

Submission to the Standing Committee on Industry and Technology by the Canadian Marketing Association on the proposed Consumer Privacy Protection Act contained in Bill C-27

October 2023



Table of Contents

| EXECUTIVE SUMMARY | 3 |
|--------------------------------------------------------------------------------------------------|----|
| INTRODUCTION AND CONTEXT | 5 |
| PRIVACY LAW REFORM CANNOT WAIT | 6 |
| THE CPPA WOULD POSITION CANADA AS A GLOBAL LEADER IN PROTECTING PRIVACY AND FOSTERING INNOVATION | 6 |
| PROPOSED AMENDMENTS | 10 |
| A. MINORS' DATA | 10 |
| B. CONSENT AND EXCEPTIONS TO CONSENT | 14 |
| C. AUTOMATED DECISION SYSTEMS | 17 |
| D. DE-IDENTIFIED AND ANONYMIZED DATA | 20 |
| E. TRANSITION PERIOD | 20 |
| APPENDIX: TABLE OF PROPOSED AMENDMENTS | 23 |



Executive Summary

Canadians 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.

As technology continues to advance, so have people's attitudes towards sharing their information. Canadian consumers increasingly understand that data exchange with business is essential to the running of modern society.

The companies fueling our economy need clear and consistent privacy rules to use data safely and effectively to provide consumers with the products and services they need and expect. Responsible use of data to personalize experiences is key to providing value and cost-savings to consumers, and to delivering on their increasingly sophisticated expectations. With more than 80% of Canadians concerned about rising everyday costs, the personalization that comes from data usage provides some relief through relevant offers and sales that save customers time and money.

The Canadian Marketing Association (CMA) urges the Standing Committee on Industry and Technology to adopt the proposed Consumer Privacy Protection Act (CPPA) – with targeted amendments – in order to modernize consumer privacy protections and to ensure Canada maintains a competitive economic position in the global digital economy.

The CPPA would preserve Canada's principles-based and technology-neutral approach to privacy, which would ensure that the law continues to apply to rapidly evolving technologies, business models and consumer expectations for decades to come.

The CPPA would protect consumers and ensure that their personal information is safe. It would give them important new rights to have more meaningful control over their data and require companies to be more transparent about their use of personal information – backed by the strongest financial penalties in the G7.

Limited amendments are required to avoid unintended consequences and achieve the core objectives of the bill:

- A. The CPPA's blanket approach to **the personal information of minors** (which deems it as sensitive in all cases and all contexts) would result in organizations collecting and retaining a significant amount of additional information about individuals well beyond what would reasonably be required for business purposes –simply for the purpose of verifying age to ensure compliance with the new law. A more targeted approach that is less intrusive and consistent with other major jurisdictions would avoid the overcollection of information and the potential risks that could result.
- B. The following changes to the bill's **consent provisions** are required to ensure a meaningful consent model and to combat consent fatigue:
 - The exceptions to consent (for 'business activities' and 'legitimate interests') must exclude only activities that a reasonable person would not expect a business to undertake or that would expose them to harm. Legitimate business activities that have no significant impact on the individual, including routine R&D activities that help organizations better understand and serve their customers, should not require consent.
 - The provision prohibiting implied consent where one of the above exceptions to consent is available should be removed, as it prohibits organizations from taking a more careful approach in cases where it is not clear whether a full exception to consent applies.



- In order to rely on the 'legitimate interests' exception to consent, organizations should be required to consider the potential adverse effects on an individual that are 'reasonably foreseeable', rather than those that are remote or unlikely.
- C. The requirement that organizations provide more transparency about **automated decision systems (ADS)** that make predictions, recommendations or decisions about individuals must be based on a definition of ADS that focuses solely on decisions that are fully automated., Further, the obligation to explain at an individual's request should be focused on decisions that are <u>likely</u> to have a "significant impact" on them. Without these amendments, the bill's requirements would overwhelm consumers and disincentive organizations from developing and leveraging automated or partially automated systems, impacting Canada's position as a global leader in automation.
- D. The bill should incorporate the amendments put forward by the Canadian Anonymization Network (CANON) to ensure **policy standards for de-identified and anonymized data** enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks
- E. The **law should come into force in a staged manner over three years**, so that Canadian organizations have adequate time to implement the required substantial changes to compliance plans, IT systems, business processes and staff training.

Reforming the federal legislative framework for privacy cannot wait, particularly in light of the need to provide organizations with time to prepare for their new obligations, including systems changes and staff training, before the new law comes into force. Further delay will put Canadian businesses and Canadians at risk. A patchwork of privacy rules across several provinces will fill the vacuum, resulting in confusion and complexity for consumers and businesses.

With new national standards, Canadian businesses operating across provincial and global borders would have coherent and consistent privacy rules. This includes sufficient alignment with the General Data Protection Regulation (GDPR) and its UK equivalent, so we can continue to effectively receive and process data from the EU and the UK – two of our largest trading partners.

We urge Parliamentarians to advance Bill C-27 for the benefit of Canadians and the economy on which they rely.



Introduction and Context

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.

Marketing – the link between organizations and their customers – is a key economic driver for Canada. It stimulates consumer demand, supports business expansion, generates substantial direct and indirect employment for Canadians across all key sectors and industries, and spurs government revenues.

Marketing is much more than advertising. It is the process of determining consumer needs and interests; tailoring and augmenting products and services to meet those needs and interests; identifying and reaching consumers who may be interested in those products or services; providing them with value to meet their needs and wants; and building a trusting relationship.

The loyalty and trust of customers is the foundation for business success. Most Canadian organizations recognize that having strong privacy and data protection practices provides a business with a competitive advantage, also helping to bolster customer retention. More than 92% of Canadian businesses consider the protection of customers' personal information to be important to their business. CMA member organizations work hard to protect and respect the privacy interests of the individuals they serve.

Modern economies are predicated on the exchange of personal information. When individuals provide personal information to an organization in connection with the purchase of goods or services, they reasonably expect the organization to use the information to serve them better. Consumers are demanding much greater speed and quality of information so that they can identify and access services provided by companies and make informed purchase decisions. Research has confirmed this shift in consumer expectations, with a substantial 71% of consumers now anticipating personalized interactions from companies. A staggering 76% of them express frustration when they don't receive this level of personalized attention.²

Responsible use of data to personalize experiences is key to providing value and cost-savings to consumers and to delivering on their increasingly sophisticated expectations in a fast-paced world. Personalization also plays a role in addressing the concerns of more than 80% of Canadians about rising everyday costs³, providing them with discounts and offers on products and services that are relevant to them and saving them time and money. Surveys show that one of the most popular reasons for data-sharing with companies, cited by 90% of consumers, is to receive discounts on products. This could be in the form of an email sign-up, with many e-commerce sites offering an immediate discount in return for a newsletter sign-up.⁴

Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) was the international gold standard for the protection of personal information before the implementation of laws in other jurisdictions over the past five years raised the bar even higher. PIPEDA has served Canadians well for

¹ <u>2021-22 Survey of Canadian businesses on privacy-related issues</u>, Office of the Privacy Commissioner of Canada, 2022.

