CANADIAN MARKETING ASSOCIATION
CMA

1 Concorde Gate, Suite 607, Toronto, Ontario, M3C 3N6
416.391.2362 ● theCMA.ca

Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics

Review of the *Personal Information Protection and Electronic Documents Act*

May 2017

While some argue that the consent model is dead, CMA believes that the model upon which the *Personal Information Protection and Electronic Documents Act* (PIPEDA) is built, is alive and well. Certainly, we acknowledge that with the proliferation of technological advancements over the last ten years alone, some consumers may, at times, feel overwhelmed by the various avenues of data collection and, perhaps, with understanding terms and conditions to which they are agreeing. Others may simply not take the time to properly inform themselves as they trust companies will do the right thing and be accountable for their data processing.

Indeed, the current consent model faces practical challenges. However, there are viable solutions available within the current legislative framework that will protect privacy and support responsible use of personal information (PI) by businesses. In seeking to find creative solutions, CMA believes that the interpretation of what is reasonable under PIPEDA must evolve with the times to make full use of existing options. However, to be clear, such an evolving approach does not require legislative amendment; PIPEDA already provides the necessary tools to address some of the challenges that technology poses to privacy, and as such legislative changes should be kept to a minimum.

Amendments to PIPEDA

1. The recent amendments contained in the *Digital Privacy Act* (the "Act"), offer guidance to organizations regarding consent requirements in various contexts. The Act also introduced additional protections such as mandatory breach notification requirements, and extended the powers of the Privacy Commissioner to enter into compliance agreements with organizations. While some may argue that further amendments to the law are necessary, CMA strongly cautions against this approach for two main reasons:

a) First, the effectiveness and impact of the amendments passed in 2015 need to all come into force and be assessed over a longer period of time. In this regard, the new breach notification provisions have not even been proclaimed in force. It would not be recommended, nor efficient, to create new laws and regulations without first understanding the outcomes of those amendments recently passed by Parliament.

b) Second, any review of the OPC's investigations, case resolutions and published findings demonstrate that PIPEDA works well in its current form. We need to look at ways of addressing current challenges not through more regulation, but by enhancing the efficacy of PIPEDA through the innovative use of the tools that are provided in the existing law.

Consent

2. PIPEDA is based on flexible principles rather than prescriptive rules. This translates into legislation that, by deliberate design, is capable of accommodating various business models, new technologies, and evolving cultural norms and reasonable expectations. PIPEDA's technology-neutral and principle-based structure has withstood the test of time, and can continue to provide the necessary framework for 'Big Data', the 'Internet of Things', and data-driven innovation provided that the interpretation of PIPEDA is not rigid or fixed in time.

3. It must be recognized that innovation remains a critical component of business development in today's markets and that the need of organizations to collect, use and disclose PI is key to business success and Canadian competitiveness. Companies are under mounting pressure to continuously innovate and introduce new products and services ever faster. Consumers expect organizations to provide and continually enhance personalized services and to introduce new products, services or new strategies

that will benefit consumers. Consequently, we need a privacy law framework that encourages and guides innovation, as well as privacy regulators that embrace this approach when it comes to interpreting PIPEDA, just as businesses and the rest of society embrace innovation.

4. With business models becoming increasingly focused on innovation and greater customization of products and services in response to consumer expectations, the constraints on the consent-based regime must be recognized. The challenges posed to meaningful consent - smaller screens, privacy policies that are rarely read, and other device restrictions – sometimes render seeking consent impossible or ineffective. The right mix of individual choice and a robust accountability framework will strengthen privacy and consent, while continuing to provide for the flexibility required to enable innovation. While consumer consent should still be regarded as an important element in privacy law, shifting to more of a risk-based model where organizations are given more freedom but also more accountability and responsibilities concerning consumer data, would modernize the Canadian privacy arena.

5. It is important to highlight that the vast majority of Canadian organizations strive to be transparent and open. Processing data responsibly not only flows from the requirement to comply with the law, but is also a result of corporate culture, a general adherence to societal values, and perhaps most important of all, a desire to satisfy customers. In some cases, organizations promote their privacy programs to enhance their brand equity or position themselves more favourably in the marketplace.

