CLOUD COMPUTING AND THE NEW AUSTRALIAN PRIVACY LAW

(FOR THE PRIVATE AND PUBLIC SECTORS)

By Alec Christie, Partner, DLA Piper

WHAT IS CLOUD COMPUTING?

Web–based email (such as Gmail and Hotmail) and social networking websites (such as Facebook) are perhaps the most ubiquitous examples of Cloud services.

However, Cloud services can be delivered through a multitude of models (including non–public models such as *"private Clouds"* and *"shared private Clouds"*). Although the term *"Cloud"* does not have a precise meaning, it generally refers to information technology services, for example web-based email and social networking sites, that:

- are delivered via the Internet (the "Cloud" being an icon for the Internet); and
- typically have a de–centralised IT infrastructure (ie the supplier's data centres are spread across multiple, and sometimes offshore, locations).

WHY IS PRIVACY AN ISSUE?

Concerns about privacy and control over data are often cited as the major impediments to the growth of Cloud and its wide adoption by both business and government in Australia.

It is easy to understand why. Moving to the Cloud means relinquishing a degree of physical control over your IT infrastructure and relying, in part, on your Cloud vendor to ensure that your information is kept private and secure. If the data is stored in offshore locations, those locations may or may not be in countries that have privacy laws which are the same or similar to those in Australia.

However, contrary to popular perception, Cloud services models are not inherently incompatible with Australia's privacy laws or with privacy protection or security in general. Cloud does not raise legal issues, especially in respect of compliance with Australian privacy law, that are wholly new or even dissimilar to issues that have arisen in respect of other IT services (such as in the outsourcing and offshoring models). In respect of these other IT services, the issues have been successfully managed by well–advised agencies and businesses.

THE NEW AUSTRALIAN PRIVACY PRINCIPLES

Australia has Federal, State and Territory laws which generally adopt similar (although not identical) privacy principles. The principal piece of Federal legislation, to which all Federal agencies and most private sector business are subject, is the *Privacy Act 1988* (Cth).

From 12 March 2014 both the private and Federal public sectors will have to comply with the 13 new Australia Privacy Principles (*APPs*) under the *Privacy Act* that regulate the collection, holding, use and disclosure of *"personal information"*. The *Privacy Act* (from 12 March 2014) defines personal information to mean:

> *"information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not"*

For example, some email addresses (such as alec.christie@dlapiper.com) are personal information, but anonymous information (such as purely statistical data) is not.

In the context of Cloud, agencies and businesses that deal with personal information need to be mindful that:

- APP8 (cross–border disclosure of personal information) regulates the disclosure/transfer of personal information by an agency or business to a different entity (including a parent company) offshore. Before disclosure of personal information offshore, the Australian

agency/business (Australian sender) must take reasonable steps to ensure the overseas recipient will comply with/not breach the APPs. This can be done by appropriate contractual provisions. However, the Australian Sender will (subject to limited exceptions) remain liable for the overseas recipient's acts and practices in respect of the personal information sent as if the Australian Sender had engaged in such activities in respect of that personal information in Australia and, where relevant, be in breach of the APPs due to the overseas recipient's acts or omissions.

- APP11.1 (Security of personal information) requires that an organisation must "take reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure". The OAIC[1] has issued a 32 page guidance as to what these "reasonable steps" might include. Please see our recent Update (click here) which details what the OAIC suggests is required to meet this "reasonable steps" obligation. It is substantially more than what most agencies and businesses are currently doing in respect of security of information.

PRIVACY AND DIFFERENT CLOUD MODELS

The practical importance of privacy issues for Cloud offerings very much depends on the nature of the particular Cloud services being acquired. In particular, whether the Cloud offering is simply renting the *"tin"* – ie under an IaaS model – or is more akin to a managed services, SaaS or EaaS[2] model, where the vendor has access to, takes possession of or processes the personal information of individuals provided by the customer.

Common customer issues

It is worth noting that there is (in our view, indiscriminate) customer concern and focus on privacy and data security issues in respect of all Cloud offerings, in particular where the Cloud is (or may be) based outside of Australia. In fact, privacy and security of information are consistently raised as the two main concerns for Australian agencies and businesses considering entering the Cloud.

Potential customers are concerned, where the Cloud offering is based/has servers outside of Australia, that the placing of any personal information in the Cloud always results in a disclosure/transfer of the personal information offshore and this raises concerns for them as to whether or not they have the appropriate notifications/consents in place. While there are some real concerns in respect of certain Cloud offerings in certain circumstances, in reality under the IaaS model, for example, the data is not usually *"transferred"* to a third party (ie the vendor). Rather, the information usually remains under the control of the Australian customer and, therefore, does not require any specific notifications or consents as the Australian customer remains liable for privacy compliance under Australian law, no matter where it takes the data.

Of course, under the managed services/SaaS model (if the vendor does access or process the customer's data), there are concerns as to overseas transfer/disclosure where the vendor's servers are outside of Australia. However, this can be (and often usually already is) covered by the customer's existing notifications/privacy policy and privacy processes.

Australian customers are also often concerned (again, we believe, indiscriminately) about the possible access to their data by foreign governments (eg under the terms of the *USA PATRIOT Act 2001* or similar legislation of other countries) if hosted overseas. While this is not the place for a philosophical debate about the rights or wrongs of government (including intelligence agencies) accessing one's information and the recent events/publicity around this issue,[3] it is safe to assume that most governments can access one's information (wherever it is kept in electronic form) if they want to. Of course, there will be information of an agency (in particular) or possibly a business which is so sensitive/of such national importance that there must be no chance of it being accessed by a foreign Government and so a foreign hosted Cloud offering is out of the question (as would be any offshoring, outsourcing or third party data centre hosted offering). However, for most of us and for most of our information, access by the Australian Government or a foreign government is

[1] The Office of the Australian Information Commissioner (**"OAIC"**), the Australian privacy regulator.

