PRISM, spying and cloud computing: should businesses be worried?

Our clients over the years have asked questions like: "*Do privacy and security considerations mean we shouldn't move our data and its processing from our internal servers to cloud computing? And should we allow it to go to the States, given spying powers in legislation such as the Patriot Act?*"

How do the answers to those questions change with this month's revelations?

In his NBR Weekend Review article, *How I learned to stop worrying and love Prism*,[1] cloud computing consultant, Ian Apperley, argues there should be little change to the approach.

Is he right?

For some, yes. For others, it's too early to jump to conclusions on what to do about these PRISM and other developments when assessing how businesses should handle cloud computing choices. That calls for balanced and careful consideration, not assessment based on one part of the story. The picture will become clearer over the coming weeks and months.

This article was first published in NBR Online on 16th June.

June 2013

In his article, Ian Apperley says:

- Such surveillance has been going on for years, via PRISM predecessors, Waihopai based surveillance and so on: PRISM is nothing more than a PR mess.
- If only the business holds the encryption key (i.e. the ability to get at the encrypted data) for data held offshore, that provides protection.
- In relation to one key remaining area of weakness – access to data when it is decrypted to enable it to be processed – new techniques, called homomorphic cryptography, are evolving which enable the processing to happen while the data remains encrypted. When that happens, data can go off shore to be held and processed, without the ability for others to access it, if the key is only held here by the business.
- Why are people so alarmed about Government spys accessing data, when private companies like Fly Buys continuously surveil us.

They're all fair points with strength, even though they can be debated. For some, that will be enough reason to continue off-shore cloud computing including in the States, assuming homomorphic cryptography is available. But that is only in development. Even without that, this may be enough for some businesses. ICT security risk assessment involves weighing up risk, benefit and practicality. Legal risk is but one facet but it is a real issue.

We've found that some things can be flavour of the month, leading to distorted outcomes. For example, some will be saying, this month: "*The ICT security risk of having data and its processing in the States is too high in view of the spy agencies' wide-sweeping surveillance of billions of transactions*". But that is too simplistic:

- Having cloud computing done in a country – such as the USA – where such intrusive steps to protect against cyber-terrorism and the like can ultimately mean that the business's overall data is more secure. For example, cyber-attacks by non-USA governments and businesses may be less likely.

- The alternatives could be worse. We've seen businesses choose to take cloud computing to countries that are less stable and secure than the US, because of the perceived problems around the Patriot Act etc. And continued processing and storage of data on internal servers can be riskier than that happening off shore on the cloud: human error for example is a key risk of internal data storage and processing systems. When assessing the risk, the comparison is not the proposed system (off shore cloud computing in the States or elsewhere) against perfection, but the proposed system compared with the real-life status quo and/ or other real-life options.
- This is not just about intrusion by Government spys. Big data use by businesses has exponentially increasing intrusion on other businesses and individuals, as we outlined in our article, *Big Data in business–father learns of teenage daughter's pregnancy from retail chain*.[2]

The sort-of gold plate standard for privacy and security has been the EU Data Protection Directive. New Zealand recently joined the very small club of non-EU countries declared to be compliant with the EU's requirements for international processing of data. This opens up opportunities for New Zealand businesses to do cloud computing for other countries, inside and outside the US. But:

- There are the media reports that there may have been PRISM-like activities in EU countries: so where do they now stand?
- If the new GCSB and telecommunications interception legislation is sub-optimal and does not contain appropriate controls on the spy agencies, NZ cloud computing suppliers may lose business.

It's too early to jump to conclusions on what to do about these PRISM and other developments when assessing how businesses should handle cloud computing choices. That calls for balanced and careful consideration, not assessment based on one part of the story. The picture will become clearer over the coming weeks and months.

1. http://www.nbr.co.nz/article/how-i-learned-stop-worrying-and-started-love-prism-ck-141576

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

Wigley+Company
PO Box 10842
Level7/107 Customhouse Quay, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com