



ONTARIO NONPROFIT NETWORK



**POWERED  
BY  
DATA**

John Roberts, Chief Privacy Officer & Archivist of Ontario  
Ministry of Government and Consumer Services (MGCS)  
Ontario Government  
Via email: [john.roberts@ontario.ca](mailto:john.roberts@ontario.ca) and [access.privacy@ontario.ca](mailto:access.privacy@ontario.ca)

October 16, 2020

**Response to Ontario Private Sector Privacy Reform -  
Improving private sector privacy for Ontarians in a digital age (Discussion Paper)**

Dear John Roberts and MGCS colleagues,

Thank you for the opportunity to share our perspectives on your ministry's discussion paper, *Improving private sector privacy for Ontarians in a digital age*. We have appreciated working with you over the past year as the Ontario Government modernizes its overall approach to data and privacy in Ontario's public, private, and nonprofit sectors.

The Ontario Nonprofit Network (ONN) is the independent 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.

The Data Policy Coalition, convened by Powered By Data, is 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 social service delivery, impact evaluation, and evidence-based planning for public benefit

## **Summary of preliminary recommendations**

1. **Engage the nonprofit sector and community representatives at multiple points and ensure sufficient time for dialogue in the legislative development process.**
  - a. Engage key segments of the sector on elements that affect them as **stewards of personal data**, e.g., fundraisers, campaigners/advocacy groups, service providers

with multiple government agreements (federal, provincial, and/or municipal), and organizations that work with vulnerable people (e.g., children, survivors of intimate partner violence, and people with developmental disabilities).

- b. Engage nonprofits and grassroots groups as **advocates for the rights and data ownership of Indigenous peoples, racialized communities, and other equity-seeking groups**, who have justified concerns about how data is currently used across the public, private, and nonprofit sectors.
  - c. Engage nonprofit intermediaries at key stages of legislative development, such as the development of **principles**, the **operationalization** of concepts such as “the right to be forgotten,” the exploration of **mechanisms** such as data trusts, and the **harmonization** with provincial funding requirements and parallel privacy frameworks affecting nonprofits.
2. **Avoid a one-size-fits-all approach (part 1):** Create distinct and tiered legislative/regulatory frameworks for:
    - 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;<sup>1</sup>
    - 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.
  3. **Avoid a one-size-fits-all approach (part 2):** Within the nonprofit sector, consider distinct regulations for **public-benefit nonprofits**,<sup>2</sup> such as charities and community sports leagues, and **member-benefit nonprofits**, such as private clubs and industry associations.
  4. **Harmonize with the rest of Canada and the “gold standard” - Europe’s General Data Protection Regulation (GDPR).**

---

<sup>1</sup> 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>

<sup>2</sup> Public benefit nonprofits include charities, nonprofit cooperatives (including most housing cooperatives), and other nonprofits with a public-oriented mission that do not qualify for, or do not choose to become, charities (e.g., community sport and recreation groups). For more information on public benefit nonprofits, please see ONN’s 2017 paper, “Introducing the Public Benefit Nonprofit Sector,” available at <https://theonnc.ca/our-work/our-regulatory-environment/public-benefit-nonprofits/>

5. **Harmonize new privacy legislation with (or replace) existing provincial health care privacy legislation.**
6. **Align the Ontario Government's role as regulator with its role as funder:** Ensure that data portability/interoperability requirements and other rules take into account the multiple data systems that Ontario Ministries 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.
7. **Use an explicit equity lens and respect Indigenous data ownership.**
8. **Include employee data privacy:** If new privacy legislation is introduced, it should address the gap in employees' privacy rights, such as the confidentiality of health information that comes into the possession of an employer. The new framework should not, however, erect barriers for trade unions to carry out their Charter-protected core functions and responsibilities as mandated by statute or otherwise prescribed by law.
9. **Tackle directly the challenge of imposing fiduciary responsibilities, i.e., an ethic of care, on for-profit corporations engaged in human services.** In areas such as child care and long-term care, personal information should not be used for profit by those who are entrusted with their care. Consult broadly to develop rules concerning opportunities for financial gain in relation to the private data of vulnerable persons on the part of those who carry fiduciary responsibilities.
10. **Refrain from imposing new administrative burdens during a recession:** Consider the impact of the COVID-19 pandemic and related economic hardships for nonprofits and other small enterprises when determining an implementation timeline.
11. **Set fines relative to global revenues** to ensure that big data companies that violate Ontario law are fined more substantially than small business and nonprofits.
12. **Educate nonprofits and produce specific, plain-language guidance for organizations.**