² The value of getting personalization right—or wrong—is multiplying, MicKinsey, 2021.

³ Despite Softening Inflation, Canadians' Affordability Concerns Remain Acute, Ipsos, 2023.

⁴ Personalized marketing: Brands and e-commerce retailers, Smart Insights, 2020.



more than two decades, but needs to be updated to provide more meaningful privacy protection in the digital age.

Canadian policymakers must ensure that any new law is not simply imported from another jurisdiction, but rather, that it reflects and supports local conditions, practices and expectations. Moreover, Canada has an opportunity to learn from the experiences of other jurisdictions, borrowing from their successes while avoiding their missteps.⁵

To reflect the critical importance of data to our economy, it is urgent to update Canada's private sector privacy law so that consumers have updated protections, and so that the businesses – including small and medium-sized enterprises (SMEs) – that are fueling our economy have clear and consistent privacy rules.

We urge the Standing Committee on Industry and Technology to adopt the CPPA – with targeted amendments in a few key areas – to modernize privacy protections for consumers and to ensure that Canadian businesses can leverage data to secure a competitive economic position in the global digital economy.

Privacy law reform cannot wait

Canada's private sector privacy law, PIPEDA, pre-dates the digital era. Consumers deserve modernized protections and rights, and businesses require more regulatory certainty. A delay in adopting the CPPA would encourage a patchwork of privacy legislation across the country, as provinces move to enact or reform their own private sector privacy laws to fill the gaps, potentially resulting in varying standards. This would create confusion for consumers and burdensome compliance for businesses – including crippling demands on SMEs. It would also complicate conditions for trade and reduce Canada's attractiveness as a nation in which to invest and do business.

We need an updated law to ensure Canada's renewed adequacy status under the European Union's General Data Protection Regulation (GDPR) and its UK equivalent, so that we can effectively receive and process data from the UK and the member states of the EU, which represent significant sources of trade for Canada. This is critically important for Canadian businesses – including SMEs – that need access to international markets to grow and compete in the global innovation race.

The CPPA would position Canada as a global leader in protecting privacy and fostering innovation

The CPPA, as currently written, has a dual-purpose statement, which is to: "govern the protection of personal information of individuals while taking into account the need of organizations to collect, use or disclose personal information in the course of commercial activities." This builds on the strengths of PIPEDA, which has been guided by the dual objective of protecting consumer privacy and enabling responsible data use and innovation since its enactment in 2001.

The CPPA's purpose statement reflects the need for Canada's private sector privacy law to continue to achieve two essential priorities: providing effective privacy protection for consumers and enabling Canadians to benefit from the enormous social and economic benefits of data use. These two priorities can and must be achieved in harmony.

_

⁵ Privacv Law Pitfalls – Lessons Learned from the European Union, Canadian Marketing Association, 2022.



Recognizing these two essential priorities in no way detracts from the importance of an individual's unquestionable rights of privacy. Indeed, the CMA supports the recognition of a fundamental right to privacy in the preamble to the bill.

The CPPA preserves Canada's principles-based and technology-neutral approach to privacy, which acknowledges the varying capacities and sizes of Canadian organizations and ensures that the law would remain resilient in the face of rapidly evolving technologies, business models and consumer expectations.

It reflects an understanding that in Canada, there are – and should continue to be – separate public and private sector privacy laws, reflecting the vastly different nature of the relationship between an individual and the state, and the relationship between an individual and a private sector organization. These different contexts demand different legislative approaches, which is why it is appropriate that the CPPA departs in some respects from the approaches taken in other jurisdictions that govern both public and private sector activities.

A notable example is the European Union's GDPR. The CMA report <u>Privacy Law Pitfalls – Lessons Learned from the European Union</u> compiles a growing body of research and commentary, including from some of the law's original drafters, that calls out weaknesses in the GDPR stemming from its overly prescriptive and complex provisions.

These pitfalls have led to several unintended consequences that Canada must strive to avoid with respect to its own privacy law reform, including:

- Undue complexity and consent fatigue for consumers,
- A staggering regulatory burden and cost for government and regulators,
- Stifled innovation and crippling compliance costs and hurdles for SMEs, and
- Obstruction of cross-border business and data flows.

In the past year (since the report was published), an additional 20 critical studies of the GDPR have found that:

- European businesses subject to the law saw their profits shrink by an average of 8.1% in response to the enforcement of the GDPR in 2018, with the main burden falling on SMEs, who experienced an average decline in profits of 8.5%. In the IT sector, profits of small firms fell by 12.5% on average.⁶
- The GDPR hurt small app developers, and contributed to fewer apps getting to market.⁷
- Consumer personal data processing has become more concentrated and the increase in concentration is highest among the web technology vendors that process personal data.⁸
- The lack of growth of EU-based digital enterprise since the introduction of the GDPR is concerning: For example, three years after the introduction of the GDPR, Europe's share of the platform economy was modest at 3%, on track to be eclipsed by Africa.⁹
- A massive 72% of consumers say that they feel annoyed about the number of times they must accept cookies to access content. Many organizations, in a bid to ensure compliance, ask their customers for consent multiple times, across multiple different touchpoints.¹⁰

⁶ Privacy Regulation and Firm Performance, University of Oxford, 2022.

⁷ GDPR and the Lost Generation of Innovative Apps, National Bureau of Economic Research, 2022.

⁸ Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR, Social Science Research Network, 2022.

⁹ New Model Code for Personal Data Protection Is Better Than GDPR, Forbes, 2022.

¹⁰ Consent Fatique, The Data Privacy Group, 2022.



Based on these and other learnings from the GDPR, UK regulators, through the 2023 Data Protection and Digital Information Bill, are rethinking some elements of the law in order to reflect practical realities for consumers and organizations.

One of the most significant of the UK reforms is the greater clarity offered on what constitutes a "legitimate interest", which is another legal means for processing data under the EU law besides consent.