6. Privacy needs to be interpreted in its social and technological context while recognizing that the context is changing. Individual direct control over PI through notice and express consent remains relevant in many situations, but we must also to acknowledge the increasing need for reliance on implied consent and accountability frameworks to ensure the fair and reasonable treatment of PI. Traditional notions of consent have shifted due to business models that are based on providing online services that are supported fully, or in part,by advertising revenue and which depend on interest-based advertising and data collection techniques.

7. In fact, the current over-reliance on notice and express consent does a disservice to individuals and potentially exposes them to harm. The reality is that most individuals do not read complex and lengthy notice and simply sign or click to obtain the good or service or complete the transaction in question. It is a somewhat artificial construct to assume that all individuals read and understand all privacy notices and carefully consider the privacy risks and benefits before deciding whether to provide their consent. Enhancing and streamlining notices and the consent process may go some way to addressing this issue, but these enhancements are not the full answer in a world of growing complexity. It is better and more honest to acknowledge common individual behaviour, acknowledge the limits of enhanced consent processes and embrace other options available under PIPEDA, provided that we avoid creating prescriptive or inflexible new rules. The CMA recommends placing greater accountability obligations on organizations and widening the scope for the use of implied consent, and the disclosures required for such consent, as this actually enhances the protection of privacy and reduces the burden on the individual.

8. Special consideration should be given to the collection, use and disclosure of PI respecting vulnerable groups. CMA has long recognized the importance of this and appropriate treatment of such groups is required by the CMA's Code. In particular, CMA Members believe that special attention needs to be given to the sensitive issues surrounding data-collection and marketing to children and to teenagers. See CMA's guidelines on marketing to children and teenagers. Children and teenagers, in particular, are increasingly interacting with the Internet. They share a great deal of PI on social media and other

Internet-based platforms. Protecting vulnerable groups starts with good educational tools and programming. Over the long-term there is also a need for some level of personal accountability. As children become teens, and then adults, they need to be better equipped to take this on.

Alternatives to consent – De-identification/ Anonymization

9. Issues surrounding anonymization and de-identification techniques and the status of anonymized and de-identified data are becoming critical issues in Canada, and in other jurisdictions. As technology evolves, the requirements for robust anonymization and de-identification must also evolve, and keep up with the times. This may mean an 'evergreen' approach to OPC guidance on anonymization and de-identification. Alternatively, current standards for anonymization and de-identification may be well-suited to a code of practice, where business, academia, civil society and other stakeholders can work to establish and periodically update a practical basis for effective de-identification.

10. Similar to the analysis to be made when determining what form of consent to use, risks of re-identification need to be considered. Further, similar to the determination of the appropriate safeguards to protect PI, we need a realistic approach to the use of de-identification. The required level and robustness of de-identification should not be based on theoretical possibilities, but should reflect the sensitivity of the information if re-identified and the likelihood of re-identification, shifting focus to the risk of harm as a key factor in setting standards

11. CMA supports more effort and collaboration to establish guidance or standards around de-identification; however, we disagree with any proposal that consent be required for the collection, use and disclosure of de-identified data. Reliable de-identification, in and of itself, poses no risk of harm and has no negative impact on the individual to whom the PI originally related. Not only is this a useful safeguarding technique, but de-identification is also one of the most privacy-protective mechanisms available for organizations to engage in data analytics and innovation in the digital economy.

12. The 'Anonymization: Managing Data Protection Risk Code of Practice' (the "UK Code"), released by the UK's Information Commissioner's Office, is a great example of a code of practice based on a self-regulated accountability model. The UK Code provides practical advice which indicates that effective anonymization of PI is not only possible, but desirable. When combined with robust and effective codes of practice, anonymizing data effectively and safely has wide reaching social benefits. While this Code was developed in the UK, the principles and guidance that it offers can easily and efficiently be adopted in Canada.