## Introduction

Each year, the federal Privacy Commissioner reports to Parliament on the state of privacy protections in Canada. Daniel Therrien's report this year sounded the alarm on the impact of COVID-19 on our privacy rights: "With the pandemic accelerating the digitization of just about every aspect of our lives, the future we have long been urging the government to prepare for has arrived in a sudden, dramatic fashion. This rapid societal transformation is taking place without the proper legislative framework to guide decisions and protect fundamental rights."<sup>3</sup> Noting the pervasive use of for-profit platforms for everything from home working to schooling to health care appointments, Mr. Therrien called for an immediate update of privacy legislation in Canada.

The Ontario Government's discussion paper sends a clear message that there are plans to introduce privacy legislation that would apply to nonprofits and the private sector operating in our province. While privacy legislation is primarily a federal responsibility, the Government of Canada has appeared reluctant to update the existing Personal Information Protection and Electronic Documents Act (PIPEDA) to bring Canada in line with the "gold standard" -- Europe's General Data Protection Regulation (GDPR)<sup>4</sup> despite repeated calls from the privacy commissioner to do so.<sup>5</sup> The Ontario discussion paper gestures towards the GDPR, with references to "the right to be forgotten" and the importance of plain language communication about how personal data will be used. At the same time, the paper implies that data protections should not get in the way of doing business.

If provincial legislation is forthcoming,<sup>6</sup> nonprofits need to know what this could mean for fundraising and list-building, managing client data across (often funder-mandated) platforms, entrusting staff and volunteers with personal information, and engaging third parties to manage data. Some organizations that operate nationally may already have aligned practices with privacy legislation in Alberta, BC, or Quebec, for instance, but other organizations will likely need to update their practices. As we outline below, proposed privacy legislation will need to take into account the diversity of the nonprofit sector, from national and international organizations with multiple offices, all the way down to the smallest volunteer-run group that runs on a few hundred dollars and a Facebook page.

---

<sup>3</sup> Daniel Therrien, Privacy Commissioner of Canada. Quoted in Catharine Tunney, "COVID-19 pandemic reveals major gaps in privacy law, says watchdog." CBC News. October 8 2020.

<https://www.cbc.ca/news/politics/privacy-commissioner-annual-report-2020-1.5754930>

<sup>4</sup> For an overview of the GDPR, see the European Union, "EU Data Protection Rules." Undated.

[https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en)

<sup>5</sup> Office of the Privacy Commissioner of Canada. "Commissioner's annual report: Pandemic raises privacy concerns highlighting urgency of law reform." News release. Oct. 8, 2020.

[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c\\_201008/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201008/)

<sup>6</sup> Some industry associations are calling for the federal government to act and for the Ontario Government to wait. (See for example

[https://www.advisor.ca/news/industry-news/feds-provinces-must-coordinate-on-privacy-clhia/.](https://www.advisor.ca/news/industry-news/feds-provinces-must-coordinate-on-privacy-clhia/))

Nonprofits, however, would be unlikely to fall under updated federal legislation because of the Constitutional division of responsibilities, so Ontario legislation should still be expected for our sector.

Beyond the direct impact on nonprofits as data managers, there are also bigger picture questions on which the Ontario Government would do well to engage nonprofits in dialogue, as part of civil society. After all, “data is the new oil” in the sense that the flow of data now contributes more to the global economy than the flow of physical goods.<sup>7</sup> There is great wealth being generated in the “attention economy” on the monetization of personal information.<sup>8</sup> As bearers of an equity lens, nonprofits have a role to play as data justice advocates when data governance frameworks are being developed. These advocates must be part of discussions on how personal information may be used for commercial purposes and how artificial intelligence may be used in the context of both the for-profit data economy as well as public programs.<sup>9</sup> To fulfill their role as voices for communities, nonprofits must be at the table in promoting data justice and the protection of privacy in the use of data by all sectors.