The reforms clarify that finding and retaining customers and donors is essential to a business or charity. It is not possible to operate a business without reaching out to customers. Direct marketing is therefore considered essential to the right to conduct a business and "legitimate interest" may be used as a basis for processing for marketing purposes.

This supports the spirit of Recital 4 of the GDPR, which indicates that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

Canadian policymakers must ensure that any new law reflects and supports local conditions, practices and expectations. The CMA report, <u>Canada's Privacy Law Priorities</u>, outlines how the proposed CPPA takes a made-in-Canada approach that learns from the experience of other jurisdictions, and takes into account the following key realities for Canada:

- The unique nature of Canada's trade and SME-dependant economy: Global trade makes up about two-thirds of Canada's GDP. Privacy law must not unduly restrict the cross-border data transfers that underpin global trade, fueling cross-border business activities and global supply chains, and providing Canadian businesses with access to the world.
 - SMEs make up 98% of businesses in Canada. Privacy requirements that are designed without regard for the resulting burden they impose on SMEs could prove debilitating in terms of the capital required and limitations on the ability of these organizations to automate and optimize.
- Consumers' growing expectations: Consumers increasingly expect organizations to intuitively
 deliver the products and services that they want and need. Research points to a notable decline
 in overall levels of online privacy concerns among Canadians, with 43% of Canadian consumers
 agreeing that data exchange with business is essential to the running of modern society—rising
 significantly from 35% who agreed with this statement in 2018.¹¹

In recent research, only 5% of Canadians indicated that they are concerned about having information that they share with a business/organization used to target ads and offers to them by that business/organization. More than 70% say they lose trust in a company when it sends them information about products and services that don't interest them.¹²

Research in Europe found that people ultimately want experiences that feel valuable to them as individuals. Overall, consumers are more comfortable sharing their data when they understand how they are benefiting. With regards to online advertising, the study found that people's attitudes towards online privacy shift based on the perceived value of an ad. People find ads valuable when they are tailored to their interests, lead to time savings or cost savings, and are brought to their attention at the right moment.

More than half of Canadians believe that with all the technology available today, it is unacceptable for a business/organization to send them ads that are not relevant to them.¹³

_

¹¹ Global Data Privacy: What the Consumer Really Thinks, GDMA, 2022.

¹² Consumer Privacy Research Findings, Sago, October 2023. I.

¹³ Ibid.



Furthermore, more than 80% of consumers are bothered when an organization sends them irrelevant information.14

The critical role of data use: Canadian investment in data grew more than 400% from 2005 to 2019. Data-related assets in Canada were worth \$217 billion in 2018—equivalent to more than two-thirds the value of the country's crude oil reserves.

For consumers, data use enables them to receive the relevant products, services and information that they expect, as outlined above. For businesses, first and foremost, data helps them to find and serve their customers more effectively, which contributes to a trusted relationship. Data analysis informs operational strategies, improves business competitiveness, drives technological advancement and increases profitability, stimulating the economy and supporting job creation across all Canadian sectors.

Data use helps businesses serve their customers more meaningfully. By leveraging data, analytics and technology, marketers can deliver tailored and relevant interactions to a wide audience through personalization at scale.

Customers reward companies that effectively meet their needs. Companies that excel at personalization generate 40% more revenue from those activities than average players. contributing significantly to the economy. 15 Organizations that have fully reoriented operations, delivery models and technology investment to meet new customer experience demands grow their year-over-year profitability by at least six times their industry peers. 16

The realities of technological advancement: Innovation is a principal driver of productivity growth and national prosperity for Canada. An overly prescriptive privacy framework would impede important new technologies and services, pushing emerging technologies—and the innovation they enable—to other jurisdictions. The CPPA avoids incorporating several of the GDPR's prescriptive rules and concepts, which are incompatible with many new technological developments.

Consumers are generally receptive to reasonable data usage by organizations that act responsibly. Canadians have indicated that increasing fines for companies that do not follow the rules (65%) and increasing requirements for plain and clear information so they can better understand how their data is being handled (61%) would increase their comfort with data sharing.¹⁷

The CPPA would effectively address these issues, while setting a new global gold standard for consumer privacy protection. It proposes strong and modernized protections, including a suite of new and augmented consumer rights, greater transparency and accountability requirements for organizations, and the strongest financial penalties in the G7.

If passed with the targeted amendments set out below, the CPPA would achieve Canada's privacy law priorities. It would strengthen privacy protections for consumers while recognizing the legitimate use of personal information by business for innovation and improving the lives of Canadians.

¹⁴ Ibid.

¹⁵ The value of getting personalization right—or wrong—is multiplying, McKinsey, 2021.

¹⁶ The Journey to Operations Maturity, Accenture, 2021.

¹⁷ *Ibid.*



Proposed Amendments

The following amendments are needed to ensure that the policy intent of the proposed CPPA is achieved without unintended consequences for consumers and organizations.

A. Minors' Data

Rather than the proposed one-line approach to the protection of minors' data that characterizes all such data as sensitive, a more targeted approach should be taken that requires organizations that know (or ought to know) that they are processing the personal information of minors to consider the needs and capabilities of minors, including mature minors, with respect to specific sections of the Act.

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, not only through privacy law, but also through online harms legislation, and opportunities for new industry codes and certifications.

We support the government's <u>proposal</u> to amend the preamble to recognize that the personal information of minors actively engaged with the digital and data-driven economy is worthy of stronger protection given their varying levels of capacity to understand how it is used by organizations and the potential long-term implications of such use. We further support the government's proposal to amend Section 12. However, for the reasons outlined below, we suggest that it instead be amended to require consideration of the sensitivity of the personal information, including by reason of being in relation to a minor, taking into account the needs and capabilities of mature minors.

Implementing the broad approach in subsection 2(2) of the CPPA would result in many unintended and undesirable consequences that are contrary to the objective of protecting minors' data, and may result in the routine collection of sensitive data from adults. Specifically, subsection 2(2) of the proposed CPPA deems **all** personal information respecting minors (i.e., those under the age of majority in their province of residence) to be sensitive, regardless of the age or capacity of the minor, the nature or inherent sensitivity of the personal information itself, or any potential risk of harm related to the collection, use or disclosure of the personal information in question. There are sweeping implications to this presumption of sensitivity, triggering several obligations throughout the bill reserved for sensitive categories of data such as health data. Sensitive personal information is generally subject to enhanced privacy protections, suggesting, among other things, enhanced transparency and consent obligations, more stringent security safeguards and more restrictive retention periods,

The requirement to treat all minors' information differently from other personal information in all cases and for all business purposes, regardless of the risk of harm or the maturity of the minor, is too blunt of an approach for such an important and nuanced issue, and would lead to significant unintended consequences.

