

Submission by the Canadian Marketing Association to the Consultation on Modernizing Privacy in Ontario

September 3, 2021

Executive Summary

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Ministry of Government and Consumer Service's consultation on modernizing privacy in Ontario.

Data is, and will continue to be, a driving force for innovation across all industries Ontario's data-driven industries will play a central role in driving post-pandemic economic recovery. It is critical for privacy regulation to enable the responsible use of data to drive innovation, efficiencies and productivity, to help ensure a strong economic future for Ontarians for years to come.

We strongly urge Ontario to continue to rely on federal privacy law for privacy protection. Federal privacy law reform is expected to be a continued priority in the new parliament, and any new provincial legislation should address only those sectors and activities that a reformed federal law will not cover. A harmonized national privacy regime that enables the responsible use of data for innovation would be the best outcome for Ontarians, making it easier for consumers to understand and exercise their privacy rights, and for organizations to compete effectively at home and globally.

Should the Government of Ontario move forward with private sector privacy legislation (ideally in the manner indicated above), it is critical that any approach to private sector privacy reflect:

- The critical importance of data, including personal information, to the digital economy,
- Evolving consumer privacy expectations, which indicate consumer appreciation of the value of responsible data use and sharing, and:
- The ability for small and medium-sized businesses (SMEs) the backbone of Ontario's economy

 to leverage consumer data to compete and grow.

We fully support Ontario's dual goal of protecting the personal information of individual Ontarians, while ensuring that any new privacy protections do not pose an unnecessary burden on businesses or inhibit the growth and prosperity of Ontario's innovation ecosystem.

Some of the recommendations in the *Modernizing Privacy in Ontario* whitepaper need to be adjusted or reconsidered to achieve this goal. The CMA has the following recommendations in seven key areas for the Government of Ontario to address should it move forward with private sector privacy legislation.

- 1. **Align with federal privacy law** to prevent complexity and disruption for organizations and consumers, and complications for trade and investment.
- Ensure any new privacy law is flexible, principles-based and proportionate to the privacy
 objectives to be achieved, permitting the law to be nimble in the face of rapidly evolving
 technologies, business models and consumer expectations.
- 3. **Protect individual privacy rights, without hindering reasonable private sector activities.** Individual privacy in a <u>private sector</u> context is best protected through a thoughtful framework of new and enhanced privacy rights and obligations. The human rights-based preamble proposed in the whitepaper would result in a chilling impact on organizations that is disproportionate to the privacy benefit.
- 4. Ensure consent requirements and exceptions are meaningful for consumers and practical for organizations. To combat consumer consent fatigue, Ontario's approach must avoid the over-emphasis on express consent, and rigid, rules-based requirements for valid consent found in Bill C-11. To permit reasonable and beneficial data use, and to focus consent on what matters

most, a new exception to consent for legitimates interests should be incorporated into the law, placing additional transparency and accountability obligations on organizations.

- 5. Ensure any new right to deletion includes sufficient exceptions to account for practical consequences, and to balance this right with other important social and economic objectives.
- 6. Ensure adequate protections around automated decision systems without unduly restricting the beneficial use of these systems for consumers and organizations. New openness and transparency obligations will provide meaningful consumer protection, without unduly restricting the use of ADS through harsher restrictions.
- 7. Preserve the ability for organizations to leverage de-identified and pseudonymized information for the benefit of consumers and organizations. Align with other global approaches by excluding de-identified information that is, by definition, not personal information, from the scope of the law, and implanting effective safeguards around the use of pseudonymized information.

Ontario's businesses – large and small – will carry us forward into economic recovery. The law must focus on preventing malicious misuse of data and material harm to consumers rather than creating hurdles and hard barriers to reasonable uses of data that have become essential aspects of business in a digital age.

The CMA looks forward to continued discussions with the Government of Ontario on these important topics.

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Ministry of Government and Consumer Service's consultation on modernizing privacy in Ontario.

The CMA is the voice of the marketing profession in Canada, representing more than 400 corporate, not-for-profit, public, and post-secondary member organizations, most of which are headquartered in Ontario. We are committed to helping marketers and their organizations maintain high standards of conduct and transparency through our mandatory Canadian Marketing Code of Ethics & Standards, and our training and professional development opportunities, including the Chartered Marketer (CM) designation program. We offer extensive resources on privacy law and best practice, including a Guide on Transparency for Consumers. Our online Consumer Centre helps consumers can understand their privacy rights and obligations. We regularly handle marketing-related privacy enquiries and requests for information from both marketers and consumers.

Marketing – the link between organizations and their consumers – is a key driver of Ontario's economic growth and recovery. Marketing stimulates consumer demand, supports business expansion and generates substantial direct and indirect employment for Ontarians across all key sectors and industries.

Ontario's marketers highly value their relationships with consumers. The loyalty and trust of customers is the foundation for business success, and most Ontario organizations work hard to protect and respect the privacy interests of the individuals they serve.

We appreciate the Government of Ontario's commitment to protecting privacy, while supporting the smart use of data to fuel economic growth.

It is critical that any approach to private sector privacy pursued by Ontario reflect the following:

• The critical importance of a harmonized national privacy regime: A harmonized national privacy regime would be the best outcome for Ontarians, making it easier for consumers to understand and exercise their privacy rights, and for businesses to comply.

