nNOVATION LLP

June 26 2015

LOOKING AT THE CHANGES TO PIPEDA UNDER BILL S-4, THE *DIGITAL PRIVACY ACT*

The *Digital Privacy Act*,[1] which makes a number of amendments to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA),[2] received royal assent on June 18. One might expect that a bill nine years in the making would dramatically reshape the law; however, this is not the case.[3] Most of the changes to PIPEDA involve tweaks that are meant to "fix" certain issues that would only be familiar to the closest (and most patient) followers of the law. Although the new data breach reporting regime has caused the most concern for businesses, a number of amendments should actually make the law easier to follow by introducing several new exceptions to the consent requirement.

The following provides a summary of the changes to PIPEDA. Note that all of the amendments except those related to the new breach reporting regime are currently in effect (these latter amendments will come into effect on a date to be determined by Industry Canada).

Breach Notification

A new Division 1.1 will require organizations to notify the Privacy Commissioner of Canada (the "Commissioner") as well as affected individuals of any "*breach of security safeguards*[4] *involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual*."[5]

Organizations will also be required to maintain a record of every breach it experiences, and provide such records to the Commissioner upon request (this record-keeping requirement could prove to be the most challenging aspect of Bill S-4).[6]

The offence provisions in section 28 - which allow for fines of up to $100,000 - will apply to contraventions of most aspects of the breach notification requirements.[7] As a result, many reports on S-4 have described the breach notification provisions as being subject to significant penalties. This is sort of true. To clarify, section 28 currently allows for fines where a person: a) obstructs a Commissioner investigation; b) destroys personal information subject to an access request under PIPEDA; or c) contravenes the "whistleblower" provisions. This is an extraordinary remedy that would have to be referred to the Crown for prosecution, which apparently has never been exercised. As such, the "penalty" aspect of breach notification has been overstated: although an organization could be subject to prosecution for a failure to notify, if past experience is any indicator, it seems unlikely except in extreme cases.

The next step is for Industry Canada to develop regulations specifying such things as: the form and contents of a report to the Commissioner, to affected individuals, and to other organizations; the records to be maintained by organizations; and further factors

---

[1] Long title: *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*.
[2] S.C. 2000, c. 5.
[3] The statutory five-year parliamentary review of PIPEDA that led to the passage of Bill S-4 began in 2006.
[4] A "breach of security safeguards" is defined as "*the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards*"; Bill S-4, s. 2; amended PIPEDA s. 2(1).
[5] Bill S-4, s. 10; new PIPEDA s. 10.1.
[6] Bill S-4, s. 10; new PIPEDA s. 10.3.
[7] Bill S-4, s. 24, amended PIPEDA s. 28.

specifying the meaning of a "real risk of significant harm".

PIPEDA will become the second private sector law with a breach notification requirement (behind the Alberta *Personal Information Protection Act*).

Several New Exceptions to Consent

PIPEDA generally requires consent for the collection, use or disclosure of personal information. A number of new exceptions to this requirement have been added to PIPEDA.

- Use or disclosure of personal information for purposes of a business transaction: Organizations can share personal information without consent for the purposes of assessing a potential business transaction (e.g., the purchase of another business or the business' assets).[8] No consent is required for the acquiring business to use personal information in accordance with purposes for which it was originally collected.
- Managing the employment relationship:[9] The awkward requirement for federally regulated employers to obtain consent for the collection, use or disclosure of employee personal information is finally removed. Now organizations can collect, use or disclose personal information about an employee without consent where it is "*necessary to establish, manage or terminate an employment relationship*" between the organization and employee.[10] Organizations must still inform employees about the collection, use or disclosure.
- Witness statements: Further clarity is provided regarding the ability of an organization to collect, use or disclose witness statements necessary to assess, process or settle an insurance claim.[11]
- "Work product" information: Consent is not required for the collection, use and disclosure of personal information "*produced by the individual in the course of their employment, business or profession*", where the collection, use or disclosure "*is consistent with the purposes for which the information was produced*."[12]
- Disclosures to identify injured, ill or deceased and communicate with next of kin: Organizations can disclose personal information necessary to identify an individual who is injured, ill or deceased, where the disclosure is made to a government institution or the individual's next of kin or authorized representative.[13] Personal information can also be disclosed to a government institution for the "*purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual*."[14]
- Financial abuse: There is more certainty around the ability of organizations to report suspected cases of financial abuse to a government institution or an individual's next of kin or authorized representative.[15] This amendment is intended to address a problem commonly referred to as 'elder abuse', where employees of banks and other institutions have reason to believe that a vulnerable individual is being manipulated into providing access to their financial assets.