## **Section A: Advice for further consultation with the nonprofit sector**

We would normally *end* a submission with a call to consult further with nonprofits before making legislative changes that affect them directly. This time we *begin* with recommendations on further engagement because there are so many facets of privacy legislation that intersect with the work of nonprofits and consultation must take place on each of them. It will be important for the Ontario Government to conduct ongoing consultations with nonprofits to ensure the legislation is appropriate for nonprofits as stewards of data as well as to provide nonprofits with adequate opportunities to speak as advocates for the rights of equity-seeking groups.

1. **Engage the nonprofit sector and community representatives at multiple points and ensure sufficient time for dialogue in the legislative development process.**
  - a. Engage key segments of the sector on elements that affect them as **stewards of personal data**, e.g., fundraisers, campaigners/advocacy groups, service providers with multiple government agreements (federal, provincial, and/or municipal), and organizations that work with vulnerable people (e.g., children, survivors of intimate partner violence, and people with developmental disabilities).

---

<sup>7</sup> James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra. “Digital globalization: The new era of global flows.” McKinsey Global Institute. February 24, 2016. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#>

<sup>8</sup> For a treatment of this idea, see John Lanchester. “You are the product.” London Review of Books. Vol. 39, No. 16. August 2017. [https://www.lrb.co.uk/the-paper/v39/n16/john-lanchester/you-are-the-product?CMP=longread\\_collection&subid=23002428&utm\\_campaign=The%20Long%20Read%20-%20Collections%202017&utm\\_medium=Email&utm\\_source=esp&utm\\_term=243865](https://www.lrb.co.uk/the-paper/v39/n16/john-lanchester/you-are-the-product?CMP=longread_collection&subid=23002428&utm_campaign=The%20Long%20Read%20-%20Collections%202017&utm_medium=Email&utm_source=esp&utm_term=243865)

<sup>9</sup> See for example CBC Sunday Magazine. “How Artificial Intelligence could change Canada’s immigration and refugee system.” August 2019. , <https://www.cbc.ca/radio/sunday/november-18-2018-the-sunday-edition-1.4907270/how-artificial-intelligence-could-change-canada-s-immigration-and-refugee-system-1.4908587>

- b. Engage nonprofits and grassroots groups as **advocates for the rights and data ownership of Indigenous peoples, racialized communities, and other equity-seeking groups**, who have justified concerns about how data is currently used across the public, private, and nonprofit sectors.
- c. Engage nonprofit intermediaries at key stages of legislative development, such as the development of **principles**, the **operationalization** of concepts such as “the right to be forgotten,” the exploration of **mechanisms** such as data trusts, and the **harmonization** with provincial funding requirements and parallel privacy frameworks affecting nonprofits.

There are particular considerations for the nonprofit and charitable fundraising community when it comes to data privacy, consent (implied and explicit), alignment with Canada’s Anti-Spam Legislation (CASL),<sup>10</sup> and repurposing data. Please see Appendix 1, a letter from the Association of Fundraising Professionals Canada, which forms part of our submission.

## **Section B: Toward a regulatory framework that is fit for purpose**

What is the primary purpose of a new privacy protection regime? Most would agree that it is to ensure individuals understand and consent to the uses of their personal information -- to have some say in the extent to which their data will be analyzed, stored, sold, aggregated (combined with others’ data), and used for purposes that range from setting life insurance rates to targeting election messages to granting parole to product marketing. Europe’s GDPR came into effect in 2018 to remedy a global regulatory vacuum, with companies extracting personal data for profit, generally without the knowledge or consent of the individuals affected. It is too soon to determine whether the GDPR strikes the right balance between personal privacy and the ability of companies to participate in the data economy but the fact that some business practices have had to be altered is a promising sign.

The Ontario Government’s discussion paper rightly recognizes the significant privacy gaps in our current regulatory environment. It will be important for legislation to take into account the vast diversity and the distinct goals and realities of different types of companies and nonprofits that will be subject to the law. We ask that the proposed legislation take into account these relevant differences rather than imposing a one-size-fits-all regime. Specifically, we recommend that size and purpose of organization/company be taken into account as outlined below. We also recommend that new legislation be harmonized with existing frameworks to which many nonprofits (particularly those that operate across Canada and/or in the health care field) are already subject. We recommend a principles-based approach and align with the GDPR as the “gold standard” of privacy protection.

