RCC RETAIL COUNCIL OF CANADA
CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

1881 Yonge Street
Suite 800
Toronto, ON M4S 3C4
(416) 922-6678
1 (888) 373-8245

October 16, 2020

Hon. Lisa Thompson, Minister of Government & Consumer Services
College Park 5th Floor - 777 Bay Street
Toronto, Ontario
M7A 2J3
LM.Thompson@ontario.ca

Dear Minister Thompson,

Retail is the largest private sector employer in Ontario, with 11% of Ontario jobs working in retail, or over 844,000 Ontarians (2019). Across Canada, core retail sales (excluding vehicles and gasoline) were $385 billion in 2019.

Like many Ontario business sectors, the retail industry has been adversely affected by Covid-19. Statistics Canada reports that May's retail sales were 20% lower than February levels. Even by July 2020, the latest Statistics Canada retail sales results, some retail sectors were still well below 2019 sales levels.

We suggest that a made-in-Ontario private sector privacy law should not be pursued until PIPEDA amendments are tabled and approved. Rather, the Ontario government should work more closely with the federal and other regional governments to ensure aligned, interoperable private sector data privacy frameworks across Canada.

We suggest that the Ontario government take a strong role in working with other jurisdictions to ensure that no proposed Ontario privacy requirements (i) overlap or differ from those in the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), as it may be amended, which already applies in Ontario and (ii) after PIPEDA harmonization, are as interoperable as possible with provincial frameworks.

Stronger regional collaboration will still protect Ontarians' personal information, given that PIPEDA modernization amendments are expected. It will also significantly reduce red tape and compliance burden, providing the clear and consistent policy landscape industry needs to innovate and compete for investment. In particular: once amendments to PIPEDA are announced, the Ontario government will be better able to evaluate whether a private-sector privacy law is indeed still desirable in the province.

RCC appreciates the government's attention to the issue of consumer privacy. In that spirit, we include some general comments from a retail perspective and look forward to continued consultation and collaboration with government.

Warm regards,

Retail Council of Canada

Sebastian Prins, Ontario Director of Government Relations, sprins@retailcouncil.org, 647 687 9049
Kate Skipton, Senior Policy Analyst, kskipton@retailcouncil.org, 647 296 7032

CC'ed:

- David DiPaul, Chief of Staff, Ministry of Government & Consumer Services
- Thomas Staples, Stakeholder Relations and Legislative Affairs Advisor, Ministry of Government & Consumer Services
- General Consultation Inbox for Access and Privacy Strategy and Policy Unit, Ministry of Government & Consumer Services

How retailers use PI

Data is critical to retail. Consumers increasingly expect retailers to know, remember, and live up to their personal expectations in how retail services are delivered. The corollary of consumer expectations is that many types of data contain or incorporate insights from personal information (PI) entrusted to retailers in the normal course of business. Examples include PI related to sales and marketing, customer experience and retention, payment processing, delivery, returns, and loyalty programs.

Many Ontario retailers do business across Canada and internationally. Because the retail industry has a strong need to create standout customer experiences, we invest in the talent and resources necessary to navigate global data privacy requirements while meeting our customers' experience expectations. Proposed changes to privacy frameworks at any level of government should not impede retailers' ability to deliver on those expectations.

Alignment across privacy regimes

The retail sector contains a variety of sub-sectors that include apparel, appliances, jewelry, health and personal care, furniture, general merchandise, cannabis, grocery and others. Generally, retailers are already subject to PIPEDA's well-established, principles-based framework in Ontario and have developed compliance programs to follow it.

Yet a mosaic of different regional privacy requirements risks developing in Canada, with the federal government as well as Quebec, British Columbia and now Ontario in various stages of private sector privacy review and reform. To try to do business in a relatively small (by global population) country containing potentially four different, yet nevertheless rigorous data privacy regimes would chill enterprise and innovation, potentially inter-provincially as well as internationally. Such a situation in Canada may prevent retailers from servicing customers and in short lead to investment going elsewhere. It may also lead to undue complexity for retailers and consumers alike, putting Canadians at risk of data breaches due to confusion between a hodgepodge of different provincial and territorial regimes.

Creating another private sector privacy regime in Ontario, especially given the ongoing business challenges presented by the pandemic, risks significantly higher compliance burden without a clear PI protection benefit, especially in areas addressed already by PIPEDA. RCC therefore suggests that the Ontario government instead work more closely with the federal government, as well as regional governments, toward clear and consistent data privacy policy across Canada.

