ontario chamber of commerce
2105-180 Dundas Street West
Toronto, ON, M5G1Z8
occ.ca | @OntarioCofC

September 1, 2021

The Honourable Ross Romano
Minister of Government and Consumer Services
College Park 5th Floor
777 Bay St
Toronto, Ontario, M7A 2J3

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch
134 Ian Macdonald Boulevard
Toronto, Ontario, M7A 2C5

RE: Modernizing Privacy in Ontario (21-MGCS015)

Overview

In a world where data underpins most of the goods and services we rely on each day, privacy and trust are imperative. Businesses of all sizes use data to operate, innovate, and serve their customers. They need clear and effective legal frameworks within which they can operate, innovate responsibly, and continue advancing our economic and social progress with data.

In Canada, this means commercial privacy laws should remain national in scope. The Government of Ontario's proposals to move forward with a provincial privacy framework would likely have significant unintended consequences – particularly for small businesses, non-profit organizations, and individuals who increasingly rely on digital services.

The timing is also regrettable. Businesses across the province are focused on reopening and recovery. Several industries, including food and accommodation services and health care, are facing labour shortages as they seek to rehire and get the economy back on its feet. Ontario's latest privacy proposals would force these organizations to simultaneously hire technical staff and invest in specialized infrastructure to comply with new, complex regulations. Even if implementation is delayed, the introduction of these measures is detracting resources from recovery.

We would like to thank the Government of Ontario for the opportunity to provide feedback on behalf of Ontario's business community. Our submission focuses on the following areas:

1. Federal leadership
2. Technical proposals
3. Supporting innovators and small businesses

1. Federal Leadership

Commercial activity within Ontario is governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA). Last year, the Government of Canada initiated a process to modernize PIPEDA through Bill C-11. This has resulted in lengthy – yet necessary – debates about the future of privacy legislation in this country.

While Bill C-11 was imperfect and delayed, the business community feels federal leadership remains the most appropriate way of moving forward with privacy legislation. Maintaining a national approach to commercial privacy protection is critical, as fragmentation across Canada would:

- Add unnecessary uncertainty and costs – particularly for small businesses looking to expand nationally or globally but lack the technical capacity to navigate a patchwork of different rules, as well as companies developing digital products (such as virtual care platforms).
- Deter innovation and investment in Ontario.
- Put Ontario businesses at a competitive disadvantage.
- Compromise Ontarians' ability to access to digital services, which have become even more important during the pandemic.

As noted in Ontario's Digital and Data Strategy, data privacy should be a competitive advantage for Ontario businesses. The approach proposed in this white paper would achieve the opposite outcome, by establishing a less harmonized approach that will discourage businesses in the province from investing in digital innovation that benefits consumers.

In Quebec, where the provincial government is moving forward with a provincial privacy framework through Bill 64, surveys indicate that 66 percent of small businesses do not understand the impacts of Bill 64 and do not have robust privacy programs needed to comply with new provisions.[1]

We understand that Ontario wants to become a leader in privacy protection. However, it is important to note that the European Union's General Data Protection Regulation (GDPR) was backed by years of extensive consultation between the 27 member jurisdictions and businesses. Such a concerted effort has not been carried out in Ontario.

As businesses recover from the impacts of COVID-19, Ontario's proposals to add more red tape would hamper those efforts. We must remember that Canada is a relatively small economy, and regulatory fragmentation only limits our global competitiveness. It would be far more effective for Ontario to advocate for necessary changes at the national level.

[1] Survey of 74 businesses delivered by Canadian Life and Health Insurance Association (CLHIA) and Federation des chambres de commerce du Québec (FCCQ) in May 2021.

2. Technical Proposals

The Government of Ontario's white paper outlines a series of proposals relevant to Ontario businesses. The following section provides feedback on some of those.

Data portability: The Ontario government is proposing to give individuals the right to access their personal information held by businesses, challenge its accuracy, have it erased, and/or have it transferred to other organizations in a machine-readable format. The latter – known as data portability – would have a significant impact on many organizations.

As noted in the white paper, sector-specific standards will need to be established around data portability. In certain cases, there are technical and operational barriers, risks around privacy and identity thefts, and legacy systems that need to be addressed. Rather than a one-size-fits-all approach, it is important to work with industries to understand the nuanced challenges and opportunities. Any new measures around data portability must align with the standards, policies, and platforms being developed internationally to avoid placing businesses in Ontario at a competitive disadvantage.

Further, it is important to focus on personal information that is provided by the individual rather than data that is generated about them (known as derived or inferred data). When companies use their own analytical tools to develop insights or inferences, the new information they create becomes intellectual property, often critical to their competitive advantage. Further, de-identified data should be exempt as it protects individual privacy. To that end, Australia has excluded imputed data, as well as data that cannot be re-identified, from portability requirements.

