CANADIAN MARKETING ASSOCIATION
CMA

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

Feb 29, 2024

Joël Lightbound MP
Chair, Standing Committee on Industry and Technology
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

E-mail: INDU@parl.gc.ca

A More Effective Approach to Protecting Young People's Data:
Amendment needed to the *Consumer Privacy Protection Act*

Dear Chair,

The Canadian Marketing Association and its members have long recognized the importance of keeping young people safe, which is why sections of the Canadian Marketing Code of Ethics and Standards are dedicated to outlining rules and best practices for marketing to kids.

As the INDU Committee completes is study of Bill C-27, we note that much of the discussion during the hearings about minors' data – by MPs and witnesses alike – was focused on online hate, bullying and sexual victimization, all of which falls outside of the scope of a commercial privacy law.

With the tabling this week of the *Online Harms Act* (Bill C-63), there is now a law before Parliament where these matters can be more appropriately and directly addressed. As a result, it is important that the INDU Committee not add provisions to Bill C-27 that would overlap with, or contradict, Bill C-63.

At the same time, the scope of the provision in Bill C-27 must be modified to avoid the overcollection of personal data of all Canadians in a commercial context. As drafted, the CPPA would require organizations to collect and verify some of the most sensitive personal information of Canadians – their birth dates, and possibly government-issued identifiers or credit card information – simply to determine whether their customers were over the age of majority to allow the organization to be able to demonstrate compliance with the CPPA.

The vast majority of organizations do not know – nor do they need to know – the age of their customers. They treat all customers the same, and there is little risk of harm to their customers – even if, unbeknownst to the organization, they happen to be minors.

For example, if an individual of any age goes online to purchase a coffee mug or a pair of jeans, or even just to browse through those items on a company's webpage, the company might collect and retain information about that transaction, and use the information to direct advertising to that individual with respect to similar products, such as a travel mug or a belt. Using data in this way poses no threat of harm to the customers – even if they are minors, so there is no benefit in having the company verify, and keep records of, the age of the person making the purchase.

Ironically, in the majority of cases, the collection and retention of authentication information may pose greater potential harm to customers than serving a relevant ad. A fundamental principle of privacy law is to minimize the collection and retention of personal information, in part to minimize unnecessary risks, such as having the information compromised through a zero-day hacking attack or similar breach incident that could arise, despite the best efforts of the organization to secure the data. The implications of a data security incident can be problematic for personal information that an organization reasonably needs to retain for business purposes, such as basic transaction records; but the results can be both damaging and entirely unnecessary where an incident involves sensitive data that is collected and retained solely to demonstrate compliance with a broad-brush legal requirement without offering significant benefits to the individuals. Once a company collects this information, it would remain in their records in case the company needs to demonstrate in the future what information it relied on to determine whether the person was a minor.

…/2

To remedy this concern, we propose that the CPPA be amended to protect children and youth in a manner consistent with the approach taken by the Children's Online Privacy Protection Act in the US, and by privacy laws in California and the EU. Specifically:

- Obligations related to minors' data under the CPPA must 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. It must not apply to organizations that may only incidentally and unknowingly process the data of minors, as conducting normal business activities would not bring potential harm to minors, and the very collection and retention of their ages and other age verification/authentication data carries its own risks.
- Organizations must not be required to treat mature minors in the same way as young children, given that mature minors 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). Organizations should be able to take into account the age and capacity of the minor, and the potential for real harms that need to be addressed.

The following amendments would achieve these objectives:

~~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.

Thank you for your leadership on the CPPA and made-In-Canada approach to privacy.

Sincerely,

Sara Clodman,
Chief Public Affairs and Governance Officer
Canadian Marketing Association