---

<sup>10</sup> For more information on CASL and nonprofits and charities, please see <https://theonn.ca/our-work/our-regulatory-environment/canadas-anti-spam-legislation-nonprofit/>

2. **Avoid a one-size-fits-all approach (part 1):** Create distinct and tiered legislative/regulatory frameworks for:
  - 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;<sup>11</sup>
  - 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.
3. **Avoid a one-size-fits-all approach (part 2):** Within the nonprofit sector, consider distinct regulations for **public-benefit nonprofits**,<sup>12</sup> such as charities and community sports leagues, and **member-benefit nonprofits**, such as private clubs and industry associations. One factor justifying distinct approaches for these groups is that public benefit nonprofits could be included in provisions applying to government (and the broader public sector) regarding the use of linked, de-identified data for public interest purposes (e.g., program evaluation). A second relevant factor is that mechanisms for recourse are much more direct for member-based organizations whereas community members using public benefit nonprofits' programs and services have less direct avenues for recourse. Note that **nonprofits and charities** should be named as such rather than as "non-commercial organizations" as suggested by the discussion paper (many nonprofits own/operate social enterprises that carry on commercial activities).
4. **Harmonize with the rest of Canada and the "gold standard" - Europe's General Data Protection Regulation (GDPR):** Align the proposed regulatory framework with parallel legislation in other provinces (BC, Alberta, Quebec) and ensure a principled approach as in the GDPR to protect privacy while reducing the administrative burden on organizations working in multiple jurisdictions. Alternately, focus efforts on intergovernmental advocacy for uniform federal legislation.
5. **Harmonize with (or replace) existing provincial health care privacy legislation:** Align the proposed regulatory framework with provincial legislation (the Personal Health

---

<sup>11</sup> 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>

<sup>12</sup> Public benefit nonprofits include charities, nonprofit cooperatives (including most housing cooperatives), and other nonprofits with a public-oriented mission that do not qualify for, or do not choose to become, charities (e.g., community sport and recreation groups). For more information on public benefit nonprofits, please see ONN's 2017 paper, "Introducing the Public Benefit Nonprofit Sector," available at <https://theonnc.ca/our-work/our-regulatory-environment/public-benefit-nonprofits/>

Information Protection Act) that already governs the health care sector, i.e., refrain from multiple or conflicting layers of privacy legislation for health care nonprofits.

There is one further issue with respect to integrated government approaches. We ask that the Ontario Government take an integrated, cross-government approach to the privacy framework imposed on nonprofits that deliver services on behalf of government. A vast amount of data is provided to ministries by an estimated 6,000 to 15,000 nonprofits as part of transfer payment agreement program reporting. Nonprofits that provide a diverse range of services are required to input data into multiple databases to report to different government ministries. Staff at these nonprofits do not necessarily have the ability to export the data that their organizations input into these programs. This prevents them from being able to answer basic questions about how many of their clients are accessing multiple programs and it inhibits them from offering integrated services to those individuals. Nonprofits require access to the data they collect and submit on behalf of their organizations. Additionally, nonprofits want to be involved in developing long-term strategies about the database software they are mandated to use.

This challenge becomes all the more pressing in the context of legislation that may require nonprofits to provide a client with data about them in a unified way (data portability) or delete information about them once they are no longer a client (the right to be forgotten).

6. **Align the Ontario Government's role as regulator with its role as funder:** Ensure that data portability/interoperability requirements and other rules take into account the multiple data systems that Ontario Ministries 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.

### **Section C: Data ownership, data sovereignty, and fiduciary responsibility**

In principle, individuals should have to provide meaningful consent for the use of their data and should know how it will be used. These rights are more difficult to exercise by members of groups that have been historically disadvantaged and in many cases the subject of greater surveillance. Ontario's forthcoming privacy legislation must be developed with an equity lens and an understanding of how certain groups are unfairly targeted, discriminated against, and disempowered by the unregulated use of their members' private data. The increasing use of algorithms and artificial intelligence for data processing makes it all the more important for an explicit equity lens and a principled approach to ensuring everyone of their privacy rights.

While data privacy and ownership frameworks often focus on individuals' data, there is a category of data that has to do with collectivities, such as genetic information affecting a family line or cultural knowledge that belongs to an Indigenous group. We support the First Nations OCAP Principles<sup>13</sup> (ownership, control, access, and possession) which explicitly includes the principle

---

<sup>13</sup> For more on the OCAP Principles, see the First Nations Information Governance Centre at <https://fnigc.ca/ocap>.



that an Indigenous community or group owns information collectively in the same way that an individual owns their own personal information.

