Canadian Marketing Association Submission on

Emerging Issues: The Personal Information Protection Act

The Canadian Marketing Association (CMA) appreciates the opportunity presented by the Alberta Standing Committee on Resource Stewardship to provide comments on the discussion paper: Emerging Issues: The Personal Information Protection Act (the PIPA).

Albertans have never been more reliant on the digital economy. At home, it supports our daily lives and well-being. At work, it supports our ability to innovate, build businesses and remain competitive.

In today's digital world, consumers are demanding much greater speed and quality of information from private sector, public sector and not-for-profit organizations than ever before to help them identify relevant products and services and make informed purchase decisions. A strong majority (73%) of consumers are willing to share personal data to receive benefits, as long as their data is properly protected.

We are living in challenging economic times. Ninety percent of consumers say one of the most important reasons for sharing their data with companies is to receive product discounts. With more than 80% of Canadians concerned about the rising cost of living, the personalization that comes from data usage provides some relief through relevant offers and sales that save them time and money.

The Changing Legislative Landscape

It is extremely important for the PIPA to be harmonized with other Canadian privacy legislation to make it easier for businesses to operate effectively in Alberta, across the country, and globally. A lack of harmony between rules across the country results in confusion for consumers, creates an unnecessary complex compliance burden for business, and impacts interprovincial and global trade.

Alberta's current PIPA is well-harmonized with the federal legislation (the Personal Information Protection and Electronic documents Act or PIPEDA) and with the BC Personal Information Protection Act (the BC PIPA). This has served consumers and organizations well for many years.

Having substantially similar privacy laws across the country will help businesses reach and serve their customers effectively across international and provincial borders. This will enable Alberta businesses to compete on a level playing field, and ensure the province remains an attractive destination for direct foreign investment.

In particular, it is critical for Alberta's private sector privacy law to ensure reasonable alignment with emerging federal legislation (i.e., the Consumer Privacy Protection Act in Bill C-27). We caution that it is too early to assert what the final provisions of a new federal law would be, since Bill C-27 could see many changes through the parliamentary committee's extensive clause-by-clause review, and the potential for further changes if and when the bill reaches the Senate.

We vehemently oppose creating an Alberta law that fully aligns with the EU's General Data Protection Rule (the GDPR). It is extremely important for all Canadian privacy legislation to reflect and support local conditions, practices, and expectations, with the goal of achieving privacy protection that is equivalent to the GDPR without alignment to the EU's legislative approach.

While the GDPR has significantly moved the dial on data protection issues and awareness, there has been growing acknowledgement in recent years that its shortcomings have led to some significant

unintended consequences, including creating a staggering regulatory burden for both government and business[1].

In contrast, many features of existing privacy laws in Canada have stood the test of time, providing privacy protection without unnecessary regulatory burden.

In January of 2024, the European Commission announced that Canada's current federal law, PIPEDA, provides an adequate level of data protection, which allows data from the EU to continue to flow to Canada. While the EU staff report notes that data transfers from the EU are subject to PIPEDA, as opposed to provincial legislation, it also recognizes that Alberta's PIPA is deemed to be substantially similar to PIPEDA.

Artificial Intelligence

Consideration of a framework to regulate AI should **not** be incorporated into a review of PIPA but should be a separate deliberation that takes place when the proposed federal statute – the Artificial Intelligence and Data Act (AIDA) – is closer to becoming law. This will promote legal consistency, reduce regulatory complexity, enhance economic efficiency, and make it easier for consumers and organizations to understand their rights and obligations.

The Speaker in the federal House of Commons ruled in April 2023 that the proposed federal privacy law and AIDA did not have a common element and therefore, that AIDA could be voted on separately. This continues to be debated by MPs.

There is no public policy merit in combining the study of these laws in Alberta or any other jurisdiction.

Application of the Law to NFPs

We support continuation of the principle that PIPA should only apply to not-for-profits (NFPs) with respect to their commercial activities. As the Alberta discussion paper points out, this approach is reflected in the CPPA.

A one-size-fits-all application of PIPA could impose undue burdens on smaller non-profits with limited resources. The law should recognize the unique and essential contribution of not-for-profit organizations to the social fabric of our society. They provide essential programs and services, offer meaningful employment opportunities, and strengthen our social safety net by strengthening communities and mobilizing volunteers to serve the needs of Albertans that go beyond public and private sector initiatives.

These organizations need to reach and communicate with individuals in the communities that they serve, and they need to identify donors to fund their activities.