RCC also recommends that any Canadian data privacy regime addressing commercial activities, no matter the jurisdiction, (i) be principles-based and technology-neutral to balance the protection of consumer trust with the commercial importance of promoting innovative new technologies, (ii) facilitate simple transborder dataflows, and (iii) not unduly restrict the adoption of new data-driven and other technologies, including those leveraging artificial intelligence, biometric data, and the Internet of Things.

Economic impact of another private sector privacy law in Canada

Ontario retailers continue to deal with the harsh impact of COVID-19 without any end in sight in the short to medium term. Concerns are now increasing with a second wave of Covid-19 appearing, which may once again lead to significant retail shutdowns and decreased consumer spending. Adverse developments in the retail sector have a significant impact on Ontario jobs in warehousing, transportation, information technology and commercial property management.

While protecting individuals' data privacy is important, it is key that any proposed new data privacy protections involve a thorough consideration of impact to consumers, compliance costs and market inefficiencies. RCC encourages government to broadly view policy development work through an economic lens. For example, upgrading legacy IT infrastructure and redesigning business protocols would be net new costs for retail and other business sectors. In an environment of conflicting privacy regimes, these costs may multiply at a time when the industry needs to recover and small retailers and other types of businesses struggle to keep their brick and mortar locations open.

In the United States, new data privacy laws are under consideration in many states as well as federally. The Information Technology and Innovation Foundation (ITIF) recently published a detailed study estimating that if Congress were to pass legislation that mirrored many of the key provisions in Europe's *General Data Protection Regulation* (GDPR) or California's *California Consumer Protection Act* (CCPA), it could cost the U.S. economy approximately $122 billion, or $483 per U.S. adult, per year. That would be more than 50% of what Americans spend on their electric bills each year.

Considerations similar to those outlined by ITIF would apply in Canada and to Ontario businesses, especially if the pending mosaic of stricter and different data privacy regimes across Canada materializes instead of a consistent national framework. For example, there would be the need to find and engage many more data protection officers and database administrators. Other data privacy compliance costs of a GDPR or CCPA-like regime would include, without limitation, a significant increase in data security audits, privacy impact assessments and technological solutions to facilitate consumer data deletion, rectification and portability requests. Again, these costs and obligations will be magnified if differing regimes are adopted federally and in other provinces currently undertaking privacy legislation reviews.

Retailers may also experience inefficiencies from decreased innovation. These would include failing to meet customer expectations for personalized offerings and creating consent fatigue with customers. They would also include reduced ad effectiveness and missing out on data-driven opportunities that could have been discovered by analyzing un-collected data.

Added together, the costs to retailers of a strict data privacy regime for Ontario alone, especially a new one that overlaps PIPEDA, could be very considerable, especially if that regime is unduly prescriptive or carries unreasonable penalties.

RCC's general comments on the Discussion Paper

RCC suggests that the Ontario government not pursue a made-in-Ontario privacy regime until PIPEDA amendments are announced. Instead, we suggest that the province take a strong role in collaborating with the federal and with regional governments toward a nationally aligned, harmonized approach to private sector privacy across Canada. New made-in-Ontario private sector privacy requirements that duplicate or differ from existing or amended federal requirements would lead to needless red tape and significant compliance burden, likely disincentivizing innovation and competition for investment in the province.

Our general comments on some of the Discussion Paper topics are as follows.

Transparency and Consent

Transparency is an important privacy principle: it is key in order for a person to meaningfully consent to how their data is used. Yet policymakers must be realistic about the levels of transparency and consent they require from commercial organizations and consumers. Requirements that are disproportionately onerous can cause consumer fatigue and have a chilling effect on commerce.

The Discussion Paper proposes a requirement for express consent for any collection, use or disclosure of personal information, unless an exception to consent has been established for a given circumstance. We agree there are several instances where individual consent is not necessary, practicable or appropriate. We suggest that consent is best leveraged as a privacy safeguard for the use, collection and disclosure of sensitive PI, or for when there are new purposes that could not have been reasonably expected by consumers.

To enable innovation and efficient operations and to spare consumers, it is also critically important that private sector privacy regulations allow for various legal bases for processing PI (e.g. for legitimate business interests) without the need to obtain consent, while requiring retailers/data controllers to demonstrate accountability for the PI they process.

