Highlights of the Canada Digital Privacy Act 2015

Wednesday, June 24, 2015

On June 18, 2015, the Canadian Parliament passed the Digital Privacy Act (DPA), Senate Bill S-4, into law. The DPA amends Canada’s federal data protection statute, the Personal Information Protection and Electronic Documents Act (PIPEDA) in important respects, including introducing a new data breach notification requirement (which is not yet in force) and making other material changes to PIPEDA. This post summarizes key changes to PIPEDA brought about by the DPA.

Summary of Key Provisions

- **Graduated consent standard.** The DPA introduces a graduated standard - some have referred to a "sliding scale" - for obtaining valid consents. The DPA stipulates that an individual's consent will only be valid "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." The upshot of this change is that organizations subject to PIPEDA will need to simplify their consent documentation and online terms when receiving data from less sophisticated individuals in order to ensure consents are valid.

- **New consent exceptions.** The DPA also introduces several additional exceptions covering PIPEDA’s consent and knowledge requirements. Examples of the new exceptions include when personal information is produced by an employee in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced, and when using and disclosing personal information to another organization in connection with a contemplated business transaction, such as a merger or acquisition, provided that the organizations enter into an agreement that ensures that the information will only be used for purposes of the transaction, be subjected to appropriate security safeguards, and returned or destroyed if the transaction does not proceed. (In the event the contemplated business transaction completes, the DPA makes clear that the information may continue to be used, provided the organizations enter into an agreement containing certain commitments with respect to the information, the information is necessary for continuing the business, and one of the organizations informs the relevant individuals within a reasonable time after completion that their information has been shared.)

- **Data breach notification.** The DPA introduces a new mandatory data breach notification requirement, which applies to organizations subject to PIPEDA when "...any breach of security safeguards involving personal information under [that organization’s] control [occurs,] if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.” If there is a “real risk of significant harm to individuals,” then the requirement also mandates notification to individuals. Where an organization fails to notify the Commissioner or record a breach, where required to do so, it will be guilty of an offence and liable to be fined up to $100,000 Canadian Dollars. However, this data breach notification regime will not take effect until the Canadian government issues implementing regulations. (Any such regulations will not be enacted until a consultation involving stakeholders and the Office of the Privacy Commissioner has taken place.)

- **Expansion of “Business Contact” PIPEDA Exemption.** PIPEDA originally excluded an employee’s “name, title or business address or telephone number” from the definition of “personal information”. The DPA revises the definition of “personal information” to refer only to “information about an identifiable
individual,” and introduces a separate definition of the term “business contact information.” The DPA also then uses this newly defined term in a specific “business contact” exemption provision, which excludes from PIPEDA use of “business contact information” for the purpose of communicating or facilitating communications with an individual in relation to their employment, business or profession.

- **Powers of the Commissioner.** The DPA also enhances the powers of the Canadian Privacy Commissioner in several respects. Most significantly, it enables the Commissioner to form “compliance agreements” with organizations that the Commissioner has reasonable grounds may have committed, or is about or likely to commit, a breach of the PIPEDA. Such agreements may contain any terms the Commissioner deems necessary to ensure compliance, and the Commissioner may go to courts to ensure compliance with the agreement’s terms if needed.

© 2019 Covington & Burling LLP