Privacy requirements that do not consider the impact on NFPs could prove debilitating in terms of the capital required and limitations on their ability to automate and optimize. NFPs lack ready access to legal advice and representation to navigate the complexities of overly prescriptive and unnecessarily restrictive legislation, making it more difficult for them to use data to innovate and succeed. Personal information used by NFPs in the course of these activities should not be captured by the Act if the information is anonymized and there is not a real risk of significant harm.

One of the weaknesses of the GDPR is that it does not effectively differentiate between issues of private sector and public sector privacy, and between low and high-risk applications and activities. The broad

[1] https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6

scope and level of prescriptiveness of the GDPR framework has resulted in fundamental flaws that lead to inefficiencies and unintended consequences.

Axel Voss, a Member of the EU Parliament (MEP) involved in the original drafting of the GDPR, launched a public consultation in 2021 about how the GDPR has impacted the daily lives of individuals and organizations. He received more than 180 replies detailing the negative impact of the GDPR on everyday life. What surprised him was that two-thirds of the responses came not from business but from "citizens, researchers, scientists, nurses, data protection officers, lawyers, non-profit associations, sport clubs and many more." In contrast, only one-third came from businesses and business associations.[2]

MEP Voss noted that the GDPR "does not differentiate between the processing of personal information by governments and by private individuals and organizations." He notes that the GDPR lacks a risk-based approach and fails to account for context and the varying scope and scale of data processing activities by organizations. Designating low-risk classes of data processing with separate bases for processing would reduce compliance burdens for organizations and regulators alike.

Protections of Sensitive Personal Information

It is well-established in Canadian law that sensitive information is protected by additional safeguards. Sensitive information typically includes data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, sexual orientation, genetic data, and biometric data.

It should be recognized, however, that any kind of personal information can be considered sensitive – or not – depending on the context in which it is used. As a result, the law should allow businesses to operationalize appropriate data protection and privacy measures by considering the nature of their enterprise, the type of personal information collected, and its intended use.

Biometric Information

The responsible, secure use of biometric data provides many advantages for Canadian consumers and organizations, including enhanced security, accuracy, cost reduction, relevance, and convenience.

Recent research has revealed that, as technology evolves, consumers demand much greater speed and quality of information so that they can readily access relevant products and services, benefit from offers and make informed purchase decisions. In the marketing sector, biometric data, used responsibly, can help marketers reach and serve consumers in the personalized and unique ways that they expect – including serving them with ads at ideal moments and in more meaningful ways.

We support the development of thoughtful regulatory guidance in this area so that consumers and companies can realize the advantages while preventing the misuse of biometric data by unscrupulous players. To ensure that biometric data is used responsibly for purposes that support consumers' interests and needs, the guidance must incorporate a spectrum of risk. For example, it should take into account the following factors:

- Whether data is obtained for a temporary use (i.e., monitoring) versus kept and re-used.
- When de-identified data is used only in a closed ecosystem, which poses much less identifiability risk than it would, however small the risk might be, if it was used openly.

[2] Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.2.

The guidance must also include a contextual approach to determining appropriate purpose by adopting a four-part test that has served organizations and consumers well through PIPEDA and PIPA for more than two decades. This entails requiring organizations to assess sensitivity, effectiveness, proportionality, and necessity.

Many consumers have reasonable and valid reasons to consent to the use of biometrics to experience more convenience, and more tailored communications and advertising.

Not all biometrics are used to identify or confirm the identity of an individual. The definition of biometrics in guidance should incorporate the concept of unique identification. This would align the guidance with PIPEDA's longstanding and effective risk-based, proportionate, and principled approach.

The Protection of Children's Personal Information

The CMA unequivocally supports the protection of minors' data. We have been a leader in setting standards for marketing to children and youth for decades, through our Canadian Marketing Code of Ethics & Standards.

The protection of minors' data is an important issue that warrants specific and special treatment. It needs to address real harms, and not lead to the overcollection of data.

Specifically, organizations that have no need to know whether their customers are minors should not be required to collect and retain the birth date – which is highly sensitive information – of every consumer that they interact with, for the sole purpose of determining whether the person is a minor.

Rather, provisions related to minors' data should apply to organizations whose business is directed to minors, and to organizations who know, or should know, that they are processing the personal information of minors.

We also recommend that the law allow for different treatment of mature minors, who bear many of the responsibilities and enjoy many of the privileges of adults (such as applying online for post-secondary education and jobs, driving a vehicle, voting in elections, and being tried as an adult). These recommendations align with laws in the US and the EU.

