Canada's New Digital Privacy Act: A Welcome Upgrade of the Personal Information Protection and Electronic Documents Act

By Kelly Friedman and Tamara Hunter, of DLA Piper (Canada) LLP, and Jim Halpert, of DLA Piper (USA) LLP.

Canada has had federal private sector privacy law for over 14 years. The Personal Information Protection and Electronic Documents Act ("PIPEDA") came into effect in Canada in 2001, and it provides general protection for personal information collected, used or disclosed by private sector organizations in connection with commercial activity.

PIPEDA is not specific to any industry sector and applies to a variety of organizations, including business corporations, trade unions and non-profits, but only to the extent those organizations are engaged in commercial activity.1 PIPEDA applies within the Canadian provinces, unless a province has enacted its own "substantially similar" privacy legislation.

On June 18, 2015, Canada's Digital Privacy Act entered into effect (see WDPR, June 2015, page 4).

How does the Digital Privacy Act change the privacy landscape in Canada?

First, the Digital Privacy Act is really just the name given to the statute which amends and augments PIPEDA. While PIPEDA has been given a "makeover," it remains the primary federal private sector privacy statute in Canada.

Second, most of the amendments to PIPEDA2 involve changes which have been recommended for some time. These welcome upgrades bring PIPEDA closer to the provincial counterpart legislation in British Columbia and Alberta, and to data protection law in the rest of the world. This harmonization is a benefit to business.

Finally, the most significant change to PIPEDA brought about by the Digital Privacy Act is the requirement for information security breach notification in defined circumstances and related monetary penalties for failure to notify. While the monetary penalties for breach of the notification provisions are potentially stiffer, the "risk trigger" or threshold for notification is relatively high.

Overall, while businesses outside Canada certainly need to be aware of the changes to PIPEDA, and adjust their policies and practices accordingly, there is no cause for major alarm arising from the Digital Privacy Act.
The new breach notification provisions, which are not yet in force, have significant teeth. Fines of up to $100,000 per violation may be imposed when an organization knowingly violates the breach notification requirements.

Changes Long Time Coming

It has been a long time coming, but PIPEDA has finally received a makeover, including new data breach notification provisions, with the enactment of the Digital Privacy Act.

In the Canadian private sector, the federal PIPEDA applies to federal works, undertakings and businesses (for example, chartered banks, telecommunications companies, airlines, railways and other interprovincial undertakings), as well as provincially regulated businesses in provinces that do not have adequately similar privacy legislation.

The new breach notification provisions, which are not yet in force, have significant teeth. Fines of up to $100,000 (U.S.$78,615) per violation may be imposed when an organization knowingly violates the breach notification requirements.

The legislated trigger for notification is a real risk of significant harm to an individual. In assessing the risk, organizations must have regard to factors such as potential humiliation and damage to relationships, as well as potential financial harm to affected individuals.

Fundamental Amendments to PIPEDA

The Digital Privacy Act amends PIPEDA in several important ways. The fundamental changes relate to the following:

- Specifying how to obtain valid consent for the collection, use or disclosure of personal information;
- Permitting the disclosure of personal information without the knowledge or consent of an individual for the purposes of:
  - identifying an injured, ill or deceased individual and communicating with his or her next of kin;
  - preventing, detecting or suppressing fraud; or
  - protecting victims of financial abuse;
- Permitting organizations, for certain purposes, to collect, use and disclose, without the knowledge or consent of an individual, personal information:
  - contained in witness statements related to insurance claims; or
  - produced by the individual in the course of his or her employment, business or profession (this is sometimes referred to as "work product");
- Permitting organizations to use or disclose, without the knowledge or consent of an individual, personal information for several purposes related to prospective or completed business transactions;
- Requiring organizations to notify affected individuals and organizations of certain breaches of security safeguards that create a real risk of significant harm and to report them to the Privacy Commissioner;
- Requiring organizations to keep and maintain a record of every breach of security safeguards involving personal information that is under their control;
- Creating offences in relation to the contravention of notice obligations respecting breaches of security safeguards;
- Extending the period within which a complainant may apply to the Federal Court for a hearing on matters related to a privacy complaint;
- Requiring that the Privacy Commissioner may, in certain circumstances, enter into a compliance agreement with an organization to ensure compliance with the sections of the act to protect personal information in the private sector; and
- Expanding the information that the Privacy Commissioner may make public if he or she considers that it is in the public interest to do so.

