decision making. We suggest language including the following:

> Preamble
> Privacy is a foundational value in society. Every individual is entitled to a fundamental right to privacy and the protection of their personal information.
>
> Changes in technology have allowed organizations to easily collect **and analyze** vast amounts of personal information about individuals. **While these practices can be used in service of important public policy objectives such as the efficient and evidence-based provision of public services, they can also undermine** the control that an individual has over their personal information.
>
> To establish the trust and confidence of individuals, organizations must be subject to rules, guided by principles of proportionality, fairness and appropriateness with respect to the collection, use or disclosure of personal information.

2) How should the concepts of personal information, and “sensitive” personal information, be defined in law?

ONN encourages harmonizing the definition of personal information to the greatest extent possible with Federal and and other Provincial privacy laws to create consistency and ease administrative burden of nonprofits operating in Ontario. Additionally, in order to protect nonprofit employees who require a free hand in commenting on individuals in their file in order for the team to serve them effectively and safely, we encourage following BC’s example in carving out work product information from the definition of personal information. Personal information should be defined in such a way as to provide the widest reasonable protection to members of the public, volunteers, and employees while still being administratively feasible for nonprofits.

3) Do the “fair and appropriate purposes” proposed in this paper provide adequate and clear accountability standards for organizations and service providers?

ONN supports limiting the collection and use of information to fair and appropriate purposes. What constitutes an appropriate purpose will be a fundamental question that will define the character of Ontario for many years to come. The proposed legislative text defines it according to what a reasonable person would find appropriate under the circumstances. However, it must be

acknowledged that the expectations of a reasonable person has been shaped by a market in which, until recently, there was not even discussion of implementing robust protections for their privacy. We are therefore concerned that the norm courts are likely to pick up on is one in which people are accustomed to the use of personal information for private gain.

Many individuals are opposed to such uses but because our social and work worlds, particularly during the COVID-19 crisis, have become so dependent on platforms whose business model is to trade in personal information, that individuals have little choice but to accept this as "an appropriate use". Consequently, even where informed consent is asked for and given, this is only against a backdrop in which people feel little actual choice. Forthcoming legislation is unlikely to be able to address the full scope of what a reasonable person ought to expect about the use of their data. We suggest convening a broad expert panel or dedicated research to inform decision-making on this question.

Additionally, we recommended explicitly recognizing the varying capacities of nonprofits when considering the factors to determine what purposes are fair and appropriate by making the following change:

> "(2)3. Whether there are less intrusive means of achieving those purposes **reasonably available to the organization** at a comparable cost and with comparable benefits." (p.5)

We recommended this change because a solution may be available on the market at a comparable cost without a low-capacity, low-tech-literacy nonprofit necessarily being able to know about it or access it. Similarly, it is unclear whether "the comparable cost" factors in the learning curve which might be higher for an organization with lower literacy. If the Government takes the view that this flexibility is already captured in the concepts of "comparable cost and with comparable benefits", then we recommend this be explicitly stated in any explanatory notes accompanying legislation.

4) How far should the data rights of erasure and mobility extend? Should they include all information an organization has about an individual, or only the information the individual provided?

ONN supports the individual right to erasure, mobility, and to be informed when personal information has been transferred. However, the Government of Ontario must align its role as regulator and funder, ensuring, for example:

- that data mandated to be kept for a given period by transfer payment agreement (TPA) holders cannot be required to be erased before then,
- that mobility requirements be consistent with the portability functionality of Government-mandated databases, and

- that the requirement to inform individuals of transferred data not endanger staff.

The nonprofit sector has lived through numerous examples of legislation being passed without adequate consideration for the Ontario government's role as funder of nonprofit services (accessibility requirements, pay equity, and Bill 148 Employment Standards changes, for example). ONN would be pleased to convene nonprofits and provincial ministries to work through how TPA requirements and forthcoming privacy legislation will interact. We also urge the Ontario government to work with funders at other levels of government and private funders to align their database/case management systems with new privacy legislation. Again, ONN would be pleased to convene.

a. Right to be Forgotten

ONN supports the creation of a right to be forgotten; however, to make it administratively feasible, the exceptions should be expanded to include data that is required to be kept by TPA holders. We would also like to ensure that Ontario government rules do not override municipal or federal funders' requirements to retain or dispose of data.

