CANADIAN MARKETING ASSOCIATION
CMA

55 University Ave, Suite 603, Toronto, Ontario, M5J 2H7
416.391.2362 ● theCMA.ca

August 6, 2019

Office of the Privacy Commissioner of Canada
Ottawa, Ontario

RE: CMA Response to OPC's Consultation on Transfers for Processing

Dear Commissioner Therrien:

The CMA appreciates the opportunity to provide feedback as the Office of the Privacy Commissioner (OPC) revisits its longstanding policy position on transfers for processing under PIPEDA. As the voice of the marketing profession in Canada, we are committed to helping Canadian marketers maintain high standards of professional conduct and transparency through our mandatory Code of Ethics & Standards of Practice and other resources, including the CMA Guide to Transparency for Consumers, which helps organizations provide clear, user-friendly information to consumers about how personal information is collected, used and shared.

We urge the OPC not to change its interpretation of the current Act with regards to third-party processing. The proposed re-interpretation is at odds with the stated objectives of PIPEDA and its original Parliamentary intent, as well as Canada's wider government and economic agenda to balance the rights of consumers with reasonable restrictions on business. In fact, it would not achieve either of these objectives. The additional consent that would be required would not be in the best interests of consumers. Consumers would not benefit from any meaningful improvement in privacy protection. Instead, the change would contribute to "consent fatigue", causing consumers to be less likely to carefully review notices and make informed decisions on when to provide their consent, rather than empowering them by improving transparency and strengthening the accountability of organizations to their customers and the public.

In addition, Canadian businesses that are vital to Canada's economic competitiveness, and other organizations (such as non-for-profits that rely on third parties for data processing), would face complex operational consequences and significant disruption. In some cases, this could result in interruptions in service and confusion for consumers.

The significant practical consequences for organizations and consumers that this change would impose must be balanced with the real additional privacy protection the requirement for consent would offer.

The prospect of the re-interpretation has already created significant uncertainty for business.

The CMA and its members strongly believe in the strength of the long-established interpretation, which states that organizations that transfer personal data to third-party service providers do not have to obtain additional consent from individuals, as long as the other PIPEDA principles are adhered to. The OPC's new interpretation on third-party transfers is at odds with the accepted treatment of consent for such relationships to date, not only under PIPEDA but also under provincial private sector privacy laws and the GDPR.

Many of the questions raised by the OPC in its reframed discussion document released on June 11, 2019 are the subject of ISED's consultation on PIPEDA reform, which was announced on May 21, 2019. The CMA, like many stakeholders, is engaging with ISED to provide feedback on how the future state of the law should provide effective privacy protection in the context of transfers for processing, and will be happy to share our comments with the OPC when they are formally submitted. In the interim, we are pleased to provide the following detailed comments on the OPC's recent reinterpretation of PIPEDA as it pertains to transfers for processing, followed by some implementation requirements.

Detailed Comments

The CMA strongly urges the OPC to maintain its longstanding position on transfers for processing under PIPEDA. The CMA, representing more than 400 corporate, public and not-for-profit organizations across the Canadian economy, is opposed to the proposed re-interpretation for the following reasons.

1. Negative consequences for consumers

The re-interpretation involves an assumption that individuals will be better served by the new consent requirement than the other requirements in place. In fact, the new requirement would have negative consequences for Canadian consumers.

Requiring consent each and every time a third-party relationship is explored within each business relationship places an undue burden on consumers. Individuals would find themselves facing more frequent and increasingly voluminous requests for consent when they interact with an organization that transfers personal information for processing purposes. This is contrary to the objective of creating more readable privacy policies and procedures that avoid information overload and facilitate understanding by individuals, as reflected in the CMA Guide to Transparency for Consumers.

The abundance of requests for consent could mislead people to think that there might be something inherently risky or wrong with third-party transfers, when in fact, they are part of normal business practice and organizations are subject to clear obligations to protect consumer data.

We appreciate the OPC's suggestion that the form of consent required (express or implied) be determined based on an assessment of the sensitivity of the information, the reasonable expectation of the individual and the risk of harm to an individual. Where there is a material risk of harm, it is recommended that express consent be required. However, based on the interpretation of material risk of harm acknowledged by privacy commissioners to date, we can foresee a slippery slope with express consent being required in most cases involving third-party processing.

Compounding this, the proposed requirement to give individuals a choice of options if they do not wish to have their personal information transferred is impractical for the majority of organizations. In fact, it works against our common goal of obtaining meaningful consent. In many cases, consent would be illusory as the requirement would not mean individuals have any choice at all but to walk away. A customer who is very interested in a product or service is not likely to make that choice.