These amendments make PIPEDA increasingly similar to the British Columbia and Alberta private sector privacy statutes. The exceptions relating to employment relationships and to business transactions will provide greater clarity and practical direction for many organizations.

Some Amendments Controversial

However, some of the amendments to PIPEDA are controversial. The requirements for valid consent now state that the consent of an individual 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.

2007/15 COPYRIGHT © BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. W2 2015 INT. ISSN 1473-3579
Some commentators are concerned that the exemptions in which consent is obtained are too broad, unclear, and have led to the erroneous procedures, which sought to include the consent statements in their personal information, subject to limited exceptions. 10

On the other hand, PIPEDA now includes additional exceptions in which an organization is unable to direct personal information without consent of the individual, including with respect to investigations regarding suspected copyright infringement. While this is a step in the right direction, it would perhaps be too difficult for them to fight in Canada.

Further, privacy advocates have raised strong opposition to the expansion of information to include real time monitoring of Canadian citizens and businesses across the country. For example, the Digital Privacy Act will require organizations to notify individuals whenever personal information is involved and, whether an individual opts to disclose personal information without consent of the individual, including with respect to investigations regarding suspected copyright infringement. While this is a step in the right direction, it would perhaps be too difficult for them to fight in Canada.

The breach notification provisions in the Digital Privacy Act are quite similar to the breach notification provisions in the Alberta Personal Information Protection and Privacy Act as matters expressly excluded from provincial authority under s 91 of the Constitution Act as matters within federal authority (e.g., banks, airlines), matters expressly excluded from provincial authority under s 92 (e.g., grain elevators).

On the other hand, PIPEDA now includes additional exceptions in which an organization is unable to direct personal information without consent of the individual, including with respect to investigations regarding suspected copyright infringement. While this is a step in the right direction, it would perhaps be too difficult for them to fight in Canada.

Digital privacy experts have raised concerns that copyright holders will take advantage of these new provisions to inappropriately target suspected copyright infringers. Copyright holders see this as a welcome amendment, because digital copyright infringers have posed for which his or her personal information will be collected, used or disclosed.

The breach notification provisions will come into force with the re-enactment of the Ontario Privacy Act, SA 2003, c P-6.5) and Quebec (An Act respecting the protection of personal information in the private sector, 92(10) (PIPEDA, s 10.1).

Some commentators are concerned that the breach notification provisions are too broad, unclear, and have led to the erroneous procedures, which sought to include the consent statements in their personal information, subject to limited exceptions. 10

On the other hand, PIPEDA now includes additional exceptions in which an organization is unable to direct personal information without consent of the individual, including with respect to investigations regarding suspected copyright infringement. While this is a step in the right direction, it would perhaps be too difficult for them to fight in Canada.

Further, privacy advocates have raised strong opposition to the expansion of information to include real time monitoring of Canadian citizens and businesses across the country. For example, the Digital Privacy Act will require organizations to notify individuals whenever personal information is involved and, whether an individual opts to disclose personal information without consent of the individual, including with respect to investigations regarding suspected copyright infringement. While this is a step in the right direction, it would perhaps be too difficult for them to fight in Canada.

The breach notification provisions in the Digital Privacy Act are quite similar to the breach notification provisions in the Alberta Personal Information Protection and Privacy Act as matters expressly excluded from provincial authority under s 91 of the Constitution Act as matters within federal authority (e.g., banks, airlines), matters expressly excluded from provincial authority under s 92 (e.g., grain elevators).
PIPEDA, s 28.


Kelly Friedman is a Partner in the Toronto office of DLA Piper (Canada) LLP. She may be contacted at kelly.friedman@dlapiper.com. Tamara Hunter is an Associate Counsel in the Vancouver office of DLA Piper (Canada) LLP. She may be contacted at tamara.hunter@dlapiper.com. Jim Halpert is a Partner in the Washington office of DLA Piper (USA) LLP and a member of Privacy & Security Law Report’s Advisory Board. He may be contacted at jim.halpert@dlapiper.com. The authors are grateful for the research assistance of Teio Senda, Articled Student.