The Canadian Marketing Code of Ethics and Standards provides organizations with clear guidance on appropriate business practices when marketing to these demographic groups.

Consent Requirements

PIPA's current provisions on consent are generally appropriate. We agree that "consent should be meaningful, while at the same time reducing the consent burden and enabling greater use of data by private and public sector entities."

It is well documented that, since the introduction of the GDPR, with its stringent consent and transparency requirements, EU consumers are suffering from increased "consent fatigue", causing them to be less likely to carefully review notices and make informed decisions. With the introduction of the GDPR, notices to consumers have become even more frequent and complex, resulting in consumers being even less likely to read them.

Researchers have discovered that "...the more information individuals have access to about what happens to their (personal) data, the less information they are able to filter, process, and weigh to make

decisions that are in line with their own privacy preferences."[3] It may also deter them from using a certain website or service altogether.[4]

Therefore, consent should only be required for actions that a reasonable person would not expect or that carry a risk of harm.

The CMA Guide to Transparency for Consumers provides a transparency framework that specifies the information consumers want to know about how their personal information is collected, used and shared, and proposes how to communicate this to consumers in a more user-friendly, easily digestible manner. The key is not to provide more information, but to provide better information that is clear and concise, and tailored to what the consumer needs to know at various stages of their journey with the organization in order to make informed decisions. The CMA Guide to Transparency for Consumers helps organizations tailor their privacy policy and practices to suit their sector, business model, consumers' preferences, and products/services.

To serve consumers better and to adopt this tailored approach, organizations should continue to have the ability to choose between express or implied consent based on context and the sensitivity of the data. Express consent should be reserved for sensitive information and activities outside the reasonable expectations of individuals. PIPA could include exceptions for legitimate business purposes, further specified through Regulations.

We agree that the purpose for collecting the information should be clearly specified, and that companies should transparently identify purposes in a granular format. However, it is impractical to expect organizations, customers, and employees to work through such a cumbersome and repetitive consent process.

However, organizations, should not be required to collect consents for the same purpose repeatedly, particularly if the use or disclosures is necessary for providing the business service. As such, organizations should be permitted to collect a single consent for multiple purposes if those purposes are related and if doing so is not misleading.

For example, a company may choose to group purposes thematically (e.g., those critical to the delivery of the product or service requested, for fraud purposes, for analytics, for communications with the customer (personalized marketing), for consultation purposes and surveys etc.). Organizations should consider the best approach in the circumstances to enhance consumer understanding, focusing the requirement for granularity more on secondary purposes or on situations where individuals have a meaningful choice.

The creation of a patchwork of consents, with individuals consenting to some elements but not others, would create an unduly complex environment for both organizations and consumers, and fails to recognize that purposes are often interconnected.

Individual Rights that are not Included Under PIPA

The consultation paper seeks feedback on establishing consumer rights in three areas:

1. the right to erasure, including de-indexing from an online search,
2. data portability, and
3. the right to know the logic behind automated decisions that relate to the individual.

[3] https://link.springer.com/content/pdf/10.1007/s10603-018-9399-7.pdf
[4] https://link.springer.com/content/pdf/10.1007/s10603-018-9399-7.pdf

The right to erasure should not be permitted for frivolous reasons, but only for a valid purpose and should not apply to data that has been deidentified or anonymized. The right of erasure should also not be unlimited. It must be subject to stringent but reasonable exceptions set out in Regulations.

Data portability introduces significant new risks in relation to fraud, privacy, and security, and its overall consequences on the economy and competition require thorough examination. It is much safer for consumers to provide their information directly to a new company, rather than having it transferred from one company to another. Additionally, it should be limited to personal information provided by the individual and not information created or inferred from that information by the organization.

Providing individuals with the logic involved in automated decision-making about them must be based on a definition of an automated decision-making system (ADS) that focuses solely on decisions that are fully automated and should be limited to decisions that are likely to have a “significant impact” on them. Otherwise, the requirements would overwhelm consumers and disincentive organizations from developing and leveraging automated or partially automated systems, impacting Alberta’s position as a global leader in automation.

An ADS that “assists” the judgment of human decision-makers is fundamentally different from automated decisions, in that they are still subject to human decision-making. Moreover, automated systems that assist human decision-making are not conceptually different from various written policies, job aids and other instructions which are currently used within organizations to assist humans in making consistent decisions in line with corporate policy objectives. To the knowledge of the CMA, enhanced transparency requirements for these existing practices has never even been considered. There is similarly no need to impose transparency requirements on such guidance to human decision-makers when it originates from a coded solution.