We strongly urge Ontario to continue to rely on federal privacy law for privacy protection. Federal privacy law reform is expected to be a continued priority in a new parliament, particularly given the need for Canada's renewed adequacy status with the EU. Any new provincial legislation should address only those sectors and activities that a reformed federal law won't cover.

The creation of a new private sector privacy framework for Ontario would create substantial additional costs for government as well as regulatory complexity for organizations as they adjust to a new law, if one set of rules were to apply to Ontario organizations when engaging in intraprovincial activities and another were to apply to those same organizations when engaging in interprovincial and international activities.

Consistent and coherent privacy regulation across the country provides certainty for consumers, organizations and government. It is also the most cost-effective regulatory approach, particularly given the current demands of the pandemic on the provincial budget.

There are some limitations on the federal law's application to certain sectors and activities in Ontario, including employees in provincially regulated sectors. Once the federal privacy law is reformed, a provincial framework should only address privacy protections for Ontarians where the

sector or subject matter will not be covered federally. This will prevent the creation of a costly and duplicative overarching privacy framework in Ontario.

• The critical importance of data to the digital economy: Ontarians have never been more reliant on the digital economy. It improves our personal lives and well-being. At work, it supports our ability to innovate, build businesses and remain competitive.

When used responsibly and in a privacy preserving manner, the analysis and use of personal information is critical to our digital economy, and can be highly beneficial to consumers, organizations, government and society.

Data is, and will continue to be, a driving force for innovation across all industries. It is estimated that Canadian investment in data has grown more than 400 percent in the last 15 years, and that 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. What's more, we are relying on our data-driven industries to play a central role in driving post-pandemic economic recovery.

Privacy regulation that supports the increasing focus on data as a vehicle to drive innovation, efficiencies and productivity will help ensure a strong economic future for Ontarians for years to come.

- Evolving consumer privacy expectations: The ability for organizations to collect, use and
 disclose personal information is key to providing value to consumers. At the same time,
 consumers increasingly expect organizations to deliver the intuitive products and services they
 want and need.
 - In a recent survey by Ipsos Canada, 50% of consumers indicated a desire to see internet
 advertising that is relevant and targeted to them, despite having concerns about the
 security of their personal information.
 - A 2018 research study <u>Data Privacy What the Canadian consumer really thinks</u> found that a strong majority of Canadian consumers (76%) are willing to share personal data in order to receive benefits, as long as the data is properly protected.
 - According to a recent survey from Kantar, more than 80% of consumers are concerned about the unauthorized access of their personal information, while only 35% are concerned about receiving unwanted ads. Although 77% of Canadians are concerned about privacy and data protection, they are significantly more concerned about criminal activity than by attempts by the private sector to serve them in a more targeted and personalized way.

Technological advancements have provided organizations across Ontario with the agility to offer relevant, useful offerings to consumers who want them.

User data-driven systems, including recommendation engines, customer service chatbots and marketing geared towards consumer preferences, are important and beneficial tools and services for consumers, and for organizations striving to better serve their customers. For example, nearly all industries (retail, banking, insurance, travel, grocery etc.) now offer recommendation engines to assist consumers with their digital choices. Many consumers have grown accustomed to, and value receiving these recommendations, as they often save time and money, and help to ensure consumers have everything they require to utilize the products and services they are purchasing.

Similarly, many companies run advanced customer pricing analytics/loyalty analytics to offer consumers discounted prices based on historic shopping behaviour. This helps consumers save money and helps companies build better relationships with consumers by providing them with opportunities to save.

Ontario's public policy approach must acknowledge evolving consumer interests and expectations, and recognize the enormous economic and social benefits of the data economy for individuals.

• The ability for SMEs to flourish and sustain our economy: A recent survey of over 1,000 Canadian small and medium-sized enterprises (SMEs), the State of Small and Medium Businesses in 2021, shows the critical importance of consumer data to SMEs. The ability to leverage consumer data to communicate regularly and in a personalized manner with customers was cited as the primary way SMEs built enough consumer trust and loyalty to weather the pandemic. Their ability to access and apply consumer data was also cited as their top ongoing strategy to continue to compete against large online competitors.

As Ontario navigates the road to post-pandemic recovery, it is critical that any proposal for privacy regulation focus on protecting consumers against bad actors and significant harms, as opposed to creating an unnecessary or ineffective administrative burden for responsible companies. This includes Ontario's SMEs that, as the backbone of our economy, must not be subject to a rigid regulatory framework that would not be adaptable to new technologies and opportunities that could deliver greater business efficiencies and provide useful products and services to consumers.

With 98% of Ontario companies falling into the small to mid-sized category, it is critical that these companies not be faced with any new privacy requirements that create a significant administrative burden without an equally strong privacy protection rationale. For many SMEs, these barriers could prove debilitating in terms of the capital required, and limitations on the ability to automate and optimize. Furthermore, SMEs slack ready access to legal advice and representation to navigate the complexities of restrictive legislation, making it more difficult for them to use data to innovate and compete.

Many of the voices calling for stricter privacy regimes aim to protect against flagrant and malicious misuse of consumer data, no doubt responding to the more extreme cases of misuse that have occurred in recent times. We do not in any way condone these abuses. It is important that the law focus on preventing malicious misuse of data and material harm to consumers rather than creating hurdles and hard barriers to reasonable uses of data that have become essential aspects of business in a digital age.