Consent: As data practices have evolved over time, obtaining informed consent from data subjects has become more and more challenging. The phenomenon of consent fatigue mentioned in the government's white paper is indeed a growing challenge. We support modernization of consent requirements but caution that they must be expressed as principles, rather than overly prescriptive rules that risk becoming outdated over time and undermine interoperability with consent requirements in other jurisdictions.

Guidance and support from privacy commissioners and industry associations can help organizations adopt best practices and update their consent policies over time. The OCC's 2020 report – *In Data We Trust: Unlocking the Value of Data in Ontario* – highlights some of these best practices:

- Phrasing consent notices in terms that can be understood at a grade seven level.
- Applying lessons from behavioural insights to develop privacy terms and conditions such that consumers better understand what they are consenting to. For example, it helps to provide information in shorter pieces at relevant times.
- Offering consumers different options for consent, which could involve proportional tiers of service and/or pricing.
- Continuously updating consent policies as technologies and consumer literacy evolve

It is also important to recognize legitimate exceptions to explicit consent. We are pleased to see Ontario's proposal to allow for implied consent under certain circumstances depending on the sensitivity of the personal information involved and the reasonable expectations of the individual. The GDPR takes a pragmatic approach by outlining five grounds for processing in addition to consent: performance of a contract, compliance with a legal obligation, vital interests of the data subject, public interest, and legitimate interests.

Fraud is one practical example. Insurance companies should be allowed to collect, use, and disclose personal information without consent for fraud detection purposes, as this aligns with consumers' interests and expectations. Bill C-11 includes a provision that would allow an organization to collect and disclose an individual's personal information to another organization when reasonable for the purposes of detecting, suppressing, or preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with knowledge or consent would compromise the ability to prevent, detect, or suppress fraud. We believe that provision should include use of data (in addition to collection and disclosure), but the general approach is adequate, and industry is working with the federal government to strengthen this clause.

Additionally, as noted in the white paper, consent is not a practical means of protecting employees' privacy as there is an inherent power imbalance at play, and employers have legal obligations to collect, use, and disclose personal information regarding their employees for tax records and other purposes. Therefore, we agree that it should be sufficient in most cases for employers to notify their employees when their data is being collected, while obtaining their consent for data collection that is not necessary to the employment relationship.

Governance programs: The government's white paper also considers a potential requirement for organizations to develop privacy management programs governing their collection, use and disclosure of personal information, and make those programs available for review. It also considers requiring organizations to carry out privacy impact assessments of the privacy-related factors on any information system project or electronic service delivery involving personal information.

While the government suggests such requirements could be scalable to the size of the organization and sensitivity of the data involved, there is a real concern about the implementation costs and burden this would entail, especially for small businesses and non-profit organizations that lack the resources and technical expertise within their staff, as well as organizations that are subject to overlapping requirements in other jurisdictions. According to the survey done in Quebec, businesses expect to double their privacy teams to comply with Bill 64. With a patchwork of provincial frameworks, the complexity and costs of compliance would multiply even further. To strike the right balance, we feel that requiring a single privacy management program would provide sufficient protection where sensitive information is collected, without the need for additional privacy impact assessments.

The white paper also considers requiring organizations to follow privacy by design principles, whereby data protection is given due consideration at all stages in the development and implementation of systems, software, solutions, and services. As noted in the OCC's report, it may make sense for governments to encourage the use of privacy by design principles as a means for organizations to comply with their privacy obligations. Sharing practical guidance and supporting the development of relevant industry standards would help achieve this.

The practices of privacy by design and privacy impact assessments are already in place in certain sectors, particularly when it comes to large enterprise or public sector contracts. There is no need to add provincial governance on top of what is already required, such as in the health care sector, where compliance processes are over-architected and exceptionally challenging given the siloed nature of data infrastructure.

Automated decision-making systems (ADS): In Ontario, automated technologies are used to support everything from autonomous vehicles to modern financial services, health care, smart cities, and more. In the long-term, widespread adoption of ADS is expected to raise productivity and output, improve the quality of products and services, create more jobs than it replaces, and lower prices for consumers.

The Government of Ontario is proposing to prohibit the use of ADS when these systems could cause harm to citizens, require organizations to inform Ontarians of when and how their data is used by ADS, and enable consumers to object or consent to their use.

These proposals are unnecessarily broad and inconsistent with global standards. The requirement on organizations to explain predictions, recommendations, *and* decisions involving ADS would apply to a large volume of everyday, low-risk scenarios in which organizations use computer coding to assist human decision-making. By contrast, the GDPR only requires explanations for decisions that replace human decisions (not recommendations or predictions), and only those that produce legal or similarly significant effects concerning an individual (such as their legal status, financial interests, access to health services, or employment opportunities). The latter takes a much more risk-based approach to ADS, balancing the need to promote innovation while protecting individuals.