The White Paper proposes that an individual have the right to order the deletion of their information except in a limited number of circumstances including

A. where it would delete someone else's personal info,
B. an Act, regulation, or contract requires its preservation,
C. The information was disclosed in the course of legal proceedings,
D. other prescribed circumstances. (p.8)

Transfer payment agreements by the Government of Ontario to nonprofits often require the collection of information for accountability and evaluation purposes. However, we have been advised that transfer payment agreements are not contracts (and therefore exempt from procurement law). We recommend that (b) be changed to avoid any confusion to the following "an Act, regulation, transfer payment or contribution agreement, or contract requires its preservation".

b. Data Portability

Regarding data portability, we reiterate our recommendation made on October 16, 2020 in response to *Ontario Private Sector Privacy Reform - Improving private sector privacy for Ontarians in a digital age* (Discussion Paper). The Government must ensure that data portability/ interoperability requirements and other rules take into account the multiple data systems that Ontario Ministries may require nonprofits to use when they deliver services on behalf of government -- or else make life easier for provincially-funded nonprofits by giving them greater freedom to select and manage their own data systems. We note that some nonprofits currently determine their own client management databases and, despite any efficiency downsides, appreciate the privacy reassurance it gives their clients, knowing that their data is held locally.

Additionally, the specific wording in the legislative text proposed in the White Paper for "Disclosure Under Data Mobility Framework" makes it unclear the extent of data mobility the Government is proposing which could significantly impact the amount of coordination necessary to make such a provision administratively feasible. While the stated rationale for such data portability is to ensure that Ontarians can "take their business elsewhere," The White Paper proposes the following wording:

> (1) Subject to the regulations, on the written request of an individual, an organization shall as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to **a** data mobility framework provided under the regulations. (emphasis added) (p.9)

The wording appears to require the dataholder to turn it over to any organization subject to a data mobility framework, and not necessarily an organization under the same framework. Consequently, this enables the individual requestor to do much more than simply transfer their business elsewhere. This could quickly create significant demands on nonprofits who serve individuals who use many services making it all the more necessary for different government funders to establish a common data infrastructure.

c. Right to Access Personal Information

ONN supports the right of individuals to access personal information held by nonprofits about them. However, in order to preserve the freedom of staff to comment on clients and warn each other about potentially problematic or dangerous behaviour, we recommend that case notes and evaluations of different kinds (e.g. psychological, behavioural, psychosocial, etc.) relating to an individual be expressly carved out from the definition of personal information as it pertains to individuals' right of access.

Similarly, ONN supports individuals' right to know what information has been disclosed about them to third parties, including in cases where a social service provider provides information to police or a children's aid society pursuant to a professional obligation to do so. Some services (such as those provided by women's shelters) are provided on an anonymous basis and there is value in keeping it that way, even where it thwarts information-sharing between authorities.

Safe Use of Automated Decision-Making

ONN agrees with the White Paper that

> "It is clear that AI technologies, such as automated decision systems, offer significant benefits for organizations and the economy. However, new risks such as surveillance and algorithmic bias have emerged that necessitate greater accountability."

Nonprofits serve many individuals and communities who are particularly at-risk of facing surveillance and discrimination, as such we make the following submissions with their interests in mind. We note broadly, however, that nonprofit corporations are themselves sometimes

discriminated against by funders, lenders, procurers of goods and services, and other financial decision-makers who may not fully understand or appreciate nonprofit business models. This is particularly true in the case of BIPOC-led nonprofit organizations, who may face discrimination due to their corporate form and the identity of their leadership.[1] As decisions in the finance industry, as well as public and private sector funding (and possibly procurement) become increasingly automated, there is a risk that nonprofits will need the protections set out in the White Paper and in our comments below. We therefore recommend that the Government consider **extending the protected category from individuals to persons (which includes corporations).**

1) Do the example provisions provided in this section offer adequate protection for Ontarians whose information is subject to ADS [automated decision systems] practices?

ONN strongly supports individuals' right to be informed about, know the basis of, and object to automated decisions. However, any system that depends on individuals to know their rights and be able and willing to enforce them will necessarily disfavour those most at risk of facing abuse. Individuals with low technological and general literacy and few resources or time to pursue their case, or the ability to advocate for themselves effectively in an appeal, will not be able to make effective use of such rights.

ONN therefore recommends that any legislation take a heavily preventative approach to AI and empower the Information and Privacy Commissioner with resources, effective investigation powers, and penalties where necessary. Consequently, we support prohibiting the use of automated decision-making in cases involving sensitive information and the possibility of significant harm to individuals (articulated on p.13). Furthermore, we applaud the choice to depart from the language of the GDPR that the decision need be solely based on automated decision-making in order for these rights to be triggered.