[2] "Everything as a Service"

[3] For example, the global press about the PRISM program as exposed by Mr Snowden.

not either anticipated or overly concerning in a practical sense. While security in general and the security standards to which a Cloud vendor complies are important, the practical impact of the *USA PATRIOT Act* for US hosted Cloud offerings (or like legislation or potential actions of foreign governments for other foreign hosted Cloud offerings) should not be overstated.

The IaaS model

Where the Cloud vendor is simply renting the *"tin"* to the customer and is not itself involved in any handling, use or processing of the personal information held by its customer, all obligations with respect to privacy (and, generally, compliance with relevant laws) rightfully rest with the customer. In such circumstances, it is usual for the customer to warrant (and be obliged to ensure) that it has all necessary privacy consents and has made all necessary privacy notifications in order to use the relevant service.

The managed services/SaaS model

Where the Cloud vendor has a more *"active"* role in handling, holding, using or processing the personal information originally collected or held by its customer, then the vendor also needs to consider its obligations under (and be compliant with) Australia privacy law even if, in practice, much of the mechanics of compliance is pushed down to the customer. That is, the customer must make the appropriate notifications/obtain the appropriate consents to provide the personal information to the vendor, but the vendor still needs to consider its separate privacy obligations.

The vendor is also likely, in such circumstances, to have an obligation to notify the individuals (whose personal information its customer provides to it) that the vendor now holds their information and to provide the appropriate privacy notifications (usually done via its privacy policy). Of course, there are practical ways of incorporating this into the customer's processes going forward but there needs to be extra care taken with (and thought given to) the personal information the customer is already holding and wishes to put into the Cloud.

Financial and health services issues

Additional requirements imposed by:

- the Australian Prudential Regulatory Authority and the Australian Securities and Investments Commission on financial services licensees; and
- Federal and State legislation in respect of "health records" and health information on health services agencies and businesses,

will require the Cloud vendor to provide/satisfy additional specific security and privacy assurances, audit rights and significantly increased related obligations.

PRACTICAL WAYS TO ADDRESS PRIVACY OBLIGATIONS

Businesses and agencies which rely on Cloud services commonly address their obligations under the *Privacy Act* by (i) notifying/obtaining any relevant consents from individuals whose personal information they collect to process and store their information in the Cloud and (ii) by placing appropriate Australian specific contractual obligations of privacy on the Cloud vendor.

From a privacy perspective, some of the most important matters for an agency or business to fully investigate and understand when negotiating an agreement with a Cloud vendor include:

- the types and sensitivity of the information that the business/agency wants to put into the Cloud (eg personal and/or confidential information about customers and employees);
- what privacy and other obligations the business/agency has with respect to the information (eg contractual, regulatory or statutory obligations);
- the mechanisms and protections that the vendor has in place to protect and manage the information, including disaster recovery processes to protect against data loss;
- the locations of the vendor's data centres and other infrastructure and, if offshore locations are involved, what foreign laws will apply; and
- the vendor's reputation and track record in relation to security and privacy.

An agency/business that enters into an agreement for a Cloud service should ensure that the agreement places appropriate privacy related obligations on the vendor. However, the customer also needs to ensure that it understands (and does not try and impose on the vendor) the privacy obligations which are rightfully those of the customer or, practically, are best managed by the customer (eg around the original collection of the information). Some of the appropriate customer rights/vendor obligations to consider will relate to:

- retention of ownership of the information (ie ensuring it is clear that this is owned by the agency/business customer);
- security arrangements to ensure that all information is safeguarded and secure, and rights to audit the vendor's compliance with those security arrangements;
- reporting of information breaches and indemnities with respect to losses resulting from privacy related breaches;
- disaster recovery measures to help protect against information loss;
- storage of information only in nominated countries that have privacy protections which are compatible with Australian privacy law; and
- rights to audit and access information, including a right to the return of information when the agreement ends.

Of course the ability to demand and negotiate contractual measures and protections will depend, in part, on relative bargaining position of the parties, the contract value and the type of Cloud services being acquired. Accordingly, in some circumstances, an agency or business may be forced to assess the risks of proceeding without certain security or privacy protections against the benefits/cost savings it will receive from the Cloud service.

CONCLUSION

As with other IT services, the use of Cloud services raises a variety of privacy, security, regulatory and other practical issues that need to be carefully addressed and managed. However, from a privacy perspective, the legal issues that arise in respect of Cloud services are similar to issues that arise in the context of outsourcing, offshoring and other IT service models and can, as in these other areas, be appropriately managed and dealt with in the agreement between the parties.

Even so, it is crucial that your legal advisor fully understands the nature of both the Cloud and privacy and is able to tailor the legal protections in your agreement to fit the relevant Cloud services model chosen.

Please do not hesitate to contact one of our dedicated team if we can assist with your move to the Cloud or if you require assistance to ensure compliance with the new APPs which become effective on 12 March 2014.

CONTACT YOUR NEAREST DLA PIPER OFFICE:

BRISBANE

Level 29, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 38, 201 Elizabeth Street
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com

www.dlapiper.com

1201594299/JPS/092013