

Reproduced with permission of the publisher from Canadian Privacy Law Review, Vol. 7, No. 11 October 2010.

Privacy Slow Cooker — Were *PIPEDA* Amend- ments Worth the Wait?



Bernice Karn
Partner
Cassels Brock & Blackwell LLP

As part of a recent flurry of Parliamentary activity, in May of this year, the federal government tabled Bill C-29 in the House of Commons to propose long-anticipated amendments to Canada's *Personal Information Protection and Electronic Documents Act* [*PIPEDA*], S.C. 2000, c. 5. Since *PIPEDA*'s enactment in 2001, practitioners have often struggled to interpret the language of *PIPEDA*, which is quite terse and cryptic in some areas, yet rather verbose and very "non-legal" in others. By its own terms, *PIPEDA* requires that Parliament conduct a review of the Act every five years, and these proposed amendments represent the outcome of the first review of the Act that took place in 2006.

Business Transactions

One of the major criticisms of *PIPEDA* has been that the Act did not make any exception for the requirement to obtain consent to the collection, use or disclosure of personal information in the context of a sale of a business or other business transaction. For M&A transactions, this oversight has caused major headaches for vendors' and purchasers' counsel alike.

If enacted, Bill C-29 would add a new s. 7.11 to *PIPEDA* that permits parties to a business transaction to use and disclose personal information as necessary for due diligence purposes and for the purpose of closing the transaction without consent of the individuals concerned, provided that the parties agree: to use and disclose the information only for purposes related to the transaction; to protect the information by security

safeguards appropriate to its sensitivity; and, if the transaction does not close, to return or destroy it within a reasonable time. The proposed *PIPEDA* amendments would obligate the parties to notify the data subjects following closing of the transaction and of the disclosure of their personal information.

Business Contact Information

One of the oddities in *PIPEDA* is that the definition of "personal information" excludes certain business contact information, but that list of exclusions surprisingly does not include a person's business email address. Thus, in at least one complaint to the federal Privacy Commissioner, the use of a person's email business email address without his consent was found to be contrary to the requirements of *PIPEDA*.¹

The *PIPEDA* amendments address this anomaly and now create a new "business contact information" definition that includes a person's business email address. This new definition is coupled with a new s. 4.01, which states that Part 1 of *PIPEDA* does not apply to business contact information if this information 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."

Data Breach Notification

Following the lead of many U.S. states, the proposed amendments to *PIPEDA* would allow for a data breach notification protocol. As is the case in many other areas of *PIPEDA*, where organizations are essentially required to use their best judgement about the actions necessary for compliance, the decision about whether or not to make a notification really depends on the organization's assessment of the seriousness of the breach.

Organizations are required by the amendments to report to the federal Privacy Commissioner any "material" breaches of security safeguards in relation to personal information under their control. Materiality is to be judged in relation to the sensitivity of the information at risk, the number of persons whose information has been affected and whether or not the breach was an isolated incident or part of a systemic problem.

The amendments further impose an obligation to notify the affected individuals in situations in which a breach of security standards involving personal information would pose a threat of “significant harm” to the individuals. “Significant harm” includes situations of bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effect on a person’s credit record and damage to or loss of property. However, organizations hoping for concrete direction from *PIPEDA* on when to notify individuals in cases of data breach will be disappointed. Organizations are directed to consider various factors (such as the sensitivity of the personal information involved and the probability of misuse of the information) in making their own determination about whether to notify affected individuals.

The amendments also go further in imposing a positive obligation on organizations to notify other organizations or government institutions that may be able to reduce the risk of harm emanating from the breach, if certain conditions, to be set forth in regulations, are satisfied.

Other Amendments of Interest

While the business transaction, business contact information and data breach notification amendments likely pose the most interesting changes for businesses, a few other amendments bear examination as well. For example:

- **Knowledge and Consent** — Parliament now is raising the bar on the type of consent (to collection/use/disclosure of personal information) that will suffice. In the present version of *PIPEDA*, consent is referred to in conjunction with “knowledge.” In other words, when collecting consent, an organization is under a duty to ensure that the individual granting consent understands what he/she is agreeing to. Under the new amendments, this knowledge concept is strengthened. If the amendments are passed, a person’s consent will only be valid if it is reasonable to expect that the individual understands the *nature, purpose and consequences* of the collection, use or disclosure of personal information to which they are consenting. This is more than mere knowledge and imposes a higher duty on organizations to ensure that individuals truly understand the purposes for which their personal information is being collected, used and disclosed.