However, the exception to this prohibition for any decision necessary to enter into or perform a contract, while standard in other jurisdictions, risks being far too sweeping to make this protection provided by the prohibition meaningful unless "necessary" is clearly defined. If necessary is defined by the requirements set by organizations providing products or services, then an organization could require its clients to submit to ADS in important decisions simply by providing no alternative method of decision-making. We therefore recommend that "necessary" be defined in a way that limits the situations in which automated decision-making systems can be used to those in which the contracts could not be performed in the manner promised unless automated decision-making systems are used.

---

[1] Rachel Pereira, Liban Abokor, Fahad Ahmad, and Firrisaa Jamal Abdikkarim. (2020) Unfunded: Black Communities Overlooked by Canadian Philanthropy. Foundation for Black Communities. Available at: https://carleton.ca/panl/2020/unfunded/

Where a decision has significant effects on an individual but falls under one of the enumerated exceptions, we recommend that regulations be set out for their design and testing to ensure they meet higher standards based on how serious the potential harm is. For example, while it may be prohibited for any ADS system that has potentially serious effects on a person (e.g. hiring decision ADS) to be based on data from sources that are likely to be biased, a more serious ADS (e.g. healthcare decision) must be specifically tested for its tendency to exhibit bias in decision making towards groups protected under *Ontario's Human Rights Code, 1990*.

2) Does the proposed regulatory approach for ADS strike the right balance to enhance privacy protections, while enabling new forms of socially beneficial innovation in AI?

In our view, the proposed regulatory approach does not strike the right balance to enhance privacy protections, while enabling new forms of socially beneficial innovation in AI. As we discussed above, the current approach mainly puts the responsibility for policing decisions in the hands of individuals who may be the least qualified to ensure their rights are being protected. Furthermore, it is unclear from the information provided in the White Paper to whom appeals will be made and what consequences will follow in the event of persistent or repeated non-compliance or discriminatory practice.

ONN supports the proposal discussed later in the White Paper that the Information and Privacy Commissioner be given the power to investigate automated decision-making systems and issue penalties not only on the basis of individual cases but based on the total volume of decisions made by the system. If the rights of one individual have been violated by an automated decision-making system, then anyone who shares their characteristics, whether they contest the decision or not, has likely faced a similar impairment. Requiring that a class action be brought to address the widespread nature of these issues will be costly and inefficient compared to enabling the Information and Privacy Commissioner to issue sufficiently robust penalties.

Additionally, legislation should explicitly address the causes of discriminatory and flawed decision-making systems rather than simply their output. Bias enters automated decision-making when personal information that ought to be extraneous to a decision are considered and influences the decision on the basis of harmful stereotypes existing in the training data on which the AI is based. The algorithms underpinning AI tend to encompass the biases and values of its builders and those who developed the data sets they use. When those builders are from a homogenous group and incentivised by profit rather than fairness, the technology can profoundly perpetuate and deepen inequities. ONN therefore recommends that the legislation builds on the concept of fair and legitimate use of personal information to require that automated decision systems be designed to exclude the use of irrelevant personal information.

The above safeguards will not impair the development of socially beneficial innovation in AI, but it will impair the development of socially harmful innovation in AI by mandating that fairness be built in from the beginning and not sacrificed as a matter of convenience or efficiency.

Beyond the inherent fairness of AI-supported decision-making, there is also the question of perceived legitimacy and the effective communication of decision-making processes. It is imperative that the decisions made by AI be easily explainable; that is, which factors, features and data sets are used in decision-making and which ones are not and why, particularly when personal information is involved.

We recognize that this is a fast-developing area of technology and we appreciate the hesitancy to be overly prescriptive at this early stage. We therefore recommend that if the Government does not wish to put the above mentioned safeguards directly in the legislation, that the legislation empower the Information and Privacy Commissioner to develop binding guidelines in the development of automated decision-making systems in how they process personal information.

3) Should there be additional recordkeeping or traceability requirements to ensure that organizations remain accountable for their ADS practices?

Without records of the design and design process, individual decision, and updates, it may be impossible for an individual to demonstrate the flawed basis of a decision or its source. Consequently, it is vital that all these records be kept and made available to individuals and investigators as necessary (as is suggested later in the White Paper when discussing the IPC's investigatory powers).