There are two main issues with the approach in the bill that must be addressed: avoiding the unnecessary overcollection of sensitive data from minors and their parents/guardians, and recognizing the material differences between young minors and mature minors. The sections below elaborate on these issues, and propose amendments to address them.



Avoiding the overcollection of minors' data

Obligations related to minors' data under the CPPA should be targeted to organizations whose business is directed to minors, and to organizations who know, or should be deemed to know, that they are processing the personal information of minors. This is consistent with the approach taken by the Children's Online Privacy Protection Act in the US,¹⁸ as well as by privacy laws in California¹⁹ and the EU,²⁰ and would avoid targeting organizations that may only incidentally and unknowingly process the data of minors.

If enhanced regulatory obligations are not focused on organizations whose business is directed to minors, or who know, or should be deemed to know, that they are processing the personal information of minors, then many organizations would feel compelled to take steps to verify the age of their customers/users in order to ensure compliance with the enhanced data handling requirements for the personal information of minors. The personal information required to verify age can be among the most sensitive (e.g., government-issued ID with birthdate). It carries the greatest adverse risk in the event of a breach, and is most sought after by criminals. Moreover, organizations would feel compelled not only to collect such sensitive data; but also to retain it in order to demonstrate compliance in the event of a complaint or investigation by the Office of the Privacy Commissioner (OPC). Such retention would increase unauthorized access and disclosure risks for both the affected individuals and the organization concerned.

The collection and retention of age verification data solely to comply with overly broad legislative language would run counter to the principle of data minimization: one of the foundational pillars of the CPPA, PIPEDA and global privacy and data protection laws. Most consumers recognize that they have at least partial responsibility for protecting their data and according to research, the approach most preferred by consumers is to limit the amount of personal information that they share.²¹ In the absence of our proposed amendment, organizations that do not target minors, or whose businesses are not known to attract large numbers of minors, will collect and retain personal information on **all** customers/users for no other reason than to confirm whether they are minors. Given the serious risks of harm associated with unauthorized access to such personal information, this may be a case where the cure is worse than the disease.

Much of the public discourse relating to the protection of the privacy of minors relates to social media platforms; however, the wording of the CPPA applies to businesses of all kinds, and even to the most innocuous information. Many organizations have no knowledge about whether a particular customer is a minor, nor do they need to know or have a strong privacy rationale to bucket the data differently. For example, neither a pizza delivery business (which would collect, names, telephone numbers and delivery addresses) nor the website of a general interest business like a local newspaper or a manufacturer of musical instruments (which may place cookies for analytics and advertising purposes, or may collect email addresses from those wishing to sign up to receive a newsletter or product updates) has a need to

¹⁸ See <u>Children's Online Privacy Protection Rule</u>, <u>16 CFR Part 312</u>. COPPA applies only to operators of websites and online services that are directed to children, or that have actual knowledge that they are collecting or maintaining the personal information of a child.

¹⁹ The <u>California Consumer Privacy Act of 2018, California Civil Code § 1798.120</u>, requires consent for the sale of the personal information of consumers under 16 years of age (including parental consent, for children under the age of 13). These restrictions apply only on business with actual knowledge that they sell the personal information of consumers under the age of 16, or that wilfully disregard the age of a consumer.

²⁰ Article 8 of the <u>General Data Protection Regulation (Regulation (EU) 2016/679)</u> requires parental consent for the processing of the personal information of a minor under 16 years of age, with respect to the offering of information society services directly to a child.

²¹ Consumer Privacy Research Findings, Sago, October 2023.



know whether its users/customers are minors; nor, arguably, is there any public policy reason to treat this type of information any differently where it happens to relate to a minor.

In the case of a telco, the company has no way of knowing whether any of the phones purchased by an adult as part of a family plan will be used by minors or, which family member will be using which phone, and the company has no way of distinguishing minors' data versus other data. All personal data is protected in accordance with privacy law, and within the context and reasonable expectations of users, regardless of age. To comply with the proposed CPPA, the company would potentially have to collect a series of names and birthdates and government-issued identification documents for the purpose of verifying the information) to determine which phone was going to be used by which family member, potentially creating separate service configurations, routing and storage for data generated through the use of those phones. This represents a significantly greater collection of personal information – included highly sensitive information – than would be required for the company's own business purposes. The necessity to collect and retain such sensitive personal information would also introduce substantial – and potentially unworkable – business costs and complexity, without a strong privacy rationale or apparent enhancement of privacy protection for the minors that may incidentally use the service.

Subsection 2(2) could result in many businesses adding an age-gate to their websites, even in cases where it may otherwise not be appropriate or necessary, 22 resulting in even more notices to consumers, without contributing in any meaningful way to the privacy of minors. Significant research in the EU has indicated that excessive privacy notices offload too much responsibility on the consumer and result in widespread consent fatigue without meaningfully enhancing privacy understanding and awareness. This is why the UK Government's 2023 data privacy reforms include an expanded range of exemptions to consent for cookies to reduce the onslaught of cookie consent banners.

Subsection 2(2) would result in significant challenges for businesses with respect to their existing customers, as they may feel compelled to canvass them for their birthdate in order to determine whose personal information need be treated as sensitive, and when it will no longer required to be treated as sensitive (i.e., when the customer reaches the age of majority). Faced with an uncertain regulatory risk, a business might feel it necessary to end services and offerings for customers who do not provide birthdates or ID, and this could inadvertently exclude seniors and vulnerable populations from access to important products and service.

In extreme cases, where the business complexity, implementation costs and potential regulatory risk outweigh any perceived benefit of providing products and services to consumers that happen to be minors, some businesses may decide not to service minors altogether. Given that minors could be old as 18 in some provinces, this could have a particularly negative impact on the offerings available for mature minors, who otherwise have many of the rights and obligations of adults.