The Discussion Paper's approach to transparency largely aligns with PIPEDA and the OPC's interpretation of the federal law, despite the paper's suggestion that enhanced transparency is needed. Plain language privacy policies that allow for meaningful consent are already a key implementation mechanism for PIPEDA transparency, consent and openness requirements. The Discussion Paper also leaves out the important role played by implied consent and the ability of organizations to rely on implied consent for appropriate data processing activities, based on the context, reasonable expectations of the individual, and the sensitivity of the information. These nuances again raise the question of what benefit a made-in-Ontario approach to consent and transparency would have, when PIPEDA already provides PI protection to Ontarians.

Outsourcing and cross-border data flows

Across a border or not, data transfers to third parties should remain governed by an accountability-focused framework that harmonizes with the federal Guidelines for processing personal data across borders. This PIPEDA framework, long followed by Ontario retailers, requires organization-to-organization accountability based on binding contractual terms for data transfers.

Data portability

While data portability offers certain benefits to both consumers and businesses, it carries inherent risks to consumer protection, privacy, confidentiality and cybersecurity, downsizing innovation and competition.

Operational considerations as well as consumer expectations may vary from industry to industry. A robust architecture to support data portability is necessary. Care must be taken to avoid data breaches and exposure to fraud, as well as to provide appropriate levels of data authentication (eg: where the data is sensitive) and encryption. Technical feasibility considerations, such as the appropriate format for sharing the data and appropriate communications and processes for engaging individuals who request that their data be shared, are also key considerations, as is interoperability with other jurisdictions.

In practice, there are many complexities and uncertainties associated with data portability. An in-depth study of the mechanics of data portability and its many privacy and non-privacy implications for different sectors is needed before integrating such a policy into any Canadian privacy framework.

De-identification

De-identification of PI to protect consumer information is a reasonable policy and increasingly important to innovation and the digital economy. RCC believes organizations would benefit from clear definitions around de-identification and related concepts and applicable consent requirements (i.e., consent is not required when certain, clear de-identification standards are met).

A common set of standards should be developed in consultation with industry to help organizations assess and implement their processes with respect to de-identifying personal information. It is important that any definitions and standards encompass a realistic risk spectrum for re-identification so that businesses can adopt innovative approaches to data analysis.

Deletion and the Right to Erasure

The Discussion Paper discusses introducing an Ontario-based data erasure, or de-indexing, right (also referred to as the “right to be forgotten”). This would enable individuals to request that organizations, notably search engines, permanently de-index or delete their personal information. We strongly urge the Ontario government to put this proposal on hold and align with the federal government’s proposed approach to modernizing PIPEDA, which explicitly excludes de-indexing because the matter is before the Federal Court of Canada.

We also reiterate our suggestion that the government consider clearly defining and setting standards for de-identification. De-identification can be an effective tool to delete PI by anonymizing it.

Breaches

Ontario retailers are already subject to PIPEDA breach notification requirements. They already need to keep records and, if there is reasonable risk of significant harm, notify the federal regulator and individuals affected.

With such requirements already in place to protect consumers, creating overlapping or different requirements in Ontario, not to mention the other provinces in the process of privacy law review and reform, may result in non-compliance due to confusion between various reporting expectations. Such new requirements would again risk significant red tape and chill on business, without providing a marked increase in PI protections given PIPEDA's protections in this area.

Enforcement and penalties

The prospect of several rigorous, but different, enforcement regimes across British Columbia, Ontario, Quebec and federally raises significant business uncertainty and risk. Retailers would need to invest significant resources to adapt their compliance programs for an activity (PI handling) that often flows across several jurisdictions. They could be looking at multiple sets of penalties calculated on pan-Canadian or even global profits, with potentially different criteria for when these penalties would be levied.

We again suggest that PI protection and trust are best accomplished through a consistent national policy and enforcement approach. It is also critical that any proposed enforcement regime include appropriate procedural safeguards.

Proactive compliance strategies

RCC is generally supportive of proactive compliance strategies such as education, specific guidance and advisory services. We suggest and will welcome ongoing government-industry collaboration as the frameworks are developed to allow consistent, well-balanced data privacy governance in Canada.

RCC thanks the Ontario government for the opportunity to consult on the Discussion Paper. We welcome further conversation and collaboration with the Ontario government about its data privacy initiatives.