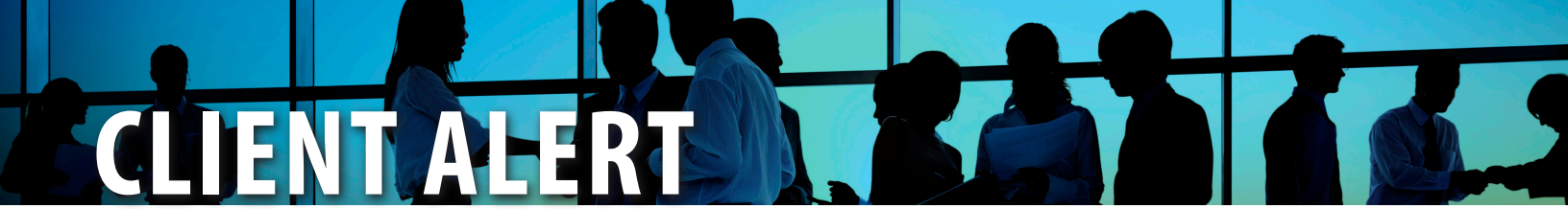


CANADIAN DATA PRIVACY LAWS ARE CHANGING. IS YOUR BUSINESS READY TO KEEP UP?

By Carly J. Walter, Dan A. Poliwoda, and Wendy G. Hulton

On November 17, 2020, Canada's federal government introduced a bill to enact new legislation that would strengthen protections for individuals from privacy loss due to the failures and limitations of corporate consumer privacy measures. The proposed legislation, known as the *Consumer Privacy Protection Act* ("**CPPA**"), would be the first major overhaul of Canada's privacy law rules on the private sector since the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") came into force in April 2000.

If the CPPA passes into law, it will replace the PIPEDA, currently the leading federal privacy law governing federally-regulated corporations and private sector companies in Canadian provinces and territories that do not have their own privacy legislation. The bill to enact the proposed legislation, including the CPPA, is at first reading. The next step would be for it to go to second reading and then to a committee for further review and recommendation, before ultimately receiving royal assent and passing into law.

KEY CHANGES PROPOSED TO CANADA'S CONSUMER PRIVACY FRAMEWORK

The CPPA proposes several key changes to Canada's corporate consumer privacy rules

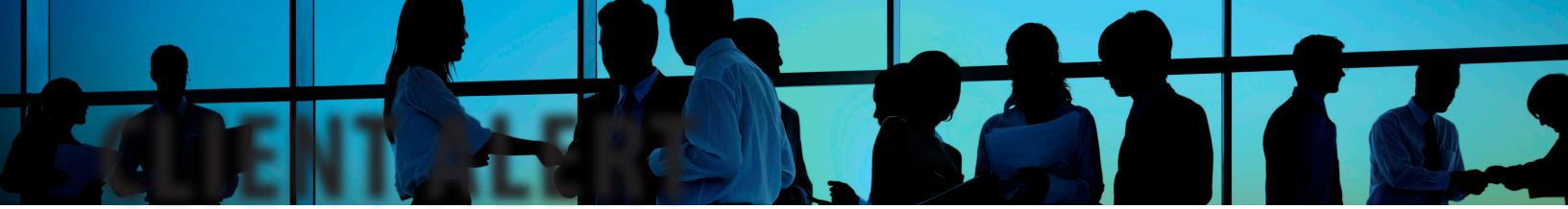
- First, the CPPA imposes **administrative penalties** of up to 3% of global revenue or $10 million CAD for non-compliant organizations. In addition, the **CPPA expands the range of privacy-related offences**; penalties for certain offences under the CPPA subject non-compliant organizations to a maximum fine of 5% of global revenue or $25 million CAD.
- Second, the CPPA creates the **Personal Information and Data Protection Tribunal** (the "**Tribunal**"). The Tribunal is empowered to issue penalties and fines under the CPPA upon recommendations from the Office of the Privacy Commissioner of Canada (the "**Commissioner**"). The Tribunal will also adjudicate appeals from the Commissioner's orders.
- Third, the CPPA **broadens the order-making powers of the Commissioner**. Under the CPPA, the Commissioner may order an organization to:
  - Take measures to comply with the CPPA;
  - Stop doing something that is in contravention of the CPPA;
  - Comply with the terms of a compliance agreement that has been entered into by the organization; or
  - Make public any measures taken or proposed to be taken to correct the policies, practices, or procedures that the organization has put in place to fulfil its obligations under the CPPA.

Furthermore, as mentioned above, the Commissioner may recommend that the Tribunal issue a fine or penalty on an organization for violating certain provisions in the CPPA.

