Businesses must fess up to privacy breaches under new law

Speed read

Relatively light changes are to be made to the Privacy Act according to the May 2014 announcement by Government. The main current structure including the Information Privacy Principles is to be retained.

The biggest developments in practice are:

- Businesses and other agencies must tell the Privacy Commissioner when there's a substantial data breach, and tell affected people as well if the breach involves a real risk of harm to those people.
- The Commissioner gets a valuable tool enabling him or her to issue a compliance notice to businesses and other agencies, requiring compliance with the Act.
- International transfer of data is further tidied up, by a regime as to transfer of data overseas, including a list of safe harbour countries deemed suitable to receive data.

An exposure draft bill is to now to be produced for comment. We are a ways off the changes being legislated.

This article focusses on businesses. For details of the current privacy regime, see the chapter we wrote in the The International Comparative Legal Guide to: Data Protection 2014.[1]

June 2014

The Minister of Justice has released high level details of the proposed changes which also reflect some of the developments internationally. Key points include:

Mandatory reporting of privacy breaches

Businesses and other agencies must report "*material*" privacy breaches. In deciding if breaches are material, businesses will take into account factors such as the sensitivity of the information, the number of people involved and whether there are indications of a systemic problem. They must also report to the affected people where there is a real risk of harm. For an example of how that might play out when forced to disclose, see our article, Big Data in business – father learns of teenage daughter's pregnancy from retails chain.[2]

So, trying to bury an exposure is no longer an option.

Compliance notices and other tools

To enforce the privacy regime, the Commissioner has few options and generally can only seek remedies from the Human Rights Review Tribunal. That can make it hard to go beyond cajoling businesses into doing things.

The proposed changes make modest increases to investigation powers which will help.

The strongest change may be the new ability for the Commission to issue compliance notices, requiring businesses to do something or restrain from doing something. Those notices can be enforced by bringing proceedings before the Tribunal. This will enable the Commissioner to act more directly and more swiftly.

This goes someway to strengthen the ability of the Commissioner to take steps.

Businesses must fess up to privacy breaches under new law

Transferring information off-shore

There are provisions being added to strengthen the application of the regime in relation to data sent offshore such as by cloud computing. But that largely restates businesses' current direct privacy obligations, such as under IPP5, in relation to information sent off shore. There will however be an express carve out from responsibility where the off-shore provider breaches its contractual arrangements.

However, of importance to those often sending data offshore, a regime is established to:

- require the business to ensure the offshore receiving country meets certain privacy standards which will be outlined under the Act; and
- have a list of safe harbour countries to which information can more readily be sent. This is along the lines of the EU's safe harbour list, on which NZ is a recent entrant.

1. http://www.wigleylaw.com/assets/Uploads/The-International-Comparative-Legal-Guide-to-Data-Protection-2014.pdf

2. http://www.wigleylaw.com/assets/Uploads/Big-Data-in-business.pdf

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com