Alternatives to consent – Legitimate Business Interests

13. An effective accountability framework needs to allow for more flexibility around lawful processing of data for legitimate business interests. While processing for legitimate purposes is currently permitted under PIPEDA, some would argue that for greater certainty, it should be permitted without individual consent in appropriate circumstances. The CMA supports broadening permissible grounds for processing under PIPEDA to include legitimate business interests subject to a balancing test. Data governance principles (as reflected in the OPC's accountability guidelines), together with the reasonable purposes test in section 5(3) of PIPEDA, provide a roadmap for "responsible use" of data and fair processing for legitimate business interests.

14. The current EU framework offers an example of how legitimate interests can be used as a ground for lawful processing without consent, while still providing strong privacy protections to individuals. The Data Protection Directive, as well as the General Data Protection Regulation (GDPR) which is set

to replace the Directive by 2018, specify that in some circumstances personal data may be processed without the consent of the data subject. Article 6(1)(f) of the Regulation states that:

> *"Processing of personal data shall be lawful only if […] the following applies:*
> *…*
> 1. *f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child …"*

Pursuant to this provision, it is possible to use personal data where the party processing the data has a 'legitimate interest' in doing so. It allows controllers and processors alike to process data on the 'legitimate interests' ground even for purposes that are incompatible with the original purposes of the processing, provided that the interests or the fundamental rights and freedoms of the individual are not overridden. While the CMA does not advocate for this exact provision to be introduced into Canadian privacy legislation, we believe that a version of this principle can be applied in the Canadian context based on Schedule 1, section 4.3.3.

15. Recital 47 of the GDPR also makes it clear that marketing-related interests constitute "legitimate interests" and states that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". This interpretation of the term "legitimate interest" also reflects the US approach to data protection, given that the "reasonable expectations of users" are the central point of departure for any consideration of this issue in the future. While such an approach is indeed permitted under PIPEDA and has been expressed in certain OPC findings, uncertainty remains.

16. To conclude, the CMA recommends that the ability to process PI for legitimate interests should be expressed more explicitly in Canada. More specifically,

> The OPC, in collaboration with industry, could develop specific guidelines with respect to legitimate business interests in the context of s. 4.3.3, recognizing legitimate purposes beyond simple fulfillment of an order. These actions by the OPC would allow many business models in place in the online and offline industries alike to no longer require data subjects to give their 'express' consent to the use of their data for legitimate business purposes. Rather, they would be relying on implied consent provided that organizations stay within the bounds of their users' "reasonable expectations" that would include sufficient notice and transparency tailored to the circumstances and context. Similarly, with respect to the collection of implied consent, the OPC could explicitly recognize a range of common and legitimate business activities as being within the reasonable expectations of consumers, as contemplated by s. 4.3.5, obviating the need to disclose these purposes in detail in all privacy policies. To be clear, the CMA believes that processing of data for legitimate purposes can already be done through the "legitimate purpose" section in 4.3.3 and the "reasonable expectations" section in 4.3.5, whether relying on express or implied consent.

17. It may be that the exercise of the legitimate business interests provision can be further supported by a recognized ethical assessment process, which could be part of or supplemental to the guidelines or codes mentioned above.

Self-regulation - Codes of Practice and Privacy Trustmarks

18. In the current legislative regime of PIPEDA, self-regulation is an added element or enhancement. It is also flexible enough to adapt to changing societal views as well as advertising media and techniques. Societal norms are constantly evolving, to the point that the values and opinions of a group of millennials may differ considerably from those of a group of retirees, depending of course on the issue. Businesses use self-regulation to decrease risks to consumers, increase public trust, and combat negative public perceptions. So self-regulation often serves to support existing laws by reflecting certain interpretations and in some specific contexts supporting supplemental rules to govern the behavior of organizations. The two complement each other: the law lays down broad principles (e.g., that advertising should not be misleading), while self-regulatory codes, because of their greater flexibility, can deal quickly and efficiently with the details and be changed or updated as required.