As an example, professional sports leagues and teams generally maintain websites intended to drive fan loyalty and to generally promote the league/team. These sites generally include biographical information about players, player and team stats, team schedules, video highlights and online stores. Additionally, they often collect browsing related information (through cookies and related analytics technologies) and allow fans to sign up for additional content and promotional material through email. The league/teams are promoting their brand and services generally (rather than targeting minors). They collect and use fairly innocuous, non-sensitive data, and have no need or interest in knowing which of their visitors or addressees may be minors. Nor, arguably, is there any public policy rationale in such a circumstance for treating any differently the personal information of fans who happen to be minors. Faced with the technical challenges, new costs and increased regulatory exposure of handling minor's data, a league/team may elect to direct its site exclusively to users that have attained the age of majority,

²² For example, while age gates are common with respect to sites promoting age-restricted products like tobacco or alcohol, they are not considered to be necessary for the website of a retailer or restaurant.



erecting an age gate to verify user age and deny access to minors. This would be an unfortunate unintended outcome of legislation that is intended to protect the privacy of minors.

To meaningfully protect minors without creating these significant unintended consequences, we propose a more practical and targeted approach, where organizations:

- 1) whose business is directed to minors, or that offer a product or service directed to minors, or;
- that have actual knowledge that they are collecting or processing personal information from a minor (or based on the circumstances, should be deemed to know that a material portion of their customers or users are minors),

would be required to take into account the needs and capabilities of the minors whose personal information they process, particularly in respect of specified sections of the Act, such as provisions related to consent, appropriateness and deletion.

Treatment of young minors vs. mature minors

Our privacy law should require organizations to consider the needs and capabilities of **mature** minors, who may 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). The proposed CPPA inappropriately treats mature minors in the same manner as young children.

It is particularly important to note that in seven provinces and territories, the age of majority is 19 years of age, meaning that individuals as old as 18 are still legally considered to be "minors". Amending the CPPA to require organizations to consider "the needs and capabilities of minors" would still use provincial ages of majority as a starting point, but would allow flexibility when dealing with mature minors, while still providing strong protections for younger children. This approach is in accord with laws in other jurisdictions that focus protections on younger children,²³ as well as with the Canadian Marketing Code of Ethics & Standards.

The CMA is adapting the relevant provisions of our Code to reflect advancements in technology, and it is our intention to work with other stakeholders to develop a marketing-related Children's Privacy Code that would be approved as a code of practice under the CPPA, assuming that the law is adopted.

To ensure that the proposed CPPA is specific enough to effectively address minors' data, a new section should be created. The reference to minors in other sections of the bill, including in proposed sections 55(2) (d) and (f) with respect to disposal at an individual's request, should be removed.

Proposed Language: CMA Amendment 1

2 (2) For the purposes of this Act, the personal information of minors is considered to be sensitive information.

11.1 (1) An organization that directs any of its activities to minors, or that has actual or deemed knowledge that it is collecting, using or disclosing the personal information of a minor, must take into account the particular sensitivity of such personal information when fulfilling its obligations under this Act, including sections 9(2), 11(1), 12(2)(a), 15(5), 53(2), 55, 57(1), 58(8) and 74.

(2) In fulfilling its obligations under subsection (1) and section 4, the organization may have regard to the needs and capabilities of mature minors.

²³ For example, the Children's Online Privacy Protection Act in the US applies to operators of commercial websites and online services directed to children under 13 years of age, or knowingly collecting personal information from children under 13. The GDPR requires parental consent for the processing of the personal information of children under age 16 by an information society service provided directly to a child.



B. Consent and Exceptions to Consent

The provision prohibiting implied consent where one of the new exceptions to consent (for 'business activities' and 'legitimate interests') is available should be removed, as it prohibits organizations from taking a more careful approach in cases where it is not clear if a full exception to consent applies.

The exceptions to consent should not preclude routine R&D activities that help organizations better understand and serve their customers. These are beneficial and necessary aspects of operating a business. Only real and direct activities that aim to influence individuals through interactions with them should be precluded.

In order to rely on the 'legitimate interests' exception to consent, organizations should be required to consider the potential adverse effects on an individual that are 'reasonably foreseeable', rather than those that are remote or unlikely.

Canadian consumers already suffer from "consent fatigue". As a result, they are less likely to carefully review notices and make informed decisions about their personal information. Canadians' reasons for either not reading privacy policies, or not reading them frequently, is that they are too long, have too much legal jargon and are too busy.²⁴

To minimize consent fatigue so that consumers focus on important decisions, consent should be required only for activities that a reasonable person would <u>not</u> expect a business to undertake, and for activities that may carry a risk of harm.

Ensuring a practical consent model

Given serious concerns about consent fatigue, it is critical that organizations continue to have the operational choice of choosing between express or implied consent for non-sensitive information and uses. This is a longstanding strength of the Canadian consent model: it ensures that the appropriate form of consent is dependent on the context and the reasonable expectations of the individual.

Any suggestion to remove implied consent, or to overly favour express consent is not only impractical but also undermines the benefits of express consent – to help consumers make informed decisions about their data. This goal would fail miserably if express consent was used too often and not reserved for sensitive information or unexpected uses. Moreover, routinely requesting express consent would negatively affect the customer experience, and could overwhelm and cause confusion for consumers, undermining the goal of effective privacy protection.

The CPPA's new exceptions to consent are important to mitigate consent fatigue, which would help ensure meaningful consent. Some stakeholders are concerned that broadening the exceptions to consent may open the door to data misuse. However, it is critical to remember that any collection, use or disclosure of personal information (even if valid consent is obtained or an exception is used) must be **only** for purposes that a **reasonable person** would consider appropriate in the circumstances. For more than 20 years, this "reasonable person test" has helped to protect against the abuse of consent provisions. Under the proposed CPPA, this would continue to be the case.

²⁴ 2022-23 Survey of Canadians on Privacy-Related Issues, Office of the Privacy Commissioner of Canada, 2023.



The GDPR, which is often touted as providing the strictest global standard for data protection, balances a requirement for express consent with several alternative bases for processing, recognizing that explicit consent is not always appropriate, effective or meaningful for consumers. These exceptions include exceptions for "legitimate interests" and "performance of a contract," which are comparable to the "business activities" and "legitimate interest" exceptions in s. 18 of the CPPA.

We support the CPPA's new exceptions to consent for certain prescribed business activities (i.e., the "business activities" exception) and for cases where an organization's legitimate interests outweigh any adverse impacts on a consumer (i.e., the "legitimate interest" exception). These new exceptions would allow consumer privacy policies and consent requests to focus on purposes and uses that are of the greatest concern to individuals, helping consumers to focus their attention on these matters.

However, we propose two amendments to clarify the language around these exceptions to ensure that they fulfill the purpose they are intended to serve.

Implied consent with exceptions to consent

Both the "business activities" and "legitimate interests" exceptions to consent are new to Canadian privacy law. To ensure the practicality of these exceptions in the face of a wide variety of business models and activities, they are understandably expressed in fairly general language. If the CPPA were to become law, there would be considerable uncertainty respecting the application of these exceptions until clear guidance was issued, particularly in the early years after the CPPA's passage.