The ONN recommends that detailed records be kept of:

- individual decisions,
- the design and design process of the automated decision-making system, in particular demonstrating what steps were taken to ensure extraneous personal information was not being used or weighed inappropriately, and
- any steps that have been taken in response to the individual's objections as well as previously similarly situated individuals' objections to check for bias and correct any issues found.

Furthermore, individuals should have a right to access these records in an accessible format and in a manner that respects the intellectual property of the organization and the privacy of other individuals.

4) Are there additional requirements or protections that Ontario may consider related to the use of profiling?

Automated decision-making systems which process personal information may be trained with data which is known to contain flawed or discriminatory information such as from adult content websites or social media. Such automated decision-making systems are known to reflect the biases of the data on which they are trained such that this should be legally presumed. We therefore recommend that where an individual can prove that an automated decision-making system was trained on data biased in a way that is relevant to the decision affecting the individual, it be deemed that it is so biased without the individual being required to prove the specific way in which this bias may have affected their individual case.

Enhanced Consent and Lawful Uses of Personal Data

ONN fully supports the Government's goal of improving the meaningfulness of consent by making it informed while providing alternative authorities so consent isn't always needed, thereby avoiding consent fatigue (p.16). Before addressing the alternative authorities to consent, we have some preliminary observations about some of the proposals mentioned in the White Paper. Following these preliminary remarks, we will directly address the discussion questions provided in the White Paper.

Plain language and clear design in privacy policies and agreements seeking consent are of vital importance, particularly where sensitive personal information is involved.

In principle, we support prohibiting organizations from making consent a condition for a service, or obtaining it by deceptive or duplicitous means. Requiring such disclosures can have a discriminatory effect on undocumented migrants, homeless individuals, and others who fear disclosing or do not have access to the required proof of personal information. However, we note that such requirements can sometimes not be up to individual nonprofit organizations and are instead determined by funding agreements, including government funding agreements. If the Government of Ontario decided to include such a prohibition in legislation, we would expect it to take a whole-of-government approach and change its funding practices to align with its role as regulator.

Related to the above, if organizations were restricted to collecting only information necessary to receive a service or product, we would expect the definition of "necessary" to include requirements under any agreement with government to fund the provision of the service or product.

1) Does the sample list of "permitted categories" provide a sufficient set of authorities for the collection, use and disclosure of personal information? Are there any categories missing? Are there any categories that are too permissive?

ONN supports the view that informed consent should be required by default, but that this is impractical and counter-productive in certain categories of situations. ONN agrees that these exceptional categories include where it is in the individual's interest and emergency situations (p. 21). Below we will consider some of the permitted categories for collection, use, and disclosure of information in terms of those we believe are overly restrictive, overly permissive, or missing.

A. Overly Restrictive Categories: Does the sample list of "permitted categories" provide a sufficient set of authorities for the collection, use and disclosure of personal information?

Personal Identification

The ONN recommends that the category permitting the sharing of personal information to identify an injured, ill, or deceased individual be expanded to include designated broader public sector organization as defined by the *Broader Public Sector Accountability Act, 2010*. This would reflect the fact that broader public sector organizations often deal with vulnerable individuals who are injured or ill and sometimes require to know their whereabouts and status.

> An organization may disclose an individual's personal information if the disclosure is necessary to identify the individual who is injured, ill or deceased and is made to a government institution, a part of a government institution, **a designated broader public sector organization as defined in the *Broader Public Sector Accountability Act, 2010*,** or the individual's next of kin or authorized representative. If the individual is alive, the organization must inform them in writing without delay of the disclosure. (22)

Research in the Public Interest

ONN strongly supports the inclusion of a category for research in the public interest. While the list of requirements broadly seems reasonable, we question whether it will create an unnecessary administrative burden to be required to inform the Commissioner every time personal information is shared.

Publicly available information

Having consulted with the fundraising community, ONN supports the following proposal: "An organization may collect and use an individual's personal information if the personal information is publicly available and the collection is consistent with the purposes and context in which the

personal information was made publicly available and the reasonable expectations of the individual," (p. 23).

B. Missing Categories: Are there any categories missing?

There are numerous instances in which nonprofits collect information when it could be a burden to be required to seek informed consent. These include drop-in programs, shelters, withdrawal management centers, food banks, grassroots/youth-led organizations and other community-based projects, and projects/programs that are trusteed by larger established providers (or shared platforms). Information collection and consent forms could be inappropriate in these contexts or cause participants to stay away for fear of being contacted by authorities. That said, workers and volunteers in these contexts should be supported through training and best practices to appropriately handle any personal information that does come into their possession.