Recommendations

We fully support Ontario's dual goal of protecting the personal information of individual Ontarians, while ensuring that any new privacy protections do not pose an unnecessary burden on businesses or inhibit the growth and prosperity of Ontario's innovation ecosystem.

Some of the recommendations in the *Modernizing Privacy in Ontario* whitepaper need to be adjusted or reconsidered to achieve this goal. The CMA has the following recommendations in seven key areas for the Government of Ontario to address should it move forward with private sector privacy legislation.

1. Align with federal privacy law to prevent disruptions for organizations and consumers, and complications for trade and investment

Ontario must align with federal privacy law, which is scheduled for reform, in order to prevent the damaging fragmentation of privacy frameworks, and negative impacts on the data-based integrated industries that operate across provinces, the country and internationally.

If approaches between the provinces and federal government are not aligned, the resulting patchwork of privacy legislation will create undue complexity for organizations, cause confusion for consumers, complicating conditions for trade, and reducing Ontario's attractiveness as a business destination. It will also create crippling demands on SMEs and opportunities for malicious actors and other opportunists seeking to exploit differences in data protection.

The federal government's Bill C-11, if subject to amendments in a few key areas, proposed an effective approach to private sector privacy law. Importantly, it would preserve Canada's principles-based, technology and sector-neutral approach to privacy, helping to ensure flexibility in the face of rapidly evolving technologies, business models and consumer privacy expectations. It also would provide consumers with added privacy protections and controls, including more explicitly articulated rights to enable more meaningful control over their data, and new requirements for companies to be more transparent about their use of personal information – backed by strong penalties and enforcement.

The CMA has provided significant feedback to the federal government on the strengths and challenges of Bill C-11. The recommendations in this submission are guided by similar concerns with respect to the efficacy and workability of the proposed framework, as well as the need to ensure interoperability with the federal approach, which is likely to be revived in similar form by the next government.

It is critical for Ontario – and all provinces enacting their own private sector privacy laws – to align with each other, and with the federal government's approach to privacy law so that organizations across the country have consistent regulation, and consumers have strong protections.

2. Ensure any new privacy law is flexible, principles-based and proportionate to the privacy objectives to be achieved

In today's digital economy, it is important for the law to be nimble in the face of rapidly evolving technologies, business models and consumer expectations, without the need to repeatedly introduce legislative amendments to keep up with the times.

Privacy law must be based on sound principles that are flexible enough to account for context, and can be thoughtfully applied to all technologies and business models. This is especially important to avoid creating a legal framework that would preclude innovative technologies, and the beneficial products and services that they would enable. A flexible approach is also important to ensure compliance is not unduly

onerous for SMEs, allowing them to determine the most effective way to meet their common obligations given operational realities and context-specific risks.

The law must be flexible enough to impose measures proportionate to the privacy interests involved and the individual's reasonable expectation of privacy in the circumstances. It must include a clear purpose clause ensuring that the law be interpreted in a proportionate and reasonable manner based on the circumstances.

Many features of existing Canadian privacy laws have stood the test of time, providing privacy protection without unnecessary regulatory burden. Newer and more prescriptive laws in other jurisdictions, including the GDPR, remain unproven in many respects, have created a staggering regulatory burden for both government and business, and have had negative and costly impacts on the economy and trade.

In considering the adoption of certain aspects of GDPR, we urge the government to evaluate each based on its merit in the Ontario context, with the goal being compatible privacy outcomes as opposed to parallel legislative requirements and restrictions.

3. Protect individual privacy rights, without hindering beneficial private sector activities

We share the Government of Ontario's goal to protect the privacy of Ontarians in all commercial contexts and to maintain a high level of trust and confidence in the digital economy. We support the creation of new rules and rights to protect individuals from potentially unfair practices, particularly those that carry a risk of material harm to Ontarians.

However, the human rights-based approach proposed in the whitepaper is not the best approach for a new law governing private sector activities, as it is unnecessary, provides no demonstrable benefit over the approach taken in existing Canadian private sector laws, and could result in a reduction in the flexibility found in those other laws, including in PIPEDA.

Characterizing privacy as a fundamental human right for legislative purposes creates complicated and nuanced challenges. The word "privacy" is a sweeping generic term used to refer to an extremely broad range of scenarios and interests, including those related to physical (body and health) privacy, locational privacy, communications privacy, and information privacy, to name just a few. The myriad of potential uses of personal information, and the effect of those uses on the individual, fall on a broad spectrum ranging from inconsequential to catastrophic.

At one end of the spectrum, "privacy" means restrictions on the interaction between the individual and the state, relating to activities such as surveillance, physical interference with the person and intrusion into the private dwellings of individuals. These aspects of privacy are already the subject of constitutional recognition and protection, such as through the fundamental rights guaranteed by the Canadian Charter of Rights and Freedoms. In addition, individual privacy interests against the state are recognized and protected in laws such as the *Freedom of Information and Protection of Privacy Act*, which governs the collection, use and disclosure of personal information by public sector organizations in Ontario, and in the various restrictions and safeguards contained in statutes like the Criminal Code. Courts have frequently recognized and preserved the privacy interests of individuals against state action, typically in cases involving Criminal Code investigations.