An overly broad definition would require the provision of information to consumers that is not meaningful, and place a significant administrative burden on organizations, without contributing to effective privacy protection. It would also create a potential burden for companies dealing with large volumes of requests (including potentially automated requests), without a corresponding privacy benefit for individuals.

In this regard, automated decisions include a broad range of routine micro-decisions, the majority of which will have no significant impact on an individual or potential to harm them (such as a call centre using AI to support call routing, or a website declining to serve copyright-protected content to a user resident in a jurisdiction for which the website provider does not hold the rights to make that content available). The fact is that not all ADS rely on complex algorithms that factor in an array of personal information; many are driven by one or two data points, and are heuristic, rather than algorithmic.

Safeguarding Personal Information

Leveraging de-identified and anonymized data is one of the most privacy-protective mechanisms on which organizations rely to innovate and provide value to consumers. It is critical for Alberta organizations to not be overly restricted in their use of de-identified and anonymized data, so that they can compete effectively through the use of important data-driven technologies and services.

The definition of the term “anonymize” must incorporate the notion of foreseeable risk of reidentification and enable adherence to “generally accepted best practices,” as it sets a statutory obligation for organizations to consider the evolving de-identification techniques and standards that would sufficiently protect personal information with respect to their unique sector and context.

We support the principle that organizations should have privacy management programs tailored to their

specific business activities and the nature of personal information they handle. Requirements should be principles-based and not create onerous prescriptive requirements that create an administrative burden for organizations – particularly SMEs for whom the costs could be crippling – and enormous complexity for regulators, as in the case of the GDPR. Approximately two-thirds (21) of European countries surveyed by the European Data Protection Board (EDPB) stated that regulatory bodies do not have enough human, financial, and technical resources to effectively regulate the full set of requirements of the GDPR.[5]

Privacy impact assessments can help an organization determine the degree of risk that their data activities pose so that the measures that are implemented are proportional to that risk. This ensures that all organizations, regardless of size, can comply appropriately. It supports innovation and efficiency while ensuring robust privacy measures. Submitting all privacy impact assessments to the Commissioner is unnecessary but in the case of an investigation, the assessment should be shared.

Breach Notification

We support changes to the breach reporting process announced by the Office of the Information and Privacy Commissioner in April. The revised process recognizes organizations who act responsibly by proactively notifying individuals in the case of a breach where a real risk of significant harm exists.

Noting that the individuals affected by a breach will all be notified, it is not necessarily in the public interest to publicize breaches. In fact, in some cases, disclosing details could harm the public interest by encouraging similar breaches. For example, widely publicizing a still-open vulnerability, or underlining a potential use or value to hacked PI that might not be widely known could attract copycats. This would align with breach notifications under PIPEDA.

For these reasons, breaches should only be disclosed when the Commissioner believes it is in the public interest to do so.

Administrative Monetary Penalties

We support the use of administrative monetary penalties (AMPs) to address “serious, repetitive, or long-term contraventions and to reinforce that individuals’ privacy rights are protected and enforced,” as described in the consultation paper. The vast majority of reputable Canadian organizations are committed to protecting consumers’ personal information. They work hard to gain the trust of their customers and part of that is a strong privacy commitment. A strong enforcement regime is important to deter bad actors.

The calculation of fines should be proportionate, considering the nature and impact of the violation, whether it was intentional or inadvertent, and the size and data processing activities of the organization. Excessive fines could deter businesses from operating in Alberta, especially if Alberta is a small part of their overall market.

When an investigation involves more than one regulator and a decision is made to impose AMPs, there should be coordination amongst regulators to prevent double – or even quadruple jeopardy – such that multiple amps are not imposed for the same offense.

[5] Contribution of the EDPB to the evaluation of the GDPR under Article 97, EDPB, 2020.

About the Canadian Marketing Association

The CMA is the voice of the marketing profession, representing corporate, not-for-profit, public, and post-secondary organizations across Canada. We help marketers and their organizations maintain high standards of conduct and transparency through our Canadian Marketing Code of Ethics & Standards, our extensive resources on privacy law and best practice, including a Guide on Transparency for Consumers, and our training and professional development programs, including our Privacy Essentials for Marketers course and the Chartered Marketer (CM) professional designation. Our Consumer Centre helps Canadians understand their privacy rights and obligations, and we respond to marketing-related enquiries from consumers and organizations