C. Overly Permissive Categories: Are there any categories that are too permissive?

Collection of Employees' and Volunteers' Personal Information

There appear to be some inconsistencies in the wording of the category entitled "collection of employee's personal information". The proposed text is as follows (pgs.20-21):

> An organization may collect, use or disclose personal information about an employee if the information is collected, used or disclosed solely for the purposes of,
>
> (a) establishing, managing or terminating an employment or volunteer-work relationship between the organization and the individual; or
>
> (b) managing a post-employment or post-volunteer-work relationship between the organization and the individual.

While (a) and (b) discuss both employment and volunteer work, the main provision mentions only employees. On the plain meaning of this text, it appears that the information of employees is exempted both connected to any work or volunteering they do with the organization, but the personal information of volunteers who are not also employees requires seeking consent. About half of all nonprofits in Ontario are exclusively volunteer run and many more depend on large groups of volunteers. Consequently, this provision will have significant effects on the nonprofit sector. If volunteers are not addressed clearly and separately from employees, then it is likely to create confusion and impose an inappropriate structure.

We therefore recommend that a separate permitted category be created for volunteers that also acknowledges volunteers are often also clients of an organization as well. The use of the word "solely" below is likely sufficient to avoid concerns arising from dual roles.

> An organization may collect, use or disclose personal information about a volunteer if that information is collected, used or disclosed solely for the purposes of,
>
> (a) establishing, managing or terminating a volunteering relationship between the organization and the individual; or
>
> (b) managing a post-volunteering relationship between the organization and the individual.

Furthermore, the way the employee information provision is drafted appears to allow wider collection, use, or disclosure of personal information than is intended. On the plain meaning, one could argue that one can collect, use, or disclose information if it was collected, used, or disclosed for the enumerated purposes. For example, an organization could disclose information for whatever reason provided it was originally collected for the purposes of managing an employment relationship. We propose the following clarifying wording: "An organization may collect, use or disclose personal information about an employee **if that collection, use or disclosure is** solely for the purposes of, …".

Investigation or Legal Proceeding

ONN understands that it may be necessary to require the sharing of personal information for the purposes of investigations and legal proceedings. However, the current wording appears far too broad. Firstly, it does not specify whose legal proceedings or investigation. Secondly, on the current wording it could be argued that as long as the information is reasonably necessary for the investigation or proceeding, then no consent is necessary, without regard to whether it is reasonable under the circumstances for an individual who may be unconnected to the proceedings and who may be prejudiced by the sharing of their information to have the opportunity to decline.

We invite the Government to consider how broad the proposed language is compared to the narrow exceptions enumerated in, for example, PIPEDA. For instance s.7(3)(c), which goes beyond simply requiring an ongoing investigation or proceeding but an actual subpoena.

> (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

In our view, this is a far more appropriate and exacting standard than mere reasonableness and it makes clear the type of proceedings and investigations in which organizations may disclose without consent.

2) Consider the sample “business activities” provision provided. Is it properly balanced to protect personal information while allowing businesses to conduct their operations? How should Ontario define the concept of “commercial risk”? Should “any other prescribed activity” be removed from the list of business activities?

In order to accomplish the Government’s goals of developing a truly comprehensive privacy framework, it will be necessary to adapt legislative language to account for the fact that these rules must now apply to nonprofit organizations as well as businesses. Below we recommend how to adjust the language to include non-commercial activities.

A. Is it properly balanced to protect personal information while allowing businesses to conduct their operations?

We find the language of business activities too narrow and propose the language of “organizational activities” or “operational activities” to account for nonprofit organizations. Similarly, exempting the requirement for consent in the use of de-identified data in “business transactions” (p.18-19) is needlessly restrictive and should be extended to all transactions whether commercial or otherwise.

Indeed, where a transaction is not a business transaction in the sense that there is no monetary component (e.g. a research agreement or service partnership between different providers), there is an additional impetus to be enabling. Some such transactions may fall under specifically enumerated categories but others may not. Rather than enumerating a category for every type of transaction, it may be helpful to simply exempt a much wider range of transactions to begin with.

B. How should Ontario define the concept of “commercial risk”?

Following what we have said above, we strongly recommend either referring to commercial and operational risk or defining commercial risk in a way that makes clear it applies to more than income-earning activities.