If it were not clear to an organization that one of the exceptions would apply, a responsible and cautious organization might reasonably elect to rely on implied consent for a particular activity, in order to ensure compliance with the law without resorting to express consent, which is necessarily more intrusive and imposes a greater burden on the individual, as well as adding to consent fatigue.

Because the CPPA prohibits reliance on implied consent where an exception would apply, it needlessly creates a scenario where organizations that take such a cautious approach to compliance could be in violation of the law – and could be penalized if the OPC subsequently determined that, in fact, one of the exceptions <u>did</u> apply.

Since many would consider implied consent to afford more knowledge and rights to a consumer than an exception to consent (including the right to opt out), it is counterintuitive to prohibit an organization from relying on implied consent in such cases.

Organizations should always have the option to rely on consent (express or implied, as appropriate), particularly where it may be unclear whether a given activity would fit within one of the exceptions in Section 18. It would not be reasonable to penalize well-intentioned and risk-averse organizations for relying on implied consent instead of an exception to consent in the interest of greater regulatory certainty.

Prohibiting the use of consent where an exception is available would also complicate transparency initiatives to the detriment of consumers: if an organization wanted to be transparent about certain business activities for which consent was not required, it would have to be list those activities in a separate part of the privacy policy, explicitly indicating that it is for information only, and not to obtain consent.

While prohibiting the use of implied consent where one of the new exceptions is available may ultimately be intended to ensure that consent is focused on matters beyond the expectations of an individual, or those causing harm – an objective which the CMA wholeheartedly supports – the negative consequences of this approach far outweigh any benefits. Therefore, this provision should be removed.



Proposed Language: CMA Amendment 2

15 (6) It is not appropriate to rely on an individual's implied consent if their personal information is collected or used for an activity described in subsection 18(2) or (3).

Marketing-related R&D activities

Both new exceptions to consent (for business activities and legitimate interests) are available only if the personal information is not collected or used "for the purpose of influencing an individual's behaviour or decisions." Depending on how this phrase is interpreted, this qualification to the new exceptions could prohibit many legitimate and reasonable business activities that enable organizations to better understand their customers' preferences, and the way they use products and services.

Customers increasingly expect organizations to work tirelessly in the background, preventing issues before they arise; knowing when, where, and how to get in touch; and proactively reaching out where necessary. Mounting such a customer service function requires an understanding of a customer through well-informed customer profiles. At a basic level, it could be a restaurant being able to record a customer's favorite wine to offer it to them on their next visit. On a more complex level, it could mean a grocery store loyalty program's ability to collect information on purchasing behavior to inform decisions on the store's layout to better serve shoppers.

If interpreted broadly, the provision would mean that consent would be required for all activities undertaken with the ultimate goal of being able to influence consumer decisions, even "preparatory" activities that do not involve direct "influencing" interactions with individuals. This would preclude organizations from undertaking, without consent, routine, legitimate and necessary back-end analytics and processing, including the internal customer analysis and segmentation that precedes the actual sending of an ad or the making of an offer.

Such a broad interpretation of the exceptions to consent clause would go well beyond what the CMA understands was the original policy rationale for this provision, which was to avoid the manipulation of personal information about individuals and groups in ways that cause public harm, including manipulating public opinion on political matters. This is an important issue; however, it falls beyond the scope of a privacy law that, constitutionally, only covers issues related to private sector trade and commerce.

The current wording of section 15(6) creates unintended consequences by potentially drawing in a range of common research-oriented business activities that may support personalized customer service, or that may ultimately inform the marketing and advertising of legitimate products and services, but that do not themselves involve the presentation of offers or promotional content to an individual.

Paragraph (b) under each of the business activities (s. 18(1)) and legitimate interest (s. 18(3)) exceptions should be revised to refer to "real" and direct marketing activities (i.e., situations where the personal information is used to communicate **directly** with the individual for the purpose of influencing that individual's behaviour or decisions). This change would be consistent with the objective of exempting common business activities from consent, and focussing privacy policies on unexpected uses.

The wording of our proposed amendment appears together with our language for Amendment 4 below, given that they both amend section 18. For clarification: the proposed exception would be confined to internal research and analysis, and would not extend to actual marketing activity, such as the sending of an offer to an individual. Direct marketing would continue to be subject to the requirements for consent under both the CPPA and CASL.



Legitimate interests exception

The proposed CPPA appears to prevent organizations from relying on the new exception for legitimate interests if those legitimate interests do not outweigh **any** potential adverse effect on the individual – regardless of how remote or unlikely that potential adverse effect may be. This is an impossibly strict standard, and not necessary to provide adequate privacy protection.

Adding the words "reasonably foreseeable" would make these sections (ss. 18(3) and 18(4)(a)) consistent with sections 15(3) and 62(2)(d), where certain consent disclosure and cross-border transparency obligations extend only to "reasonably foreseeable" consequences. According to well-established principles of statutory interpretation, where the phrase "reasonably foreseeable" is included with respect to some obligations under the Act, its absence in ss. 18(3) and 18(4)(a) would be interpreted to mean that Parliament's intention was that the legitimate interests exception would be available only where the interest outweighed any potential adverse effect, no matter how remote or unlikely.

As a practical matter, if all potentially adverse effects need to be considered in the balancing test, this may mean that the legitimate interests exception can never be relied upon without compliance risk.

Proposed Language: CMA Amendments 3 and 4

- **18 (1) Business activities** An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity described in subsection (2) and
 - (a) a reasonable person would expect the collection or use for such an activity; and
 (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions. (b) the personal information is not used to interact directly with the individual for the purpose of influencing the individual's behaviour or decisions.
- **18 (3) Legitimate interest** An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable potential adverse effect on the individual resulting from that collection or use and
 - (a) a reasonable person would expect the collection or use for such an activity; and
 (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.
 (b) the personal information is not used to interact directly with the individual for the purpose of influencing the individual's behaviour or decisions.
- (4) Prior to collecting or using personal information under subsection (3), the organization must (a) identify any reasonably foreseeable potential adverse effect on the individual that is likely to result from the collection or use;
 - (b) identify and take reasonable measures to reduce the likelihood that the <u>reasonably foreseeable</u> effects will occur or to mitigate or eliminate them; and comply with any prescribed requirements.