In addition, organizations may have trouble re-obtaining consent from current customers who may be unresponsive or difficult to reach. This could lead to interruptions and stoppages in ongoing services that individuals rely on, including critical services, such as banking, internet access and phone services. The potential for service interruptions is highest and of the utmost concern for those in vulnerable groups (e.g., elderly people and those with health or disability issues), where interruptions in communications services could be disastrous.

2. Operational challenges for organizations

We reiterate that the proposed shift from a notice approach to a consent approach would be considerably more onerous, resulting in negative practical consequences and additional costs for the Canadian organizations that fuel our economy and create jobs for everyday Canadians. Organizations would have to revise policies and procedures (already recently updated in compliance with the new Guidelines for Obtaining Meaningful Consent) to account for a vast number of situations in which additional consent would have to be obtained from data subjects.

Any organization subject to PIPEDA would have to re-evaluate and likely adjust its approach to its relationships with third-party data processors, significantly affecting its outsourcing and cloud computing relationships with vendors and related companies. Organizations would need to invest significant time and resources into re-arranging or updating the terms of their third-party processing relationships, including through renewed vender due diligence and the renegotiation of terms.

We would expect an inevitable push for some organizations to engage in a costly switch of third-party providers, including assuming penalties for the early termination of otherwise productive contracts, and passing these costs on to consumers. For organizations with several outsourced providers, the task could be crippling. Other organizations may decide to keep everything in-house, thereby not realizing costs savings and losing the ability to leverage service providers' expertise. In addition to stifling innovation, the change has the potential to create competition issues. For example, a lack of suitably compliant providers overseas may push organizations to shift their outsourcing arrangements in favor of a select few local providers.

In addition, the burden has consequences for third-party service providers themselves, who in most cases perform essential functions. Many of the CMA's members are trusted and renowned third-party service providers, tasked with analyzing and providing insights on client data for thousands of individual clients. These businesses operate in full compliance with PIPEDA, and there would be an undue burden without a corresponding privacy-related benefit, not only on each of these organizations' clients but also on individuals if additional consent was required.

3. Misalignment with original Parliamentary intent

There is no specific mandate under PIPEDA to require consent for third-party data transfers, whether they be domestic or cross-border. The legal argument for the re-interpretation of the consent requirement seems to be that because nothing explicitly exempts data transfers from consent requirements, that consent should now be required. This is particularly concerning because additional consent is not the best tool for effective privacy protection in this case.

The original PIPEDA legislation passed by the Parliament of Canada makes a careful distinction between two terms used for the sharing of personal information between entities: "disclosure" and "transfer". Subsequently, the OPC's January 2009 guidelines on transborder data flows of personal information to a third party for processing explicitly state that "assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required", unless an exception is applied. To date, the OPC has taken the position that the sharing of information with a third-party service provider constitutes a "use" and not a "disclosure" for the purposes of PIPEDA. This is an appropriate interpretation given PIPEDA uses the word "transfer" in reference to third-party processors, when it could have used "disclosure".

Parliament was clear in its original intent and wording. The issue of consent for third-party processing, including across borders, was not a new concept at the time of the passing of PIPEDA. In fact, “onward transfers” were being intensely debated in the policy sphere, including with respect to the EU Data Protection Directive. It is consistent with Parliament’s original intent to enable all transfers for third-party processing to proceed without additional consent and to have this practice applied consistently, whether within Canada or across borders.

4. Lack of interoperability with other privacy frameworks and jurisdictions

No other jurisdiction in the world requires consent in this regard, not even the GDPR. Similar Canadian privacy laws, such as Ontario's PHIPA, explicitly treat the sharing of information with an agent or service provider as a "use" of information by the custodian, rather than a "disclosure" to a third party that would require additional consent. If the OPC was to adopt the opposite interpretation with respect to PIPEDA, organizations may find themselves subject to conflicting rules and obligations of different privacy regimes across the country. The decision will be at odds with our common goal of interoperability across Canada, and across borders. Requiring consent would also be inconsistent with the APEC Privacy Framework, the APEC Cross-Border Privacy Rules, and the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows.

5. Consent not a remedy for failure to adhere to other PIPEDA principles, offers no additional meaningful privacy protection for individuals

We live in an increasingly globalized and digitalized world. In the modern digital economy, a reasonable person would recognize that the storage and processing of data are functions frequently performed by third-party service providers on behalf of organizations. While consent remains an important aspect of PIPEDA, we must be careful not to place too much emphasis on it alone. Consent does not waive an organization’s other obligations under PIPEDA, most notably Openness and Accountability, and it becomes superficial in their absence. Whether or not an individual consented to the transfer of personal data for processing would not address the governance issue the OPC wishes to solve.