C. Should “any other prescribed activity” be removed from the list of business activities?

ONN supports keeping a reference to “any other prescribed activity”. As the province gains more experience applying such legislation it will be helpful to have the flexibility in regulation to prescribe other types of activities.

3) Are there any additional protections or requirements that Ontario should consider in respect of service providers?

We have no proposed additional requirements at this time as this is not our area of expertise.

Data Transparency for Ontarians

1) Is the "privacy management program" requirement sufficient to ensure that organizations are accountable for the personal information they collect?

The privacy management management program may be insufficient on its own to ensure that organizations are accountable for the personal information they collect in two crucial respects. Firstly, while we whole-heartedly agree with the requirement for plain language information, we note not all organizations have the capacity or expertise to develop such materials. Secondly, it is unclear what consequences will follow if an organization fails to have a plan in place and what enforcement powers and resources will be given to ensure effective enforcement.

a. Make Plain Language and Clear Design Mandatory

We recommend developing templates and assess the feasibility of creating a free plain language privacy policy builder similar to Community Legal Education Ontario's bylaw builder whose development was funded by the Ministry of Government and Consumer Services. The Government could also consider creating such resources in languages other than English and French to ensure that the consent of individuals who speak neither official languages is also meaningful. This would certainly contribute to Ontario becoming the leading digital jurisdiction in the world.

b. Make Privacy Management Programs Enforceable

It is unclear from the White Paper how the Government envisions these plans being enforced, by whom, and with what penalties. Additionally, it is unclear if individuals have any rights of complaint. While we wholly support the provision that a failure to create plain language documents results in consent being invalid, we wonder if this is sufficient incentive, given that most people will likely not know their rights in this regard.

We recommend looking to disability rights legislation, such as the *Accessible Canada Act, 2019* for a model framework around such plans, including: the timeline in which they must be developed, the rights of individuals to complain, the ability to inspect, as well as the tiered nature

of the obligations based on the size of organizations. Below we reproduce the tiered structure we recommended in our submission concerning the 2020 Discussion Paper.

a. **for-profit corporations whose business models rely primarily on the generation of profit from personal data** (such as social media, data analytics/mining companies, rewards/loyalty programs, and credit bureaus);

b. **other large corporations and nonprofits** with 500+ employees;[2]

c. **small and medium enterprises including nonprofits with paid staff**, and

d. the approximately 25,000 Ontario **nonprofits that are entirely volunteer-run** and have no paid staff. While these nonprofits may have access to private data (e.g., the names and addresses of children and other vulnerable persons), the cost of compliance must be proportionate to their small budgets and volunteer capacity.

To make privacy management plans a meaningful requirement, it is likely that the Information and Privacy Commissioner will require more resources.

2) Are the sample provisions in this section sufficient to ensure that Ontarians understand the nature, purpose and consequences when an organization collects or uses their personal information?

The sample provisions in this section appear sufficient to ensure that Ontarians understand the nature, purpose, and consequences when an organization collects or uses their personal information.

3) Should Ontario consider a mandatory requirement for “Privacy by Design” practices or “privacy impact assessments”? What kind of burden would this kind of requirement cause for organizations? How should Ontario balance the value of these requirements with this potential burden?

ONN supports mandating privacy by design since a legal requirement is likely to mainstream these design practices thus bringing down their costs. However, it is true that there is an added

[2] The Government of Canada defines small and medium enterprises as those with 1 to 99 and 100 to 499 employees, respectively. https://www.ic.gc.ca/eic/site/061.nsf/eng/Home

cost to fully understanding the privacy impact and designing systems with them in mind. For a sector, such as the nonprofit sector, in which digital adoption has been hampered by a funding culture that discourages investment in the administration of organizations, such costs are likely to be even higher.

ONN recommends that if Privacy by Design and privacy impact assessments are mandated that they be phased in over a number of years and accompanied by funding to develop nonprofit solutions to assist the nonprofit sector to transition.

Protecting Children and Youth

1) What additional considerations are needed in determining appropriate age of consent for the collection, use and disclosure of personal information?

We have no additional considerations to suggest here as it is not our area of expertise.

2) What operational challenges might organizations face by including age of consent requirements for the collection, use and disclosure of personal information?