Closer to the other end of the spectrum, the term "privacy" can involve the collection and processing by a business of personal information necessary to complete a simple transaction between that business and a consumer, such as payment and delivery details. Also nearer to this end of the spectrum would be the use of consumer personal information by the business for other lawful and appropriate purposes, such as to better understand customer behaviour and preferences, in order to variously improve or expand its product and service offerings, gain business efficiencies, protect business and consumer interests, and

provide information, offers and promotions to consumers that align with their individual interests and preferences.

The majority of potential scenarios denoted by the word "privacy" do not involve unfair practices, do not carry a risk of substantial harm to individuals' relate to democratic freedoms, such as those guaranteed in the Canadian Charter of Rights and Freedoms, and do not encroach on the concepts of freedom, equality and dignity that underlie declared human rights.

In comparison to other recognized fundamental rights, privacy – specifically "information privacy" - stands out in two important ways. First, privacy is uniquely about a relationship between two parties (a provider and a receiver), the interchange of data between them and the knowledge that can result.

The whitepaper indicates that privacy is more than an individual concern, suggesting that it is part of the social capital of a democratic society. As such, privacy, and the exchange of information between parties, is an important and necessary element of both modern societies and modern economies. A singular focus on the individual interests involved in such exchanges does not do justice to the broader societal and economic interests at play.

Second, while most recognized human rights are qualified in some way (such as by the reasonable limits in s.1 of the Canadian Charter of Rights and Freedoms), the proposed right of privacy stands out as being more nuanced and context-specific.

It is incorrect to suggest that a privacy law governing private sector activities must enshrine privacy as a human right to be effective and appropriate. The fact that Canada or Ontario does not legislatively or constitutionally recognize a single, over-arching "human right to privacy" to cover all contexts, including private sector and commercial ones, does not mean that the government and its agents cannot pursue regulatory approaches that place limits on private sector activities where necessary to protect the privacy interests of individuals. Privacy law already does so and can be amended to introduce further controls if needed.

The whitepaper proposal could not create an enforceable human right, as the Charter does, as this would not be legally possible through privacy law. Rather, the proposal aims to replace the current approach taken by Canadian privacy laws to date, which references the importance of both individual privacy interests and legitimate business interests, with a purpose statement that indicates that, by default, individual privacy interests should always prevail over business and broader societal/economic interests.

The reframing of the traditional approach of Canadian private sector laws is both unnecessary and illadvised. We are not aware of any complaint or investigation considered by the federal Privacy Commissioner (on matters of private sector privacy), where the commissioner was constrained by the existing purpose statement in PIPEDA, or where the outcome of the investigation would be different under the newly proposed approach. The Privacy Commissioner has not put forward practical examples that would support the need to recalibrate the federal law in the way proposed in the whitepaper.

In fact, both PIPEDA and Bill C-11 incorporate principles that recognize important aspects of individual privacy interests, including principles of minimal impairment, necessity and proportionality. They also require fair and appropriate purposes, and limits on collection, use and disclosure.

Rights-based language was also observable in C-11 in the context of cross-border data flows, and in the requirement to use proportionality when assessing the level of de-identification of personal information. Individuals would have several explicit rights with respect to their personal information, including access, correction, new mobility rights, as well as consent-based rights, including more explicit rights to withdraw consent and require the deletion of personal information.

This more practical and flexible approach constitutes the most meaningful approach to protecting individual privacy rights without having a chilling impact on important and beneficial private sector activities.

The purpose of a law for the private sector is to set rules governing the collection, use and disclosure of personal information in a manner that recognizes both individual privacy rights and the appropriate needs of organizations. This balanced objective continues to be the prudent approach so that businesses can thrive and support Ontarians and the economy.

A skewed and singular human rights-based approach to privacy would lead to disproportionate regulation without necessarily providing meaningful additional protection to consumers.

Placing privacy interests over business interests by default would potentially paralyze normal business activities and have damaging effects on the economy at a time where data innovation is critical to our economic recovery.

To date in Ontario, the legal treatment of "privacy" in relationships between businesses and consumers has appropriately recognized the interests of both parties and allowed for interpretations that consider both interests in context in determining what rules or approach is in the public interest. It is critical that this approach continue federally, and be incorporated into any new Ontario private sector privacy law.

4. Ensure consent requirements and exceptions are meaningful for consumers and practical for organizations

We support Ontario's goal of "improving the meaningfulness of consent" by making it more informed, while providing alternate authorities for collecting and using personal information to reduce consent fatigue.

Consent must be meaningful and focused on what matters most. The CMA provides significant guidance to the marketing community on how to ensure these principles are met.

Ontario's consumers already suffer from consent fatigue, causing them to be less likely to carefully review notices and make informed decisions. It is critical that any new requirements not exacerbate this problem.

The whitepaper proposes a number of consent provisions that are consistent with those proposed in Bill C-11. Several of these are problematic.

Overall, it presents a framework that would be more prescriptive than the GDPR, which offers an objective principles-based approach to consent and alternative legal bases for processing. The bill's overemphasis on express consent – coupled with its rigid, rules-based requirements for requesting valid consent and for relying on exceptions to consent – will be problematic for both consumers and organizations.

The approach would result in a lack of interoperability with other consent regimes, which would cause organizations operating in Ontario to re-consider their operations due to the additional compliance burdens associated with managing the law's unique consent requirements.