7. **Use an explicit equity lens and respect Indigenous data ownership:** Explicitly address questions of data ownership in the development of privacy legislation and adhere to the First Nations OCAP Principles, which provide a coherent and ethical framework for how the owners of data are entitled to control how their data may be used.

We are aware of the gaps in existing privacy legislation with respect to the private information of employees held by their employers. For example, employer knowledge of mental or physical health issues should not be used for any purpose other than that for which it was collected, but there is currently no law in Ontario that provides an employee with recourse in this area. We support the inclusion of employee privacy rights in a proposed privacy legislative framework. That said, new barriers should not be erected for trade unions to carry out their Charter-protected core functions and responsibilities as mandated by statute or otherwise prescribed by law.

8. **Include employee data privacy:** If new privacy legislation is introduced, it should address the gap in employees' privacy rights, such as the confidentiality of health information that comes into the possession of an employer. The new framework should not, however, erect barriers for trade unions to carry out their Charter-protected core functions and responsibilities as mandated by statute or otherwise prescribed by law.

Our last point that falls under the ethical use of private data is that the personal information of vulnerable people should not be used for profit by those who are entrusted with their care. There are many parts of the care economy -- e.g., child care, long-term care, home care, and services for people with developmental disabilities -- where both nonprofits and for-profit corporations are active. When there are opportunities for financial gain in relation to the private data of vulnerable persons, explicit rules will be needed to reconcile the profit motive and fiduciary responsibilities.

9. **Tackle directly the challenge of imposing fiduciary responsibilities, i.e., an ethic of care, on for-profit corporations.** Broad consultation on a proposed privacy framework with care recipients, caregivers (paid and unpaid), and the broader community is recommended to address this issue.

## **Section D: Implementation, education, and enforcement**

There is a compelling case for the Government of Ontario to build greater awareness and capacity among nonprofits to understand existing and forthcoming legislation regarding the use of personal information and requirements to manage data effectively - as well as how they may use it to maximize the public benefits and prevent harm. Nonprofits that operate programs and services on behalf of government, such as community health centres and homes for persons with developmental disabilities, are already subject to rules under FIPPA that govern their document retention, records maintenance, and disclosure of information. Despite this legislation having been recently amended, there has been little communication with nonprofits about the major

changes to their legislative requirements regarding communication to clients about how their information will be used.

Forthcoming privacy legislation provides an excellent opportunity for the Ontario Government to commit to a robust educational framework for organizations in all sectors of the economy to understand their obligations to protect private data. That said, an enforcement regime will be required following an initial educational period. We recommend that fines be proportional to global revenues in keeping with the global nature of the data economy. A precedent has been set in this regard, in that Europe's Information Commissioner's Office can seek a fine of up to four percent of a company's global annual revenue for a breach under the GDPR.<sup>14</sup>

**10. Educate nonprofits and produce specific, plain-language guidance for organizations:**

Plan and fund a robust sector-specific education program for Ontario nonprofits -- with the sector. The BC Office of the Information and Privacy Commissioner has set a good example with clear guidance targeted specifically to nonprofits. Organizations like Community Legal Education Ontario (CLEO) are well-positioned to manage an educational program for nonprofits in Ontario.

**11. Set fines relative to global revenues** to ensure that big data companies that violate Ontario law are fined more substantially than small business and nonprofits.

There is a second reason for forthcoming privacy legislation to have a phased implementation approach. Nonprofits, like many parts of the economy, have been hard hit by the COVID-19 crisis. A recent survey of Ontario nonprofits found that three in ten organizations had laid off staff, six in ten had experienced revenue drops, and one in five expected to close by the end of 2020.<sup>15</sup> Now is not the time to impose new administrative burdens on the sector. We are hopeful that 2021 will see nonprofit revenues bounce back (from ticket sales, fees, and other earned income as well as donations), but if the recession is prolonged, it may be necessary to wait for legislative implementation so as not to add to the stresses of an already stressed sector.

**12. Refrain from imposing new administrative burdens during a recession:** Consider the impact of the COVID-19 pandemic and related economic hardships for nonprofits and other small enterprises when determining an implementation timeline.