Further, giving individuals detailed information about algorithms is unlikely to arm them with useful information about their privacy, but it could force organizations to share proprietary information that compromises their intellectual property. There must be reasonable limits on disclosure requirements similar to the GDPR, so that organizations must provide "meaningful information about the logic involved" in ADS and consequences for the data subject without disclosing confidential information. For example, organizations should not be expected to disclose the details of fraud detection analytics, as doing so would undermine the effectiveness of such tools.

The unilateral overreach in Ontario's proposals will disincentivize businesses from developing or using ADS, undercut Ontario's competitive advantage in artificial intelligence, and limit consumers' access to products and services that use ADS.

Oversight: Effective oversight is essential to protect individuals, ensure accountability, and create a level playing field for businesses. Some experts have criticized the federal and provincial privacy commissioner offices in Canada for lacking sufficient enforcement authority. However, there is a concern that giving the privacy commissioners greater powers could deter organizations from approaching them for guidance when they are contemplating using data in new ways.

On balance, greater enforcement may be necessary, but the focus should be on where there are real risks to individuals. Specifically, the white paper proposes to establish administrative monetary penalties of $10,000,000 or 3 percent of an organization's global annual revenue (whichever is higher) to deter and punish noncompliance. These amounts are disproportionate to the size of Ontario's market when compared to other frameworks like the GDPR. They should also be scalable to the severity of the wrongdoing, with the maximum fine reserved for repeated offenders and/or serious and intentional non-compliance that causes demonstrable harm to the consumer.

One advantage of a national privacy law is that it avoids duplication in enforcement. In the absence of a national law, provincial privacy regulators should coordinate to avoid levying penalties in different provinces for the same incident.

Finally, there must be checks and balances on the privacy commissioner's enforcement powers through appeals and mediation processes. While the white paper does reference an appeal process, it only applies to matters of law and not the quantum of the fine. Since non-compliance can sometimes result from a lack of clarity, a mediator could help provide certainty that decisions are fair and grounded in facts. Codes of practice and certification programs could be another proactive tool for compliance.

3. Supporting Innovators & Small Businesses

The final pillar of the government's white paper is focused on supporting organizations in Ontario that wish to use de-identified personal information for research and innovation purposes. This complements important work the Province is doing to support digital innovation, such as developing a government-issued digital identity for individuals and businesses.

De-identified information: As noted in the white paper, there are many opportunities for organizations to use de-identified or anonymized personal information for research that can spur economic activity and help address social challenges. We agree that there is a need for clarity around how privacy rules apply to these types of data and support Ontario's suggestion that data access, portability, correction, and deletion requirements should not apply to anonymized information.

Further, as noted above, explicit consent should not be required as long as appropriate techniques have been applied to protect against re-identification.

To that end, there is a need for clear and consistent definitions and standards around de-identification. Under existing federal laws, information that has been de-identified by removing or replacing direct identifiers is still considered personal information as it can be re-identified, while information that is fully anonymized is subject to less restrictive requirements. Similarly, the GDPR states that the principles of data protection should apply to pseudonymized data (i.e. data which could be attributed to a natural person by the use of additional information) but not anonymous information (i.e. personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable).

In the OCC's report, we explain that this is an area where organizations would benefit from guidance to ensure de-identification techniques are robust and secure. For example, one technique more organizations could adopt is known as differential privacy, which involves adding random noise to datasets to prevent them from being de-anonymized. Differential privacy has been increasingly adopted by businesses, as well as the US Census Bureau.

Data sharing: One important opportunity for the Province to support innovation is by facilitating data sharing across siloes. To that end, Ontario should work more closely with the private sector and the federal government to develop a more robust national data sharing strategy. Information collected in Ontario should be aggregated and shared with entities across Canada, including with smaller businesses that have been hit hardest by the pandemic and lack the capabilities to carry out their own data collection and analysis.

Data trusts are a mechanism for governments, businesses, and non-profit organizations to access and share data more easily under robust privacy and security protections. The Government of Ontario should experiment with data trusts to make better use of its own data while taking its open data system to the next level. Eventually, data trusts could underpin a variety of digital government services and enable cross-jurisdictional data sharing. Meanwhile, Ontario should work with its federal, provincial, and territorial partners to develop clear policy parameters to support the development of data trusts by businesses and other organizations. Again, a coordinated approach across Canada is important. Participating in these data trusts should be voluntary for organizations.

Conclusion

Privacy is fundamental to the prosperity of Ontarians and our economy. If Ontario is to become a world-leading digital economy, it needs to work with the federal government and business community to ensure privacy legislation is principles-based and interoperable with global norms.

For more information about the recommendations in this submission, please see our previous privacy submission and our report, *In Data We Trust: Unlocking the Value of Data in Ontario*. We welcome the opportunity to discuss this issue further.

Sincerely,

Rocco Rossi
President and CEO
Ontario Chamber of Commerce