Aspects of the approach that need to be adjusted are:

a. Form of consent, and requirements for valid consent: Express consent would be required for the collection, use, and disclosure of personal information unless the organization established that it is appropriate to rely on an individual's implied consent. Making express consent the default form of consent would be counter to the Ontario's goal of improving the meaningfulness of consent, as it would result in the need for consumers to positively affirm consent in even more situations than they do currently. Such explicit requests are daunting for consumers, and would exacerbate consent fatigue. Worse, given the potential liability of organizations for non-compliance and the uncertainty over the scenarios where reliance on implied consent would be considered to be appropriate, it is likely that risk adverse businesses would resort to reliance on express consent by default, including in situations that would not warrant it.

Legislating express consent as the default departs from PIPEDA's current balanced approach, which encourages organizations to make a contextual analysis of whether to seek express or implied consent, based on the reasonable expectations of the individual and sensitivity of the information. It also stands in contrast to the GDPR's approach, which balances a requirement for express consent with alternative bases for processing. Both approaches recognize that explicit consent is not always appropriate, effective, or meaningful for consumers.

These prescriptive rules for requesting valid consent would not serve organizations or consumers as well as the more balanced approach under Canadian privacy laws to date. This includes indicating that express consent "should" rather than "must" be obtained, and that consent is valid only if "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." Where necessary, through decisions and guidance, the Information and Privacy Commissioner for Ontario could draw boundaries with respect to the use of implied consent in specific areas of concern. Such a considered and targeted approach to express consent would be far more effective than a default requirement within legislation.

In addition to the overemphasis on express consent, Bill C-11 proposes even more rigid and prescriptive requirements for valid consent, mandating organizations to provide information to individuals in a number of specific areas.

This will result in consumers being faced with more repetitive and lengthy requests for consent. Disclosure requirements that are too prescriptive will not result in better consumer understanding. Given the wide variety of business models and data uses, organizations need the flexibility to determine how best to communicate with individuals in an understandable way, considering the context, target audience and actual risks. The CMA recommends organizations be permitted more flexibility to satisfy the validity requirement using different methods.

b. Refusal to deal: The whitepaper indicates that an organization must not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service.

Currently, PIPEDA provides a preferable, more flexible approach by prohibiting an organization from requiring consent to processing beyond what is required to fulfil explicitly specified, legitimate purposes. It is not clear what concern the narrower language proposed in the whitepaper is intended to address, let alone the materiality of any consumer harms it is intended to reduce, or why the concern needs to be addressed in the statute itself, as opposed to being the subject of guidance by the OIPC.

The narrower language proposed could result in the loss of the ability of many organizations to operate and manage their business in the broader sense, beyond the narrow administration of a particular consumer transaction. It is uncertain whether common and beneficial uses of information by organizations, including internal and administrative purposes, can continue to be

conditions of using a product or service, such as personalizing experiences or making recommendations (where these experiences or recommendations are part of the product or service). Again, faced with the imposition of very significant monetary penalties for non-compliance, risk-averse businesses will likely err on the side of tailoring any required consents to be very narrow, potentially excluding data uses that would have ultimately been determined to be "necessary". This would have a negative impact on innovation, limiting the opportunities and learning that could have resulted from a larger data set or expanded uses.

A more appropriate standard would be PIPEDA's standard of beyond the "explicitly specified and legitimate purposes."

c. Alternatives to consent: The whitepaper is proposing to adopt many of the same exceptions to consent as Bill C-11, but framing these exceptions as instances in which personal information can be collected, used or disclosed as alternatives to consent. These exceptions are unduly narrow and only cover specific circumstances. Even under the GDPR, the additional legal bases for processing (e.g., for legitimate interests) offer more flexibility.

Whether they are framed as exceptions or alternatives, the proposed list is too prescriptive to accommodate many common activities that a reasonable person would expect a business to undertake.

The list of business activities that would give rise to an alternative legal basis for processing must be broadened to recognize additional common practices for businesses with respect to R&D activities that may use personal information (e.g., to allow businesses to better understand their customers, their preferences, and the way they use products and services). This will support consumer understanding by allowing privacy policies to focus on more unexpected uses.

Consumers would be well protected under this approach because any collection, use or disclosure of personal information (even if valid consent is obtained or an exception is used) must be <u>only</u> for purposes that a reasonable person would consider appropriate in the circumstances¹. For more than 20 years, this "reasonable person test" has been an overarching requirement helping to protect against the abuse of consent provisions. This will continue to be the case.

To respond to the call for more demonstrable accountability by organizations with regards to the proposed business activities exception, we urge Ontario to consider adapting the approach taken in Singapore's privacy law, which provides an exception to consent for legitimate interests, but includes built-in safeguards that create greater accountability for organizations that may choose to rely on this exception, including enhanced transparency measures and a balancing test.

This conceptual approach is practical enough to apply to any type of processing for any reasonable purpose, and unlike the Bill C-11 approach, it is not limited to "collection" and "use".

