Wigley & Company

BARRISTERS and SOLICITORS

Cloud Computing: Privacy and Security Legal Issues

November 2009

When evaluating cloud computing options, organisations are of course concerned about security issues, as information is hosted elsewhere, often offshore. Legal aspects are important for wider security considerations. But these form only part of the risk/benefit/cost analysis. Very often the PR damage from a security breach will be more significant than the legal implications. Further, the risk of security/privacy breach may be lower overall under cloud computing than applies in the status quo (e.g. on-site processing of data), as we outline in our article The Case against Cloud Computing… revisited. In the article that follows we address the legal aspects of security and privacy for cloud computing. We use the New Zealand position to illustrate the approach. That approach can be varied to suit issues in other jurisdictions.

It's not just about privacy legislation

People often discuss cloud computing as though the considerations stop and start with privacy legislation, such as New Zealand's Privacy Act, US legislation, the EU Directives, etc. However, privacy and security raises potential legal responsibilities and liabilities in other ways, as we outline in our article, *Privacy Implications for Information Technology*.[1] We deal first with the NZ Privacy Act, to illustrate, and then other legal grounds.

Privacy Act

For cloud computing, the key obligation[2] is in Information Privacy Principle 5 (IPP5) in the Act:

> **Principle 5 Storage and security of personal information**
>
> An agency that holds personal information shall ensure—
>
> a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
>
> (i) Loss; and
>
> (ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
>
> (iii) Other misuse; and
>
> b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

For cloud computing, several conclusions flow from this (as they do for other ICT scenarios, very often):

- 100% security protection is not required. What is called for is protection of information by such safeguards as are "reasonable in the circumstances to take". So, for example, personal health records call for high levels of security protection; less sensitive information can have lower protection.
- Robust industry practice, codes, etc, are likely to be relevant in determining the appropriate approach.
- Under (b) of IPP5 above, if the agency (e.g. the NZ-based company using cloud computing services) gives information to a

[1] http://wigleylaw.com/Articles/LatestArticles/privacy-implications-for-information-technology/

[2] But not the only obligation

cloud computing provider, that agency must "ensure…that everything reasonably within [its] power … is done to prevent unauthorised use or unauthorised disclosure of the information." This obligation applies whether the cloud computing provider is based in New Zealand or offshore.

The obligation also means that the NZ based organisation often won't be able to rely solely on, for example, a supply contract under which the provider takes responsibility. This assumes that the provider does take responsibility. At present, many cloud computing providers do the opposite. So, further due diligence, systems, monitoring, etc, are likely to be required on the part of the NZ organisation in order to be Privacy Act-compliant.

Off shore considerations and the Privacy Act

As noted above, the NZ-based user of cloud computing services retains responsibilities around security in respect of the information, including when it is sent off shore. The organisation should assess whether a particular service and provider should be permitted to have the information in various countries, some of which may have a weak privacy regime. It is one thing to send the data to Australia or Europe (each with a robust privacy regime) and another to send it to a country without such law and practice.

The EU provides useful guidance on the adequacy of protection of data in other countries.[3]

Increasingly, cloud computing customers can require providers to limit the transmission of their information to certain countries. For example it could be limited to Australia, to New Zealand itself, or even, in the case of government, limited to public sector networks and servers (the so called G-cloud).

The judgment call depends on a variety of factors including the sensitivity of the information in question.

But it is always valuable to compare cloud computing options with the status quo: the real risks associated with on-site retention of data, or using NZ-based data centre hosted services.[4]

Other legal considerations

Very often, Privacy Act compliance will lead to compliance with duties owed to stakeholders in relation to their data, arising under the law of contract, tort or equity.

In broad terms an organisation would owe a duty to a third party, whose confidential information is held by it, or by a cloud computing provider on its behalf, to take reasonable care to protect that information. That has overlaps with the Privacy Act responsibilities noted above such as compliance with robust industry practice to reflect the sensitivity of the data etc.

The Privacy Act is limited to personal information (that is, information about people). There will be confidential information such as sensitive financial information about a company which is not affected by the Privacy Act, where duties still lie under contract, tort or equity.

Contractual reduction of risk

The way contracts are framed can of course impose greater risk (for example, a contract term ensuring that all data will remain secure).

Of course, just as the cloud computing provider will seek to limit its risk in its contract with the NZ organisation, so can the latter seek to do so with its customers.

This may be achievable where the NZ organisation's customers are businesses. It is more difficult where the information is personal information and the customers are individuals.[5]

Standard form contracts from cloud computing providers currently tend to eliminate liability to a large degree. Increasingly over time, larger users of cloud computing services, in particular, may be able to negotiate more favourable terms.

[3] http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

[4] See our article, *The Case Against Cloud Computing* http://wigleylaw.com/Articles/LatestArticles/the-case-against-cloud-computing-revisited/

[5] Protected under the Privacy Act and the Consumer Guarantees Act

Public Sector considerations

The public sector has additional considerations such as the Public Records Act and the Official Information Act, as well as certain security requirements specific to Government.

There is an outline of the requirements – which is also very helpful guidance as for the private sector – in the April 2009 SSC publication, *Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on risk Management.*[6]

[6] http://www.e.govt.nz/policy/trust-security/offshore-ICT/

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.