Business Contact Information Now Includes Email

The definition of "personal information" in PIPEDA has been simplified by removing the statement that the

[8] Bill S-4, s. 7; new PIPEDA s. 7.2.
[9] PIPEDA only applies to federally regulated works and undertakings, which includes organizations such as banks, railroads, airlines and telecommunications providers.
[10] Bill S-4, s. 7; new PIPEDA s. 7.3.
[11] Bill S-4, s. 6(3), 6(5), 6(11); new PIPEDA paras. 7(1)(b.1), 7(2)(b.1), 7(3)(e.1).
[12] Bill S-4, s. 6(3), 6(5), 6(11); new PIPEDA paras. 7(1)(b.2), 7(2)(b.2), 7(3)(e.2).
[13] Bill S-4, s. 6(10); new PIPEDA para. 7(3)(d.4).
[14] Bill S-4, s. 6(7); new PIPEDA para. 7(3)(c.1)(iv).
[15] Bill S-4, s. 6(10); new PIPEDA para. 7(3)(d.3).

nNovation LLP • Barristers & Solicitors
World Exchange Plaza • 45 O'Connor Street, Suite 1150 Ottawa, ON K1P 1A4
p. 613.225.2906 • f. 888.314.5997

definition "*does not include the name, title or business address or telephone number of an employee of an organization.*" The new definition of personal information is now "*information about an identifiable individual*", meaning that business contact information is brought within the scope of the Act as personal information.[16]

A separate definition of "business contact information" is defined as "*any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address".*[17]

The new section 4.01 exempts business contact information wherever it is collected, used or disclosed "*solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.*"[18] This amendment addresses the fact that business email addresses were previously within the scope of PIPEDA due to how it had been drafted and interpreted by the Commissioner.

Investigative Bodies Process Replaced

The cumbersome process requiring Industry Canada to approve "investigative bodies" has been replaced with a simpler model under which one organization may disclose personal information to another organization without knowledge or consent where reasonable for the purposes of

- investigating a breach of an agreement or contravention of a law that has been, is being or is about to be committed, or
- preventing, detecting or suppressing fraud,

and, it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the purpose for making the disclosure.[19]

Meaning of "Valid" Consent

A new section states that consent is only 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.*"[20] This is, in part, an attempt to address the difficult issues around privacy of minors without going down the path of prescribing specific consent requirements according to age (i.e., COPPA). In practice, it is not clear how much this amendment alters the existing requirement to obtain consent that is informed and knowledgeable, but businesses may want to revisit policies and practices to ensure that they are reasonably clear to the intended audience.

New Powers for the Commissioner

The Commissioner has not been given the powers to issue orders or impose penalties, as some stakeholders would like to see. However, two new mechanisms enhance the Commissioner's powers within the ombudsman framework.

First, the Commissioner can enter into a compliance agreement with an organization if he believes "*on reasonable grounds*" that the organization "*has committed, is about to commit, or is likely to commit*" a contravention of PIPEDA.[21] The agreement can "*contain any terms that the Commissioner considers necessary to ensure compliance*". This means that a compliance agreement could require an organization to change its practices, and if the Commissioner believes that the terms of the agreement are not being met, he can apply to the Federal Court for an order requiring the organization to

[16] Bill S-4, s. 2(1); amended PIPEDA s. 2(1).
[17] Bill S-4, s. 2(3); amended PIPEDA s. 2(3).
[18] Bill S-4, s. 4; new PIPEDA s. 4.01.
[19] Bill S-4, s. 6(10); new PIPEDA paras. 7(3)(d.1) and 7(3)(d.2).
[20] Bill S-4, s. 5; new PIPEDA s. 6.1.
[21] Bill S-4, s. 15; new PIPEDA s. 17.1.

nNovation LLP • Barristers & Solicitors
World Exchange Plaza • 45 O'Connor Street, Suite 1150 Ottawa, ON K1P 1A4
p. 613.225.2906 • f. 888.314.5997

comply with the agreement, in addition to any other remedies deemed appropriate by the Court.[22]

Second, the Commissioner's public interest disclosure powers have been expanded. Previously, section 20 the Act allowed the Commissioner to make public "*information relating to the personal information management practices of an organization*" (if in the public interest to do so). Now the Commissioner is able to make public "*any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers*."[23] This would allow the Commissioner to publicly comment on more than just an organization's information handling practices; e.g., the manner in which an organization did or did not cooperate with an investigation.

More Time for Complainants to Apply to Federal Court

The time for a complainant to apply to Federal Court for a hearing after receiving a report of findings or notification that an investigation has been discontinued is extended from 45 days to a full year.[24] This addresses the fact that in some cases organizations may require more than 45 days to implement recommendations by the Commissioner, meaning that a complainant could be barred from applying to Federal Court if they wait to see if the organization complies.

[22] Bill S-4, s. 15; new PIPEDA s. 17.2.
[23] Bill S-4, s. 17(2); amended PIPEDA s. 20(2).
[24] Bill S-4, s. 13; amended PIPEDA s. 14(2). The Commissioner's Office has in the meantime developed what is essentially a workaround, in that a "Preliminary Report of Findings" is issued, giving an organization time to respond before issuing the final Report of Findings. It would seem that the Preliminary Report of Findings may no longer be necessary with this amendment.

nNovation LLP • Barristers & Solicitors
World Exchange Plaza • 45 O'Connor Street, Suite 1150 Ottawa, ON K1P 1A4
p. 613.225.2906 • f. 888.314.5997