Further, it would enhance interoperability with leading privacy laws elsewhere, including the GDPR. The GDPR incorporates a three-part test that considers if there is a legitimate interest behind the processing, if the processing necessary for that purpose, and whether the legitimate interest overridden by the individual's interests, rights or freedoms. Singapore has supplemented the GDPR approach with explicit requirements that organizations relying on the exception must

¹This requirement would have prevented the concern outlined in the whitepaper that Bill C-11 would have allowed businesses to process Ontarian's data without consent "simply on the basis of convenience or expedience". While s. 18 provided that organizations could process personal information without consent where the processing was undertaken for the purpose of one of the business activities listed in that section, such processing could <u>only</u> occur without consent where a reasonable person would expect such a collection or use for the activity in question and where the purposes did not include influencing the individual's behaviour or decisions.

conduct an assessment of the business and individual interests at play, as well as informing individuals of the organization's reliance on legitimate interests.

If Ontario considered this approach, it would need to ensure the level of assessment required is not too onerous on SMEs that could benefit from the use of this exception. The level of assessment should be based on specific factors, and should take into account existing requirements expected of organizations through Privacy Management Programs.

Below is how we suggest the Singapore approach be incorporated into the list of business activities that were included in the whitepaper.

List of activities

- (2) Subject to the regulations, the following activities are business activities for the purpose of subsection (1):
 - (a) an activity that is necessary to provide or deliver a product or service that the individual has requested from the organization;
 - **(b)** an activity that is carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk;
 - (c) an activity that is necessary for the organization's information, system or network security;
 - (d) an activity that is necessary for the safety of a product or service that the organization provides or delivers;
 - (e) an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual Any other business activity pursued by an organization or another person where:
 - i) the activity is undertaken in pursuit of the lawful business interests of the organization or other person;
 - ii) that activity does not materially or unduly interfere with the privacy interests of an individual;
 - iii) the organization or other person makes readily available a description of its lawful business interests, including identifying the purposes for which it collects, uses and discloses personal information in relation to the activity; and
 - iv) prior to pursuing the activity, the organization or other person considers the following factors, documenting and retaining its analysis and decision to proceed with the activity:
 - a. the nature and necessity of its lawful business interests;b. the resulting benefits to the organization or other person, or any
 - the resulting benefits to the organization or other person, or any other persons;
 - any adverse effect that the proposed collection, use or disclosure is likely to have on an individual;
 - any reasonable measures that may be implemented to eliminate any such adverse effect, mitigate the effect or reduce the risk of occurrence of the effect
 - e. any other prescribed requirements; and
 - (f) any other prescribed activity.

Finally, its not clear why Ontario is proposing to frame what the federal regime considers to be exceptions to consent as alternatives to consent. If the government proceeds with this approach, in the context of what is largely a consent-based statute, it will be necessary to specify explicitly that consent will not be required with respect to any of the alternatives to consent that may be set out in the law. To the extent that an Ontario law would include a general requirement for consent, it's not clear that the proposed wording for the alternatives contained in the whitepaper would be interpreted by a court as overriding the general requirement for consent.

5. Ensure any new right to deletion includes sufficient exceptions to account for practical consequences

We support the government's goal of ensuring personal information is not held by organizations for longer than necessary, and for consumers to have sufficient control in that regard. A right to deletion already exists implicitly in PIPEDA through its ability to withdraw consent, which implies the ability to withdraw consent to retention. PIPEDA already limits the scope of personal information that can be collected, the purposes for collection, the requirement for consent, the ability to withdraw consent, and places limits on the retention of personal information. To date, these obligations have given Ontarians sufficient control over their personal information, and the ability to trigger the cessation of collection, use, disclosure and ultimate disposal in appropriate circumstances.

Should Ontario proceed with the right to deletion proposed in the whitepaper, it is critical that the right be subject to sufficient exceptions that balance disposal with other important social and economic objectives and practical considerations.

The organization must be able to retain information that may be required for legal or business purposes (to the extent that is appropriate in the circumstances), to comply with other requirements under privacy law, or with respect to an existing legal proceeding, inquiry or investigation (or one that could be initiated within an applicable statutory limitation period).

Even under the GDPR, the right to erasure applies only where the legal basis on which the processing was conducted no longer exists (and there are five bases for processing in addition to consent). Furthermore, it is balanced with a series of exceptions (such as when processing is necessary for freedom of expression, archiving purposes or other compelling legitimate grounds).

The law should not require organizations to dispose of personal information:

- that privacy law would otherwise permit the organization to retain (e.g., records of bad debt or poor payment history, which would be relevant to a subsequent transaction with the individual);
- that privacy law permits the organization to collect, use or disclose without knowledge or consent (e.g., personal information processed to prevent fraud); and
- that is required to give effect to a withdrawal of consent by the individual and permit the
 organization to continue to comply with laws respecting adherence to such requests (e.g., to
 comply with CASL or Unsolicited Telecommunications Rules).

As currently proposed in the whitepaper, the only exception that would permit the continued retention of personal information for legitimate business purposes (as opposed to in response to legal requirements) would be for an organization to spell out in its customer contracts the organization's legal right to retain all data subject to its retention policy, even after a disposal request. This would lead to lengthier, more detailed consumer agreements, working against the policy objective of focussing privacy policies on unexpected areas where a consumer has a meaningful choice.

6. Ensure adequate protections around automated decision systems without unduly restricting the beneficial use of these systems for consumers and organizations

We support greater accountability around the use of automated decision systems, as well as enhanced efforts to ensure consumers are aware of how automated decision systems may impact them.