Under the principle of Accountability, an organization is responsible for personal information transferred to a third party for processing, including overseas transfers, and must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Under the principle of Openness, an organization must clearly notify individuals at the time of collection that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities in that jurisdiction.

We understand that the proposed reinterpretation was influenced by the OPC’s finding that two well-known companies fell short of a number of their obligations under PIPEDA. We believe these cases do not warrant a far-reaching reinterpretation of the consent requirement for third-party processing that is disruptive for all organizations. Rather, they highlight the importance of organizations upholding their current obligations under PIPEDA, including fundamental Openness and Accountability obligations.

Given the nature of data flows, these obligations are the most effective form of responsible data governance. Organizations must be responsible for their accountability chains, and for assessing and mitigating associated risks. Their reputations depend on it. If this responsibility is transferred to individuals, it can become illusory.

Self-regulation is an important and effective tool to ensure these requirements are upheld. At the CMA, we continue to champion self-regulation, including through our mandatory CMA Code of Ethics and Standards of Practice for members, and through our guides on Privacy Compliance and Transparency for Consumers.

6. Inconsistency with principles of recently signed trade agreements

In the context of transborder data flows, the proposed re-interpretation is inconsistent with the principles of recently signed and/or soon to be ratified trade agreements, which offer unprecedented trade opportunities for Canadian businesses and prosperity for Canadian people. In this case, the imposition of consent requirements for data transfers could be regarded as a non-tariff barrier to trade that imposes restrictions greater than those required to achieve our common objective of reasonable privacy protection. This includes the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA), and the Canada-European Union (EU) Comprehensive Economic and Trade Agreement (CETA).

CPTPP features a commitment to allow transborder transfers of information by electronic means. The treaty limits restrictions on the open-border principle for data transfers, stipulating that any limitations may not be arbitrary, discriminatory or a disguised restriction on trade, and cannot be greater than those required to achieve a legitimate policy objective. The requirement for consent in this case would not fulfills its intended objective of greater privacy protection, given that transferred personal data would continue to be protected by the same measures as before, and asking for consent would result in no real or incremental improvement in privacy protection for the individual choosing to receive the service.

CETA has similar language to encourage the interoperability of privacy frameworks, indicating that all parties **"**shall take into due consideration international standards of data protection relevant of international organizations of which both Parties are a member".

USMCA stipulates that "no party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person." It also states that the parties shall "recognize the importance of … ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented". USMCA also requires countries to promote compatibility between their privacy frameworks, and to consider and recognize the principles and guidelines of relevant international bodies, including APEC and OECD. The proposed reinterpretation would operate against all of these principles, reducing compatibility and creating an unnecessary obstacle disproportionate to the risk presented.

Implementation Requirements

For all of the reasons noted above, consent should not be required for transfers for processing.

Recognizing the extraordinary implementation challenges that our members (private, public and not-for-profit organizations) will face if the OPC chooses to proceed with this new approach under PIPEDA, and the significant consequences to consumers, the change can be operationalized only if the following accommodations are made:

- **36-month transition period:** A change of this scope and magnitude will require time for organizations across Canada, and to some extent internationally, to understand and implement. If the OPC intends to proceed with the new interpretation, organizations will require a minimum of 36 months to retool their procedures and contractual relationships. This is particularly

important for Canada's SMEs. This timeframe is in line with other regulatory changes with significant operational implications. For example, when the Canadian Securities Administrators established rules known as "Client Relationship Model – Phase 2", or more commonly "CRM2" requiring firms to be more transparent with investors about their investment returns and fees, the industry was given 36 months to implement the changes.

- **Forward-looking implementation:** Given the myriad of difficulties associated with re-obtaining consent from individuals with regards to current service agreements, including the risk of service disruptions for critical services (e.g., cell phone access, banking) that Canadian consumers rely on, the guidance must be forward-looking only, i.e. organizations will not have to re-obtain consent in cases where consent has already been provided and is being relied upon.

For questions or comments regarding this submission, please contact:

Fiona Wilson
Director, Government Relations
fwilson@theCMA.ca
(416) 644 3748

The CMA appreciates the opportunity to participate in this important consultation.

Yours sincerely,

Sara Clodman
Vice-President, Public Affairs and Thought Leadership