Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA: http://laws.justice.gc.ca/eng/UpdateNotice/index.html?rp14=%2Fen%2FP-8.6%2Findex.html

The long-awaited result of PIPEDA's five-year review was introduced on May 25, 2010 as Bill C-29 and has yet to get to second reading. Here are the main features:

Business Contact Information: The first significant change is the exclusion of "Business Contact Information" from the purview of the statute. "Business Contact Information" refers to an individual's name, position name or title, work contact details (including e-mail address) and any similar information of the individual so that, in the new Section 4.01, business contact information is excluded from the provisions of PIPEDA if business contact information is collected, used or disclosed solely for the purpose of communicating with the individual in relation to their work.

Valid Consent: Bill C-29 raises the bar, or at least clarified, what is necessary to get consent from an individual. Section 6.1, entitled "Valid Consent" clarifies that the consent that is required under Principle 3 of the CSA Model Code is only 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 likely raises the bar on what is valid consent.

Witness Statements and Work Product: In Section 7, which allows the collection, use or disclosure of personal information without consent a number of changes have been added to permit the collection, use and disclosure of information in witness statements where it is necessary to assess, process or settle an insurance claim. In addition, information produced by individuals in the course of their employment is exempt from the consent requirements provided that the collection, use and disclosure are consistent with the purposes for which the information was produced. This particular exemption codifies what is often referred to as "work product" exception to consent.

Lawful Authority: Also in Section 7, the government has attempted to clarify what has been a very confusing provision regarding disclosures to law enforcement. Section 7(3)(c.1) permits the disclosure to government institutions and law enforcement where the government body has identified its "lawful authority" to obtain the information. The meaning of "lawful authority" has been very problematic since the first version of PIPEDA, with interpretations ranging from legal authority to compel or just part of a lawful process.

Gag Order: A notable addition to PIPEDA is a "gag order" that prohibits an organization from notifying an individual that information has been requested or obtained by a government institution or part of a government institution under a range of provisions contained in Section 7(3). Before it notifies the individual, it has to notify the government institution and get their OK. If the government institution vetoes the disclosure, the organization is not allowed to notify the individual but is required to notify

the Privacy Commissioner. This above provision supplements what had previously been the case where an individual had made a request for access to their own personal information or an account of its collection, use or disclosure where that personal information had been the subject of a government request.

Removing Investigative Bodies: Notably, these amendments have completely done away with investigative bodies. It used to be that under Section 7(3), an organization could disclose personal information to designated investigative bodies for the purposes of investigations. Investigative bodies included the Insurance Fraud Bureau of Canada, most Barristers' Societies and other professional regulators. Instead, the new Section 7(3)(d.1) permits disclosures to another organization where that disclosure is necessary to investigate a breach of an agreement or a violation of the laws of Canada or Province or is necessary to prevent, detect or suppress fraud where it would be reasonable to expect the disclosure with the knowledge or consent of the individual would undermine the ability to prevent, detect or suppress the fraud. Subsection (d.2) allows disclosures to government institutions or next of kin related to "financial abuse". Finally, Subsection (d.3) further permits disclosures for notifying the next of kin of injured, ill or deceased individuals.

Business Transactions: The new Section 7.1 permits disclosures and uses of information in connection with a "prospective business transaction". This term is defined to include a range of transactions, including purchase or sale of a business, mergers and amalgamations, financings, leasings, and joint ventures. This section 7.1, parties to a perspective business transaction can use and disclose personal information without the knowledge or consent of the individual if they have entered into an agreement that requires the recipient to use the information and disclose it solely for the purposes related to the transaction, to protect that information with appropriate safe guard and, if the transaction does not proceed, to return or destroy the information within a reasonable period of time. This provision that permits the use and disclosure of personal information for business transactions does not apply to business transactions where the primary purpose or result is the purchase, sale or other acquisition of personal information.

Employee Personal Information: The new Section 7.2 will mark a significant change in how PIPEDA applies to employees of federal works, undertakings and businesses. No longer is consent of the individual required to collect use and disclose employee personal information if that collection use or disclosure is necessary to establish, manage, or terminate the employment relationship, provided that the employer has notified the individual that the personal information will be or may be collected, user disclosed for these purposes.

Breach Notification - Notification of the Commissioner: Perhaps the most notable addition to PIPEDA in Bill C-29 is the addition of Division 1.1, which deals with breaches of security safe guards. The new section 10.1 requires an organization to report to the Privacy Commissioner any "material breach" of security safeguards. Whether the breach is material depends upon the sensitivity of the information, the number of individuals whose personal information was compromised and an assessment by the organization whether the cause of the breach or a pattern of breaches indicates a systematic problem. The form of the notice will be set out in the regulations. The Commissioner has no power to require the organization to notify individuals, nor does

she have any power to seek a remedy on behalf of affected individuals unless they themselves complain.

Breach Notification - Notification of the Individual: The new Section 10.2 deals with notification to the individual, which is mandatory if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. Section 10.2(2) defines significant harm to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. Subsection (3) then goes on to provide guidance on whether there is a "real risk", which is based on the sensitivity of the information and the probability that the personal information has been, is being or will be misused. The notification has to contain enough information to allow the individual to understand the significance of the breach to them and to take steps to mitigate that harm. Notice has to be given as soon as feasible after the organization confirms the occurrence of the breach and concludes that they are required to give notice occasionally under Section 10.2(1). The form and manner of notice may be prescribed in regulations, which I anticipate will allow for notice to large groups of people though the mass media where it is not feasible to give individual notice. This new Section 10.3 allows organizations to give breach notification to other organizations that will help to reduce the risk of harm that could result from the breach or to mitigate that harm.

SOURCE: http://privacynewshighlights.wordpress.com/2011/02/18/01-31-january-2011/