C. AUTOMATED DECISION SYSTEMS

The CMA supports the bill's proposal that organizations provide more transparency upfront (and at an individual's request) about automated decision systems (ADS) that make predictions, recommendations or decisions about them – as long as the definition of ADS is appropriately scoped to focus on solely automated decisions, and the obligation to explain at an individual's request is focused on decisions that are likely to have a significant impact on individuals.

Without these amendments, the bill's requirements could overwhelm consumers, create significant financial and administrative burdens for organizations and disincentivize organizations from developing and leveraging automated or partially automated systems, impacting Canada's position as a global leader in automation.



The CMA has long been a champion of transparency: our Guide to Transparency for Consumers helps organizations provide clear, user-friendly information to consumers about how their personal information is collected, used and shared. A recent CMA survey found that transparency is one of the most pivotal factors for consumers to feel comfortable with companies using their data.²⁵

We support the goal of ensuring that consumers are aware of how certain ADS may impact them. However, amendments are critical to meet the government's policy intent without unduly restricting the beneficial use of ADS for organizations and consumers.

Appropriately scoping the definition of ADS

The CMA recommends that the definition of ADS refer to only those decisions that <u>replace</u> the judgment of human decision-makers.

In its current form, the requirement would not focus on decisions that are truly automated. Systems that "assist" the judgment of human decision-makers are 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.

The proposed definition of ADS in the CPPA is broader than other frameworks. It is also broader than the Treasury Board definition, which is limited to "administrative decisions". Given the bill's subsequent transparency obligations, the 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. By contrast, the CMA's proposed amendment to the definition of ADS is in line with the approach taken in other jurisdictions, including in Quebec where only decision-making based exclusively on automated processing is subject to special requirements.

Requiring a "likelihood of significant impact" for explanations on request

The suggestion in the OPC's submission on Bill C-27 that organizations explain, on request, <u>all</u> predictions, recommendations, decisions and profiling made using automated decision systems – and not just those that could have a "significant impact on an individual", as the bill suggests – is completely impractical for both organizations and consumers.

Removing the threshold of "significant impact" would result in large amounts of innocuous information being provided to consumers, making it difficult for them to determine what is most important. 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.

²⁵ Consumer Privacy Research Findings, Sago, October 2023.



The days of collecting personal information via pen and paper are long gone. Technology is how companies collect data to serve their customers. There is a growing number of helpful automated decisions being made about us each day, resulting in beneficial services for consumers. Examples include chatbots that provide consumers with relevant and personalized advice, or the use of AI in market research to deliver adaptive surveys to customers (as opposed to more rudimentary systems, under which every respondent would be asked every question regardless of how they answered earlier questions).

Alongside the tangible benefits to individuals, automated decisions help Canadian businesses improve accuracy and efficiency and reduce costs. For example, one of the CMA's members is a media agency implementing an optimization tool that uses machine learning based on a decision tree to test, learn and optimize its creative, offers and copy in real time. Another CMA member in the not-for-profit sector has implemented a consumer voice initiative that uses natural language processing to transcribe voice to text. This greatly enhances the organization's ability to gain deeper and quicker insights into how individuals perceive their interactions with the organization, allowing it to adjust marketing and fundraising efforts accordingly.

There is no basis for restricting this type of activity unless there is a clear likelihood of significant impact.

The CPPA reasonably focuses its upfront transparency requirement and its obligation to explain at an individual's request <u>only</u> on ADS usage that could have a significant impact on the individual. We further suggest that the obligation to explain (at an individual's request) reflect a <u>likelihood</u> of significant impact, which moves the requirement from theoretical impacts to a more pragmatic assessment of real risk. This is appropriate to the nature of automated decisions in practice, as well as to the privacy risk of automated decisions.

These changes will greatly reduce unintended impacts and unnecessary restrictions on innovation and technology-use, while providing individuals with greater transparency respecting complex ADS that are used to make high-impact decisions about them.

The CMA's proposed approach – a properly scoped definition of ADS, a transparency obligation regarding the broader use of impactful ADS and a very specific obligation to explain upon request (for decisions that are <u>likely</u> to have a significant impact on an individual) – leaves room for OPC guidance or industry best practices (codes or certifications) to support these requirements, including how to best provide a "general account" of ADS, and what explanation would be reasonable under the circumstances.

Proposed Language: CMA Amendment 5

- **2 (1)** *automated decision system* means any technology that <u>assists or</u> replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets.
- **63 (3)** If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could-is likely to have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision.



D. De-identified and Anonymized Data

The bill should incorporate the amendments put forward by the Canadian Anonymization Network (CANON), which aim to ensure that policy standards for deidentified and anonymized data enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

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 that the CPPA not create unworkable definitions of de-identified or anonymized data, nor overly restrict its use, which would impede important data-driven technologies and services, and redirect the innovation they enable to other jurisdictions with less restrictive frameworks.

The CMA urges the INDU Committee to adopt the amendments to the CPPA's de-identification and anonymization provisions proposed by CANON in its <u>May 2023 submission</u>.

The proposed definition of the term "anonymize" within the CPPA sets an extremely high and practically unworkable threshold for the circumstances in which information would no longer be deemed to be "identifiable" (and therefore no longer subject to the CPPA), essentially requiring something close to a standard of perfection. A more realistic approach to defining when personal information will be treated as anonymized must incorporate the notion of foreseeable risk of reidentification.

The suggestion in the OPC's submission on Bill C-27 to delete from the definition of "anonymize" the words "...in accordance with generally accepted best practices..." would only make things worse, rendering anonymization useless as a privacy enhancing tool. As noted by CANON, the reference in the existing definition to "generally accepted best practices" is appropriate 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. In addition to being practically unworkable, the OPC's proposal goes counter to longstanding jurisprudence that indicates when personal information is no longer considered to be personal information subject to the law.

E. Transition Period

The law should come into force in a staged manner over three years, so that Canadian organizations have the appropriate time to implement the significant operational changes and undertake staff training to ensure compliance.

Organizations will need time to assess the new law, once passed, and to implement potentially sweeping changes to compliance plans, business processes, staff training and IT systems. SMEs may face resource issues in having to tool up quickly to comply with the new law, while large enterprises with numerous and complex applications, systems and processes will need sufficient time to reprogram and redevelop systems and processes, and to train personnel.

Except for obligations that are similar to existing PIPEDA requirements, we recommend a phased approach to implementation for all net new obligations under the law, providing organizations with either 24 or 36 months after the Digital Charter Implementation Act receives Royal Assent or the applicable provision comes into force.



