DOLDENWALLACEFOLICK LLP
Insurance Law Expertise... It's our policy.

Insurance Journal

In this Issue…

By Paul Dawson

Canada moves to private sector breach notice: Cyber Insurers beware

Last week Parliament passed the *Digital Privacy Act* ("*DPA*").[1] The DPA was the fourth legislative attempt since 2010 to amend the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), and its implementation will both expand the powers of Canada's Privacy Commissioner and increase the burden on businesses to ensure they notify persons whose personal information has been exposed as a result of a data breach. The cost to Canadian businesses resulting from data breaches are likely to increase dramatically – as will demand for cyber insurance to cover those costs.

The biggest change arising from the *DPA* has yet to be felt, but will likely result in an increase in first party claims under cyber policies. Section 10 of the *DPA* inserts into *PIPEDA* a new requirement that organizations *must* report to the Privacy Commissioner any data breach involving personal information. This obligation is triggered if it is reasonable in the circumstances to believe that the breach creates a "*real risk of significant harm to an individual*". Determining whether there is a "*real risk of significant harm*" involves a consideration of both the "*sensitivity*" of the information that has been breached, and the likelihood that this information has or will be misused. This will inevitably involve the costly step of trying to determine what happened to the information and who, if anyone, might have improper access to it.

Furthermore, the organization will also have to notify individuals of a breach that might reasonably create a real risk of "*significant harm*" to those individuals. A "*significant harm*" to an individual can include things like humiliation, damage to reputation or relationships, financial loss, loss of employment, identity theft, and negative effects on credit records.

The notice must also be sufficiently detailed to allow the individual to understand the significance of the breach and take steps to minimize their

[1] SC 2015, c. 32, previously Bill S-4.

impact. This requirement to provide sufficient notice can, in certain circumstances, cost hundreds of thousands of dollars, if not more. Hence, organizations will obtain cyber insurance in order to pass these costs onto their insurer, making these policies more popular in the insurance market.

The *DPA* also increases the regulatory burden on Canadian businesses and organizations subject to *PIPEDA*. The latter statute already contained a set of principles governing when and how organizations must obtain an individual's consent before collecting, using, or disclosing the individual's personal information; the *DPA* now says that such consent is only valid if the organization reasonably believes that the individual would understand the nature, purpose, and consequences of granting such consent.

However, insurers will be particularly interested to note that the *DPA* also creates an exception applicable to insurance adjusting: personal information may now be collected, used, and disclosed without consent if it is contained in a witness statement obtained to investigate or settle an insurance claim.

The mandatory breach notice provisions in the *DPA* are not yet in force, and will come into force only after further consultation with businesses and other stakeholders – but they will fundamentally transform privacy law in Canada. Until now, the Privacy Commissioner only became engaged when an individual complained that an organization had breached *PIPEDA*; now organizations themselves must report breaches to the Commissioner and to affected individuals. When the new mandatory notice provisions come into effect, data breaches will be much more likely to become publicly known; to trigger legal and business costs in providing information and responses to the Commissioner; and to trigger privacy-related litigation.

The *DPA* is anticipated to come into effect sometime in the summer of 2015. However, Canadian businesses – and their insurers – should begin examining immediately how the *DPA* will affect their commercial and underwriting practices. Mandatory notice provisions have been in place in the United States for years, where public notice programs

have proven very expensive, and have often triggered class action suits. That reality is likely soon coming to Canada – and with profound effect.

Editor

Keoni Norgren, Tel: 604-891-5253 E-mail: knorgren@dolden.com

Please contact the editor if you would like others in your organization to receive this publication.

Contributing Authors

Paul C. Dawson, Tel: 604-891-0378 E-mail: pdawson@dolden.com

Vancouver, BC

Tenth Floor - 888 Dunsmuir Str
Vancouver, B.C.
Canada / V6C 3K4

Telephone (604) 689-3222
Fax: (604) 689-3777
E-mail: info@dolden.com

Toronto, ON

200-366 Bay Street
Toronto, Ont.
Canada / M5H 4B2

Telephone (416) 360-8331
Fax: (416) 360-0146
E-mail: info@dolden.com

Kelowna, BC

308-3330 Richter Street
Kelowna, B.C.
Canada / V1W 4V5

Telephone (250) 980-5580
Fax (250) 980-5589

E-mail: info@dolden.com