## Conclusion

The nonprofit sector is a principal focus of forthcoming Ontario privacy legislation and must therefore have a seat at the table in helping to shape it. Nonprofits support, in principle, privacy legislation that would ensure an ethical approach to the treatment of personal information in the public, private, and nonprofit sectors. As managers of personal data, nonprofits respect the need

---

<sup>14</sup> Mark Sweney. "Marriott to be fined nearly £100m over GDPR breach." The Guardian. July 9 2019. <https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico>

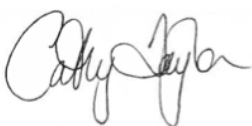
<sup>15</sup> ONN and l'Assemblée de la Francophonie de l'Ontario. "Risk, resilience, and rebuilding communities: The state of Ontario nonprofits three months into the pandemic." August 2020. <https://theonnc.ca/our-work/covid-survey-2020/>

for a robust governance framework to protect privacy rights while ensuring that data can be leveraged for the public good by the public sector and public benefit nonprofits. We are committed to helping the nonprofit sector understand that their practices -- whether in terms of fundraising, managing client data, training employees and volunteers, or engaging third parties for data management -- must align with modern privacy legislation.

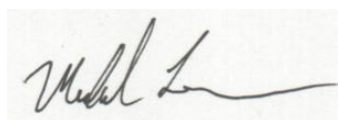
At the same time, nonprofits seek to be champions of equity and want to see legislation provide for meaningful mechanisms for individuals to know that their personal data is used only in ways they know about and consent to -- by all sectors, public, private, and nonprofit. With the extraction and manipulation of private data being a source of wealth generation for enormous and growing sectors of the economy, nonprofits support the calls for a robust regulatory framework, similar to the GDPR, that puts constraints on the monetization of personal information. As artificial intelligence is used in an increasing range of public and private initiatives, we call attention to how inequality can be exacerbated by technologies that magnify the biases of the humans who design their algorithms. A new data privacy regime must address these risks in order to have any legitimacy.

Nonprofits look forward to engaging with government on how we can all promote data justice, the genuine protection of privacy in the use of data by all sectors, and the ethical use of data in the public interest by the public and nonprofit sectors.

Sincerely,



Cathy Taylor, Executive Director  
Ontario Nonprofit Network



Michael Lenczner, Founding Director  
Powered By Data/ For the Data Policy Coalition

Appendix 1: Letter to the ONN from Paula Attfield, Chair, AFP Canada re: ONN's response to the Ministry of Government and Consumer Services' discussion paper "Improving private sector privacy for Ontarians in a digital age".



October 15, 2020

Liz Sutherland  
Director of Policy  
Ontario Nonprofit Network

Dear Liz Sutherland,

AFP Canada appreciates the opportunity to provide input to ONN regarding its response to the Ministry of Government and Consumer Services' discussion paper "Improving private sector privacy for Ontarians in a digital age". We hope that this will offer additional considerations from a fundraising perspective.

The Association of Fundraising Professionals (AFP) represents 29,000 individual fundraisers and charities that raise more than \$115 billion annually for charities around the world—equivalent to nearly one-third of all charitable giving in North America. In Canada, AFP's 3,300 members in over 21 chapters work for more than 1,800 charities across the country and raise billions of dollars every year.

While AFP Canada's mandate is a national one, we recognize the importance of these proposed privacy reforms. We believe that the potential impact on fundraising must be considered as part of this process. We fully support ONN's recommendations for sector engagement, avoiding a one-size-fits-all approach and harmonizing with the rest of Canada.

Charities have made significant efforts and investments to understand existing and prospective donors' interests and preferences. This activity stems from a desire to treat supporters with respect, by better understanding their charitable interests; the ways in which they prefer to communicate; and to broaden revenue streams for fundraising entities. Changes to legislation and regulations that inadvertently suppress the ability of charitable fundraising entities to generate revenue would hinder the ability of organizations to meet goals that are critical to the health and wellbeing of Ontarians. Please see below for our responses to specific recommendations currently under consideration.