It is important that requirements around the use of automated decision systems not be unduly restrictive, as this could impact Ontario's position in the global innovation ecosystem, as well as the availability of innovative goods and services for consumers by discouraging organizations from developing and leveraging automated or partially automated systems.

Enhanced transparency requirements around the use of automated decision systems, such as those proposed in the whitepaper (and under Bill C-11), would provide consumers with adequate protection in the context of automated decision systems

Harsher restrictions on the use of such technology outlined in the whitepaper – such as the proposed prohibition on automated decision systems - would put organizations in Ontario at a competitive disadvantage with respect to their counterparts in other jurisdictions, like the United States, that do not impose such restrictions. Furthermore, they will add unnecessary administrative burden for organizations – with the associated cost being passed along to consumers – without a compelling privacy protection benefit.

There are 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, Al helps organizations across Ontario improve accuracy and efficiency and reduce costs. For example, one of the CMA's media agency members is implementing an optimization tool that uses machine learning based on a decision tree to test, learn and optimize its offers 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, and better understand verbal queues. 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.

The bill's proposed right to explanation will be highly beneficial to support consumer understanding and awareness of automated decision systems. However, we suggest re-consideration of both the definition of ADS and the right to explanation outlined in the whitepaper, both of which are broader than what is necessary for effective privacy protection.

The overly broad definition of automated decision systems will result in the provision of unnecessary information to consumers, which works against the government's objective of streamlining privacy disclosures to consumers in order to allow them to focus on matters of greater concern. It would also result in a significant administrative burden on organizations. The definition itself should be narrowed to only those decisions that <u>materially</u> assist or replace human decision-making, and the element of "judgement" should be removed.

The proposed right to explanation in the whitepaper indicates that, on request by an individual (and regardless of whether there is any impact on the individual), an organization must provide an explanation of: (i) any prediction, recommendation or decision made using an automated decision system; and (ii) how the personal information used to make the prediction, recommendation or decision was obtained.

This requirement, as drafted, would capture a broad range of routine, micro decisions, the majority of which have no significant impact on an individual or potential to harm them (such as a call centre using automated decision systems to support call routing, or a website declining to serve copyright-protected content to a user in a jurisdiction where the website provider does not hold the rights to make that content available). The law would also capture a range of decisions for which similar transparency and explanation requirements do not apply when those decisions are made by humans. In this regard, it is important to note that while some automated decision systems might incorporate AI, many others do not. Many automated decisions are the result of programming that incorporates similar thresholds and instructions to those that might otherwise be given to human employees.

The requirement would result in large amounts of innocuous information being provided to consumers, making it difficult for them to determine what is most important. The requirement would also create a potential burden for companies dealing with large volumes of requests (including potentially automated requests), without a corresponding benefit for individuals.

Any new right to explanation should focus <u>only</u> on the use of automated decision systems that could have a significant impact on an individual, permitting them to engage if they feel they have been harmed. Furthermore, given the nature of data flows and automated decisions in practice, particularly with regards to machine learning, deep learning and neural nets, the explanation required by organizations should be "reasonable in the circumstances."

Organizations should provide <u>summary</u> information to individuals about the use of automated decision-making, the factors involved and where the decision is impactful, as long as it does not require organizations to reveal any confidential or proprietary commercial information, algorithms or procedures.

The approach could leave room for privacy commissioner guidance or industry best practices (codes or certifications) to support these requirements, including what explanation would be "reasonable in the circumstances".

Although we are supportive of Ontario pursuing the approach to transparency and explanation taken by Bill C-11 (with the above adjustments), we do not recommend Ontario pursue the additional proposals outlined in the whitepaper.

In particular, the proposed prohibition on automated decision-making is highly problematic, and will have negative implications for both organizations and consumers.

A regulatory response should be remedial, prohibiting or restricting only those activities where there is clear evidence of harm. It is far from clear that all forms of automated decision-making are problematic or warrant a regulatory response. In fact, automated decision-making includes a range of legitimate activities. As data becomes more complex, the use of automation is critical and beneficial. There are a growing number of helpful automated decisions being made each day, resulting in beneficial services for consumers, such as chatbots that provide consumers with relevant and personalized advice. Individuals are demanding faster, easier and more intuitive services and automation is central to the delivery of this promise.

Although the prohibition contains an exception to account for cases where automated decision-making is linked to the actual provision of a product or service requested by the consumer, the requirement for express consent for all other cases is disproportionate to the risk involved, and would offer little additional privacy protection – instead contributing to the considerable consent fatigue already felt by consumers.

It is also unclear how this provision is intended to apply to marketing activities that may be deemed to "significantly affect" people. This proposal may impose new obligations on the marketing community's ability to provide consumers with relevant, tailored and useful advertising.

In the case of marketing, profiling is intended to provide an individual with a more relevant experience, such as if a product or service is offered based on an individual's previous preferences and habits. Many organizations create a profile or use automated decision-making to target their marketing efforts, including using third-party analytic tools and software, such as cookies, pixels and beacons. This helps organizations provide consumers with the relevant products and services that they want or need. There is no basis for restricting this type of activity unless there is clear evidence of harm.

Under the GDPR, which places restrictions on <u>solely</u> automated decisions that produce "legal or similarly significant effects,", there is significant uncertainty by organizations in assessing "similarly significant effects," stifling innovation and resulting in industry confusion.