- Fourth, the CPPA **clarifies the rules for valid consent to data sharing**. To obtain valid consent under the CPPA, an organization must provide individuals with certain information before the individual can consent to having his or her data collected. Specifically, the information that organizations must provide includes the purpose(s) of the collection, use, and disclosure, the "reasonably foreseeable consequences of the collection, use or disclosure," the types of personal information involved, and the "names of any third parties or types of third parties to which the organization may disclose the personal information." Implied consent will be acceptable in certain circumstances, taking into account the individual's reasonable expectations and the sensitivity of the personal information.
- Fifth, the CPPA **enhances consumers' control over the personal information organizations collect**. Under the CPPA, individuals are allowed to request disposal of their personal information, and individuals are allowed to withdraw consent to the use of their information. Individuals will also be granted data mobility rights, namely the ability to transfer their personal information from one organization to another. However, it should be noted that **in certain circumstances organizations will be allowed to use de-identified information without an individual's consent**. For example, the CPPA would allow organizations to disclose de-identified data to public entities in certain circumstances for "socially beneficial purposes."
- Sixth, the CPPA introduces **new transparency rules for "automated decision systems"** (aka algorithms) organizations employ "to make predictions, recommendations or decisions about individuals that could have significant impacts on them." The provisions provide individuals the right to request that organizations explain how a prediction, recommendation, or decision was made by an automated decision-making system and explain how the information was obtained.

GLOBAL CONSIDERATIONS

If the CPPA passes into law, Canada would be following many



other jurisdictions that have strengthened and updated their privacy laws in recent years, including the European Union.

In 2018, the European Union implemented the General Data Protection Regulation (the "**GDPR**") to strengthen and modernize its corporate consumer privacy regulations. The rules and regulations contained in the GDPR inspired many of the recommendations in the House of Commons Standing Committee on Access to Information, Privacy and Ethics' 2018 report entitled *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act* (the "**Report**"). In turn, the Report influenced many of the new rules and regulations for corporate consumer privacy measures in the CPPA.

The GDPR's influence on the CPPA is also relevant to the extent that the CPPA would harmonize between the corporate consumer privacy rules in the European Union and Canada. Since the European Union implemented the GDPR in April 2018, Canadian companies have faced legal obstacles to doing business in the European Union. The GDPR imposes strict rules on corporate consumer privacy measures, and until now, most Canadian companies' consumer privacy measures coincided with the comparatively lower standards in the PIPEDA. By bringing their measures in line with the CPPA, Canadian companies doing business in the European Union would likely avoid many of the legal obstacles posed by the GDPR's standards.

IMPACT ON PROVINCIAL LEGISLATION

The impact of a new federal legal framework for assessing corporate consumer privacy measures on provincial data privacy legislation remains unclear at this point. In fact, many provinces are currently in the process of revising their own rules regarding consumer data privacy. Quebec has introduced Bill 64, which brings its private sector privacy law close to the GDPR. Ontario has conducted consultations to establish privacy sector privacy protection laws that might be stronger than the PIPEDA, while British Columbia has started a review on improving its private sector privacy law.

STEPS ORGANIZATIONS SHOULD BE TAKING NOW

While companies can expect a transition period to bring their practices in line with the new legislation, we recommend companies take the following steps:

- **Affirm** the company's commitment to ensuring consumer data privacy by reminding employees that data should not be misused under any circumstances, and emphasize that current privacy measures should be taken seriously;
- **Organize** a team to review the current state of the company's consumer data collection practices and privacy measures;
- **Identify** where current practices and measures may be falling short of current statutory requirements, and where improvements can be made to enhance consumer data privacy and reduce the risks of data privacy breaches;
- **Develop** a plan to rectify any non-compliance with current statutory requirements and improve current practices and measures;
- **Implement** rectification and improvement plans; and
- **Prepare** current procedures for additional changes by regularly monitoring and periodically revising consumer data collection practices and privacy measures.

CONCLUSION

Private sector companies in Canada should pay close attention to changes to the draft legislation as it moves through Parliament. Though it remains to be seen which aspects of the draft legislation will be adopted, what is clear is that Canadian privacy law is changing, and most companies will find it necessary to change their consumer data collection practices and enhance privacy measures in light of the stricter requirements and stiffer penalties included in the CPPA.

ABOUT THE AUTHORS

Wendy G. Hulton is a Member in Dickinson Wright's Toronto office. She can be reached at 416.777.4035 or whulton@dickinsonwright.com.

Carly J. Walter is an Associate in Dickinson Wright's Toronto office. She can be reached at 416.646.6877 or cwalter@dickinsonwright.com.

Dan A. Poliwoda is a Law Student in Dickinson Wright's Toronto office. He can be reached at 416.646.6870 or dpoliwoda@dickinsonwright.com.