Some provisions would require significantly more effort by organizations than others to adjust systems and processes to fully comply. In some cases, organizations would need to implement or completely redesign IT systems, including legacy or layered IT systems for which changes require time to secure budgets, scope, plan, execute, and test. Even small changes to IT systems can result in time-consuming challenges, including system disruptions. Further, most organizations plan for capital expenses several quarters in advance.

A new law would require substantial staff training, as well as updates to internal and external policies and procedures, consumer-facing interfaces, and contractual arrangements with service providers. Some provisions will also require time to evaluate complex regulations to determine how to best develop and implement policies and practices to address them. OPC guidance and industry best practices also require sufficient time to evolve. These processes are challenging for SMEs who do not have in-house capabilities to assess, plan and comply. They are also challenging for large organizations with complex, and in some cases, legacy systems, and thousands of employees to train.

A phased-in approach would be consistent with Quebec's Law 25, which has a three-year phased implementation period.

The CMA proposes that the following sections of the bill should come into force, by order of the Governor in Council, within the time periods indicated below:

- 1) To come into force no earlier than **24 months** after the *Digital Charter Implementation Act*, *2022* receives Royal Assent:
 - S. 4 Minors' authorized representatives
 - S. 18 Business activities and legitimate interest exceptions to consent
 - S. 53 Period for retention and disposal
 - S. 54 Personal information used for decision-making
 - S. 62 Openness and transparency policies and practices
 - S. 123 Data mobility frameworks

To come into force no earlier than **36 months** after the *Digital Charter Implementation Act*, *2022* receives Royal Assent:

- o S. 15 Form of consent (express consent default)
- S. 55 Disposal at individual's request
- o S. 63 (3) & (4) Automated decision system explanation
- o S. 72 Disclosure under data mobility framework
- 2) To come into force no earlier than the tabling of the report following the first Parliamentary review as set out in s.129 of the *Consumer Privacy Protection Act*:
 - S. 107

Proposed Language: CMA Amendment 6

- 130 (1) Subject to subsections (2),(3) and (4), this Act comes into force on the day on which section 3 of the *Digital Charter Implementation Act*, 2022 comes into force.
- (2) Sections 4, 18, 53,54, 62 and 123 come into force on a day to be fixed by order of the Governor in Council.
- (3) Sections 15, 55, 63(3) and (4), 72, 76 to 81, paragraph 83(1)(d), subsection 94(3) and section 125 come into force on a day to be fixed by order of the Governor in Council.
- (4) Section 107 comes into force on a day to be fixed by order of the Governor in Council.



For questions or comments regarding this submission, please contact:

Sara Clodman

VP, Public Affairs and Thought Leadership sclodman@theCMA.ca

Fiona Wilson

Director, Public Policy & Chief Privacy Officer fwilson@theCMA.ca

About the Canadian Marketing Association

The CMA is the voice of marketing in Canada and our purpose is to champion marketing's powerful impact. We are the catalyst to help Canada's marketers thrive today, while building the marketing mindset and environment of tomorrow. We provide opportunities for our members from coast to coast to develop professionally, to contribute to marketing thought leadership, to build strong networks, and to strengthen the regulatory climate for business success. Our Chartered Marketer (CM) designation signifies that recipients are highly qualified and up to date with best practices, as reflected in the Canadian Marketing Code of Ethics and Standards. We represent virtually all of Canada's major business sectors, and all marketing disciplines, channels and technologies. Our Consumer Centre helps Canadians better understand their rights and obligations. For more information, visit thecma.ca.



Appendix: Table of Proposed Amendments to Part 1 of Bill C-27 by the Canadian Marketing Association

| Section | Proposed Amendment |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 | Interpretation – minors |
| | 2 (2) For the purposes of this Act, the personal information of minors is considered to be sensitive information. |
| | 11.1(1) An organization that directs any of its activities to minors, or that has actual or deemed knowledge that it is collecting, using or disclosing the personal information of a minor, must take into account the particular sensitivity of such personal information when fulfilling its obligations under this Act, including sections 9(2), 11(1), 12(2)(a), 15(5), 53(2), 55, 57(1), 58(8) and 74. |
| | (2) In fulfilling its obligations under subsection (1) and section 4, the organization may have regard to the needs and capabilities of mature minors. |
| 15 | Consent – Business activities |
| | 15 (6) It is not appropriate to rely on an individual's implied consent if their personal information is collected or used for an activity described in subsection 18(2) or (3). |
| 18 | Exceptions to Requirement for Consent – Business activities |
| | 18 (1) An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity described in subsection (2) and (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions. (b) the personal information is not used to interact directly with the individual for the purpose of influencing the individual's behaviour or decisions. |
| 18 | Exceptions to Requirement for Consent – Legitimate interest |
| | 18 (3) An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable potential adverse effect on the individual resulting from that collection or use and (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions. (b) the personal information is not used to interact directly with the individual for the purpose of influencing the individual's behaviour or decisions. |
| | (4) Prior to collecting or using personal information under subsection (3), the organization must (a) identify any <u>reasonably foreseeable</u> potential adverse effect on the individual that is likely to result from the collection or use; (b) identify and take reasonable measures to reduce the likelihood that the <u>reasonably foreseeable</u> effects will occur or to mitigate or eliminate them; and comply with any prescribed requirements. |
| 55 | Minors' Data |
| | 11.1(1) An organization that directs any of its activities to minors, or that has actual or deemed knowledge that it is collecting, using or disclosing the personal information of a minor, must take into |



| | account the particular sensitivity of such personal information when fulfilling its obligations under this Act, including sections 9(2), 11(1), 12(2)(a), 15(5), 53(2), 55, 57(1), 58(8) and 74. (2) In fulfilling its obligations under subsection (1) and section 4, the organization may have regard to the needs and capabilities of mature minors. |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2, 63 | 2 (1) automated decision system means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets. Access to and Amendment of Personal Information – Automated decision system 63 (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could is likely to have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision. |
| 130 | Coming into force – Order in council 130 (1) Subject to subsections (2),(3) and (4), this Act comes into force on the day on which section 3 of the <i>Digital Charter Implementation Act</i> , 2022 comes into force. (2) Sections 4, 18, 53,54, 62 and 123 come into force on a day to be fixed by order of the Governor in Council. (3) Sections 15, 55, 63(3) and (4), 72, 76 to 81, paragraph 83(1)(d), subsection 94(3) and section 125 come into force on a day to be fixed by order of the Governor in Council. (4) Section 107 comes into force on a day to be fixed by order of the Governor in Council |