Transparency offers the most meaningful protection for consumers. Organizations should be transparent in their privacy policies about their use of third-party analytic tools and software to track, identify and target individuals to serve them relevant advertising. Where possible, they should also refer individuals to the opt-out mechanism accessible through the service provider's platform.

If concerned individuals are permitted to submit observations to the organization for review, an organization must have the discretion to determine whether to ultimately change its decision.

7. Preserve the ability for organizations to leverage de-identified and pseudonymized information for the benefit of consumers and organizations

De-identification and pseudonymization of personal information are longstanding practices that are commonly used by organizations to fulfill data minimization requirements and principles. These techniques are generally regarded as hallmarks of responsible data stewardship, particularly when organizations use them internally to analyze and extract key insights from data sets while protecting individual privacy. These best practices have long been viewed as important privacy-protective mechanisms by privacy commissioners across Canada, including the Information and Privacy Commissioner of Ontario (IPC), who have recommended their use when analysis and other processing does not require the use of individually identified data. Privacy laws should encourage, rather than discourage, such techniques.

It is important for privacy law to clarify that the simple act of de-identifying or pseudonymizing personal information is not, of itself, a use of personal information that requires individual consent. Like other non-substantive manipulations of data (e.g., truncation, encryption, creation of subsets of personal information from a larger sets), de-identifying or pseudonymizing personal information results in no detrimental impact on the individuals in question. In fact, many of these techniques serve to enhance privacy protection.

The government proposes to impose certain privacy law requirements on de-identified information, such as requiring the implementation of a privacy management program, or ensuring that adequate safeguards are in place to protect de-identified information, while not imposing other privacy law obligations and restrictions. Where there is a serious possibility of re-identification of de-identified data, there may be some merit to such a targeted approach to the application of privacy requirements. The advisability to proceed with this proposal ultimately depends on the details of such restrictions, which should be proportionate to an assessment of the context, the risk of re-identification, and the risk of any significant harms that could result from such re-identification.

We support the concept of a risk-based approach to the nature of the de-identification protocols that organizations would be required to implement. However, the proposed "proportionality of technical and administrative measures" provision must be reworded to, among other things, explicitly reflect the fact that assessing the efficacy and adequacy of any de-identification measures (as to whether they remove a serious possibility of re-identification), is necessarily a context-specific exercise, taking into account the sensitivity of the personal information in question, the proposed use and handling and the associated risk of re-identification and other related factors:

An organization that de-identifies personal information must ensure that the efficacy of any technical, and administrative or operational measures applied to the information are is proportionate to the purpose for which the information is de-identified and risk of reidentification in the circumstances, taking into consideration all relevant factors, including the sensitivity of the personal information.

There is no one-size-fits-all approach to de-identification for privacy purposes. As technology evolves, standards for de-identification will need to evolve. Organizations and consumers would benefit from having one set of common, practical standards for reliable de-identification that would protect personal information while supporting necessary and beneficial digital economic activity. Adhering to these standards should create a safe harbour for organizations, reducing or eliminating potential regulatory liability for failing to implement appropriate de-identification measures. This approach would encourage the use of de-identified information (thereby reducing privacy risk) and help pave the way for data-based innovation and the success of Ontario businesses in the digital economy. There is a significant opportunity for government to draw upon private sector work in this area.

The CMA supports the apparent objective of the proposed prohibition on re-identification, however, the proposed wording is overly broad, capturing a wide range of parties and circumstances without a compelling public policy rationale. Revisions are required to ensure that the organization in question is aware that it is re-identifying data that had been purposely de-identified, and additional exceptions are needed for situations such as those where data intended for internal analysis by an organization might be de-identified for security purposes or to comply with "need to know" data minimization principles.

It would be inappropriate to prohibit organizations from re-identifying data that they control and that they themselves de-identified. Today, organizations already use various forms of de-personalization/de-identification as security safeguards when engaging in data analytics etc. (thinking with data). If the insights are useful, they may decide to re-identify or use actual personal information to apply those insights (acting with data). We do not want to prevent or somehow cast doubt on the ability to do this, so the prohibition on "re-identification" must not apply to internal analytics/R&D.

As an example of the above, data or automation analysts may de-personalize/de-identify information for the purpose of identifying appropriate customer segments for marketing purposes, after which the organization identifies the audience/individuals from within the data set to whom they will communicate offers. Identifying information may not be required during the actual analysis/building of predictive models but would clearly be required to reach out to the targeted customers.

Under PIPEDA, re-identifying truly de-identified information may amount to collection, and any subsequent use or disclosure would certainly be subject to the law, including consent requirements. The same would be true under the approach proposed.

For questions or comments regarding this submission, please contact:

Sara Clodman

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

Fiona Wilson

Director, Government Relations fwilson@theCMA.ca

About the Canadian Marketing Association

The Canadian Marketing Association (CMA) strengthens marketers' significant impact on business in Canada. We provide opportunities for our members from coast to coast to develop professionally, to contribute to marketing thought leadership, to build strong networks across all economic sectors, and to shape positions advocated by the CMA 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. Our Consumer Centre helps Canadians better understand their rights and obligations as consumers in a variety of areas, including how to protect their personal information, avoid being a victim of fraud, identify spam, reduce the amount of print mail they receive, opt out of online ads, and protect themselves from Covid-19 scams.