- **Employee Information** — Although *PIPEDA* only applies to employees’ personal information if the employer is a “federal, work, undertaking or business”, over the years the issue of whether an employee’s work product is considered to be his/her personal information has attracted a bit of controversy. Bill C-29 attempts to settle the matter through amendments to s. 7 of *PIPEDA* that would make it clear that the employer (or any organization) does not require the employee’s consent to the collection, use or disclosure of this information if it is produced in the course of their employment and the collection/use/disclosure is “consistent with the purposes for which the information was produced.” Unfortunately, these amendments merely do away with consent and seem to be premised on the assumption that information produced by an individual in the course of their employment, business or profession is personal information about an individual, which is debatable. In at least one set of findings from the federal Privacy Commissioner’s Office, “work product” information was found not to be personal information² while subsequent sets of findings took a contrary view.³

- **Lawful Authority** — Canadian businesses have sometimes been presented with letters from policing authorities requesting personal information to aid the authorities in their investigations. While most businesses are more than willing to assist police in carrying out their duties, some organizations have been concerned about their liability for contravening *PIPEDA* for disclosing personal information without consent. The existing provisions of s. 7(3)(c.1) of *PIPEDA* permit disclosure without consent if the disclosure is made to a “government institution” that has made a request for the information, the government institution has identified its “lawful authority” to obtain the information and has indicated the reasons for the request (which are law-enforcement related).

“Government institution” has never been defined (although the current version of *PIPEDA* says that it may be defined by regulation). However, the bigger question has revolved around what is “lawful authority?” Some observers believe that “lawful authority” means

a warrant, subpoena or other judicially authorized process, while others believe that it simply means that the government institution is acting within its statutory mandate. The proposed amendments to *PIPEDA* only answer part of the question. While they say that “lawful authority” means something other than a subpoena, warrant, etc., unfortunately, the amendments do not actually say what that “something other” is, which is not helpful to businesses trying their best to comply.

The amendments go further and state that the organizations that are presented with a government institution demand for disclosure of personal information are not required to verify the validity of that lawful authority. While presumably Parliament is trying to be helpful by not requiring businesses to seek advice in determining whether “lawful authority” exists or not when faced with a demand for personal information, it seems to be a roundabout way of saying that the non-disclosure without consent rule just doesn’t apply in law enforcement situations. One wonders why Parliament could not simply state such a simple rule in the legislation.

Witness Statements — Another curious amendment to the consent rules is that information contained within a witness statement may be collected, used and disclosed if necessary to “assess, process or settle an insurance claim.” No doubt those amendments will be welcomed by the insurance industry.

However, if this type of exception is useful for insurance litigation, it seems strange that a broader amendment was not proposed for litigation generally, especially since groups such as the Canadian Bar Association made submissions to the Standing Committee on Access to Information Privacy and Ethics (during the mandatory *PIPEDA* review) that *PIPEDA* should not affect existing litigation processes.⁴

PIPEDA continues to be a work in progress as these proposed amendments make their way through the legislative process.

- ¹ *PIPEDA* Case Summary #297 (December 1, 2004): Available at <http://www.priv.gc.ca/cf-dc/2005/297_050331_01_e.cfm>.
- ² *PIPEDA* Case Summary #14 (September 21, 2001): Available at <http://www.priv.gc.ca/cf-dc/2001/cf-dc_010921_e.cfm>; *PIPEDA* Case Summary #15, (October 2, 2001): Available at <http://www.priv.gc.ca/media/an/wn_011002_e.cfm>.
- ³ *PIPEDA* Case Summary #220 (September 15, 2003): Available at <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030915_e.cfm>; *PIPEDA* Case Summary #303 (May 31, 2005): Available at <http://www.priv.gc.ca/cf-dc/2005/303_20050531_e.cfm>.
- ⁴ Canada. Parliament. House of Commons. Standing Committee on Access to Information, Privacy and Ethics. *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA): Fourth Report*. Ottawa: Communication Canada — Publishing, May 2007 at 20: Available at <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?Doid=2891060&Language=E&Mode=1&Parl=39&Ses=1>>.