19. The CMA is highly supportive of the creation of targeted industry codes of conduct or practice. Section 24 of PIPEDA explicitly calls for the Commissioner to: *(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 and 10*. Targeted codes of conduct can be expected to provide additional visibility into the activities of organizations and provide a developing standard of best practices. They also provide practical targeted guidance and a process for evolving the guidance over time in the face of significant technological change. The innovative use of codes and other tools to give guidance for the fair and reasonable collection, use and disclosure of PI will allow the protections afforded by PIPEDA to evolve with society.

20. The CMA Code is an example of a code of conduct that has guided with great success the business practices of many organizations operating across different industry sectors. Recognized as the foundation of the marketing community's self-regulation and a benchmark for effective self-regulation, the CMA Code has evolved over the years to become the best practices document for Canada's marketing community. Governments and regulatory bodies have often referred to the document when enacting legislation and have included key provisions of our Code in those statutes and regulations. As well, the media often reference the CMA Code as an example of best practices for business.

21. Industry-led self-regulatory trustmarks can also be appropriate in certain cases. The Ad Choices program for interest-based advertising, for example, is an effort to give consumers more information and choices about the advertising they receive online. The program requires participating companies to clearly inform consumers about their data collection and use practices in order to enable consumers to exercise greater control over how their online browsing data is used and the types of ads they see. Launched in September 2013, the program was developed by the DAAC, a not-for-profit consortium of eight leading advertising and marketing associations in Canada. The DAAC and the Ad Choices program is part of a global program whereby the Ad Choices icon and choice mechanisms are offered in 34 countries and 26 languages. The program is based on six key principles consistent with Canadian privacy laws, including transparency, choice and accountability. For such programs to be truly effective they must be industry led, requiring industry buy-in and adoption.

Enforcement

22. The current enforcement powers of the OPC, including recent enhancements made by the Digital Privacy Act, will enable the OPC to continue to effectively enforce any evolution of the rules governing consent in an era of technological change. The focus on resolving complaints through negotiation and persuasion continues to work very well and is bolstered by the use of mediation and conciliation if appropriate. If voluntary co-operation is not forthcoming the Commissioner has the power to summon

witnesses, administer oaths and compel the production of evidence. Further, the Commissioner has the power to enter into compliance agreements if necessary, or to take matters to the Federal Court and seek a court order to rectify situations that remain unresolved.

23. The ombudsman model under which PIPEDA operates has been highly effective and has resulted in a high level of voluntary compliance from Canadian businesses, allowing the OPC to successfully resolve 84% of cases within the last 5 years. Given this success rate, additional enforcement and order making powers are not required to give the OPC the regulatory teeth it seeks.

24. Additionally, and of significant importance to the OPC's mandate of advocating for the privacy rights of Canadians, the ombudsman model of oversight permits the OPC to protect and promote the privacy rights of individuals not only through enforcement powers, but also through positive and proactive engagement with industry associations and organizations seeking guidance on compliance and emerging privacy issues. Organizations are innately less forthcoming, or apt to consult in a cooperative way with a regulator that has the direct power to impose monetary penalties or issue orders against those organizations.

Conclusion

CMA has always been and will always continue to be supportive of privacy legislation that protects individuals' privacy and security. PIPEDA needs to continue to offer robust privacy protections for Canadians. At the same time, it must be recognized that PIPEDA was also created to "support and promote electronic commerce". Given today's highly competitive markets and the importance that commerce plays in promoting a healthy national economy, innovation remains a critical component of business development. The need of organizations to collect, use and disclose PI is key to business success and Canadian competitiveness. As such, PIPEDA needs to remain flexible for business in the face of rapidly evolving technologies, business models and customer privacy expectations.

About the CMA

The Canadian Marketing Association embraces Canada's major business sectors and all marketing disciplines, channels and technologies. The Association's members make a significant contribution to the economy through the sale of goods and services, investments in media and new marketing technologies and employment for Canadians. Against this backdrop, the Canadian Marketing Association is the national voice for the Canadian marketing community, with CMA's advocacy efforts designed to create an environment in which responsible marketing can succeed.

For questions regarding this submission, please contact Wally Hill at whill@theCMA.ca or Cristina Onosé at conose@theCMA.ca

** END **