For youth-serving nonprofits, particularly those serving youth in crisis, 2SLGBTQ+ youth, or youth experiencing abuse, a requirement to obtain parental/guardian consent to access services could deter the youth from accessing the services altogether. ONN recommends waiving parental consent in these instances, with the details of any carve-outs for certain types of organizations or certain situations be laid out in regulation, following a dedicated consultation with youth-serving organizations on this topic.

3) Should Ontario consider other requirements to enhance protections for other vulnerable populations, such as seniors and people with disabilities?

We have no additional considerations to suggest here as it is not our area of expertise.

A Fair, Proportionate and Supportive Regulatory Regime

ONN strongly supports this entire section of the White Paper and agrees wholly that such resources, powers, and potential penalties are necessary to ensure the other provisions set out in the White Paper are meaningful.

1) Would certification programs and codes of practices be effective in proactively and collaboratively encouraging best practices in privacy protection?

ONN supports this proactive education-first approach. We would stress that in order for these codes of practice to be appropriate to the context of nonprofits, many of whom have not been subject to Ontario privacy laws previously, the IPC would need to specifically develop expertise in this area. We welcome the opportunity to collaborate with the IPC in building this capacity.

2) Are administrative monetary penalties effective in encouraging compliance with privacy laws? Are the financial penalties set at an appropriate level?

ONN supports the application of administrative monetary penalties particularly where the purpose is to ensure that no organization profits from intentional non-compliance. Additionally, the financial penalties appear to be appropriate in even addressing very large organizations that do not comply. We note, however, that where non-compliance is owing to a lack of capacity or knowledge, monetary penalties are less likely to encourage compliance. To assist organizations who do not have the capacity to develop the required expertise in privacy, it will be necessary to make investments in publicly accessible training and tools, such as templates or the privacy policy builder mentioned earlier. We also urge the Ontario government to carefully consider liability for volunteers associated with unincorporated grassroots groups to ensure that the penalties for unintentional privacy law breaches are not disproportionate.

3) Would the ability for the IPC to issue orders requiring organizations to offer assistance or compensate individuals be an effective tool to give individuals quicker resolutions to issues?

ONN supports the ability of the IPC to issue orders requiring organizations to offer assistance or compensation to individuals as a quicker alternative resolution to litigation. It is simply not

realistic to expect most individuals, particularly those most vulnerable to exploitation as a result of privacy breaches, e.g. low-literacy or elderly individuals, to have the resources, time, and ability to engage in litigation effectively.

Support for Ontario Innovators

1) Would the clearer articulation of which privacy rules apply to de-identified information, as discussed in this section, encourage organizations to use de-identified information, and therefore reduce privacy risk?

ONN supports administrative data sharing for improved service delivery, innovation, research and development, and advocacy. Privacy legislation that makes clear what needs to be done to ensure sharing can happen while respecting the rights of individuals has an important role to play in facilitating this sharing. Consequently, ONN supports setting out standards for the use of de-identified data.

2) Would the inclusion of the concept of anonymized information, and clarifying that the privacy law would not apply to this information, encourage organizations to use anonymized information?

The nonprofit sector is increasingly using anonymized information in service delivery, program evaluation, and policy and system change work. Through the Data Policy Coalition, nonprofits are advocating for the expanded availability of anonymized data to support their work. For instance, in the Coalition's 2019 progress report, we noted that "Data on offending are already tracked by police for operational purposes. If shared securely and anonymously with nonprofits, it could help organizations measure their impact on reducing recidivism and to inform policy." If privacy considerations were clearly elaborated in law, it would indeed assist the nonprofit sector in leveraging the value of anonymized data.

3) For sharing information for socially beneficial purposes, what additional safeguards or governance would be needed in addition to de-identification of information, in order to protect privacy?

In order to ensure that de-identified information collected by nonprofit organizations is not inappropriately commodified, legislation could include restrictions around the transfer of data from nonprofit to for-profit organizations under agreements other than service provider agreements.

Thank you for giving serious consideration to our recommendations. For more information, please contact Liz Sutherland, Director of Policy, at liz@theonn.ca.

Sincerely,

Cathy Taylor, Executive Director

Copy to: Marlene McRae, Manager of Access and Privacy Strategy and Policy Unit, MGCS, via Marlene.McRae@ontario.ca
Ontario Digital Service, Ministry of Finance, via digital.government@ontario.ca
MGCS Privacy consultation portal, via access.privacy@ontario.ca
Michael Lenzcner, Founding Director, Powered by Data, via michael@poweredybdata.org