### **Increased Consent and Clear Transparency**

*For all other collections, uses, and disclosures of personal information, the organization would need to obtain affirmative, demonstratable, informed, and unambiguous consent. Requiring individuals to “opt-in” to the collection, use, or disclosure would set the default setting as the most privacy protective option. Enhanced consent and transparency provisions would not allow organizations to collect information unconditionally but enable more explicit agreement and understanding between individuals and their service providers.  
(Ontario Private Sector Privacy Reform page 5)*

Many charities would be unable to comply with the enhanced consent and transparent privacy guidelines. It must be noted that small and mid-sized organizations in the sector are often at a disadvantage in terms of staffing levels and resources. According to Mark Blumberg’s review of CRA charity listings, more than 50% of Canadian charities have revenues under \$150,000. Many of these organizations are entirely driven by volunteers. These organizations may face undue pressure in implementing new or improved systems governing the collection and use of an individual’s information. It is rare for organizations of this size to have IT infrastructure and personnel, which hinders their ability to quickly adjust to changing technology needs.

In addition to the potential administrative burden that increased consent might have on charities, the move to “opt-in” consent if applied in a blanket way to all communications will seriously hamper charities’ ability to find new donors and to communicate effectively with existing donors. In jurisdictions where strict opt-in consent has been applied, the substantial administrative cost to charities has paled in comparison to lost revenue due to the inability of charities to solicit donations from donors where opt-in consent is difficult to obtain. At the very least, there must be room for “implied consent” for charities who have a relationship with existing donors.

AFP Canada recommends that an exemption be provided for nonprofits and charities (similar to CASL – see <https://us1.campaign-archive.com/?u=005f6731841412b698044ce64&id=9a3bb1dba1&e=95345016e8> in cases where adhering to privacy guidelines would adversely impact the organization from carrying out its mandate.

Protocols should be developed for how an individual can withdraw their consent (e.g. a request in writing to an organization; a secure link via their website; standard disclaimer in electronic communications comparable to ‘unsubscribe’ functions).

Enforcement of the legislation should be carried out in a series of warnings with educational components before more serious penalties (e.g. fines) are assessed.

### **Repurposing and Derived Data**

*Data that is “derived” from personal information is data that companies may have about customers that was not directly supplied by the customer. This kind of data (such as assessments or evaluations) repurposes personal information that has been previously supplied,*

*as well as other recorded behaviour (such as web-browsing habits). For example, companies may categorize customers based on observed shopping habits, or develop other insights about an individual's routine actions.*

*(Ontario Private Sector Privacy Reform page 8)*

Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

[\(https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda\\_brief/\)](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/)

Charitable organizations employ strategies and tactics that incorporate the repurposing of information from publicly available sources, seeking to gain insight about existing and prospective donors' 'capacity' to donate, which is partly based on estimates of relative levels of personal financial wealth (e.g. publicly available information about the selling price of a dwelling or business).

Fundraisers develop, maintain and employ derived data such as capacity assessments which categorize existing and prospective donors' and are based on both publicly available information as noted above, and information created through transactions and interactions with existing and prospective donors (e.g. charitable giving; volunteering; advocacy). This information enables a charity to identify potential supporters who are aligned to the cause and thus ensure that their fundraising efforts are more efficient and effective.

Under any new legislation or regulation, the definition of personal information should be very clearly communicated so that charities are not burdened with unnecessary administration of data that is not beneficial to the protection of the interests of Ontarians.

The definition of derived data, and the way in which fundraising entities are required to manage such data are critical issues in the success of charities in meeting their missions.

It is recommended that further consultation regarding definitions be undertaken in a timeframe that permits more comprehensive engagement with leaders within the nonprofit and charitable sector.

The most important consideration is that the charitable sector, and especially the fundraisers within it, need to have a seat at the table for any discussions about tightening privacy regulations. What do we need? We need to be heard, along with industry, in public consultations. We are a significant part of the economy and we do very important work, often on behalf of the most vulnerable members of our society. A new privacy code which constrains

our ability to solicit funds on behalf of beneficiaries could have tragic consequences. There is no question that citizens have privacy rights that need to be protected but these must be balanced by the rights of the beneficiaries whom we help.

We need to establish the absolute necessity for charities and fundraising to be represented at the table where substantive and detailed discussions are going on. The devil is very often in the details, and unless we are represented, there is a good chance that the new regulations will have unintended negative consequences.

AFP appreciates this opportunity to submit these considerations. For additional information please contact Lisa Davey, vice president, AFP Canada, at 613-407-7169 or [lisa.davey@afpglobal.org](mailto:lisa.davey@afpglobal.org).

Sincerely,

Paula Attfield  
Chair, AFP Canada