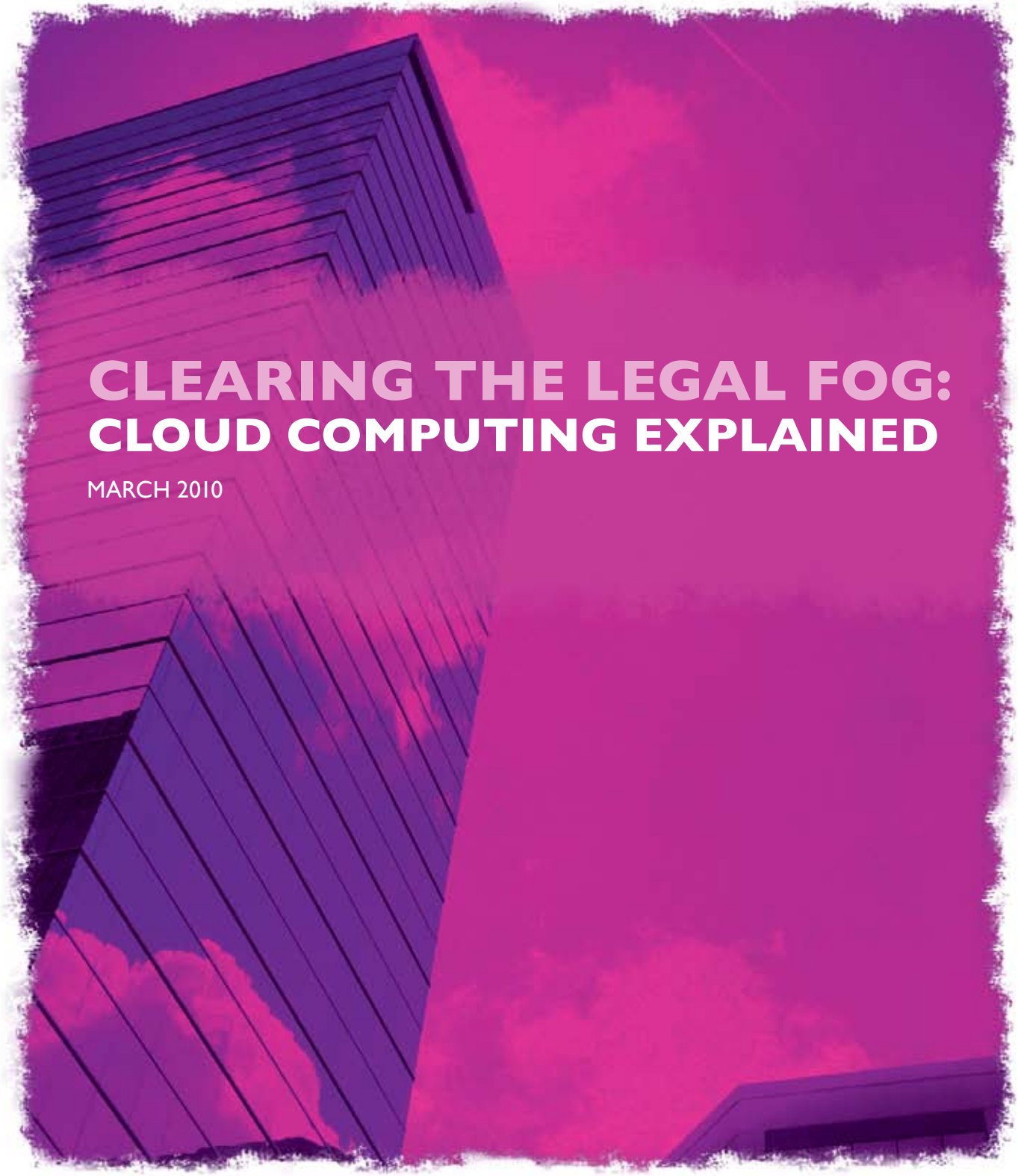

CLEARING THE LEGAL FOG:
CLOUD COMPUTING EXPLAINED

MARCH 2010

DLA PHILLIPS FOX

EVERYTHING MATTERS

This issues summary highlights some of the main legal issues that are claimed to negatively affect users of cloud computing and provides practical solutions to assist cloud adopters.

WHAT IS CLOUD COMPUTING?

'Cloud computing' means different things to different people and can be delivered through a multitude of models. Cloud computing can range from delivering basic office applications to individuals or small businesses at one end of the spectrum through to major bespoke combined service offerings to large corporates and government at the other.

The common elements that these different perceptions and models share are that they all involve information technology services which are:

(i) Delivered via the Internet (the 'cloud' being the IT industry-created icon for the Internet) and de-centralised IT infrastructure (typically including the supplier's data centres spread across multiple locations).

(ii) Truly elastic/scalable and 'on-demand' (ie no significant lead time to increase or decrease capacity).

Depending on the cloud model chosen, cloud users can become a 'thin-client', reducing their own IT infrastructure requirements and largely eliminating the need to host bulky servers and store large quantities of data locally.

The underlying technology of cloud computing is not new. For many years cloud computing technologies have been used for internet based records management, data processing and communications. Cloud computing is a natural evolution of SaaS, ASP and other IT models.

No wholly new legal risks arise in respect of cloud computing which have not already been identified and successfully managed in other IT models. However, it is crucial that your legal advisor understands cloud computing and is able to tailor the legal protections in your agreement(s) to address the cloud's specific characteristics.

IS CLOUD COMPUTING IMPORTANT?

A recent global CIO survey by Gartner found, for the first time, that virtualisation and cloud computing were the top 2 technology priorities for CIOs for 2010.[1]

As previously noted, however, cloud computing is not new: for some time individual users have been enjoying cloud computing services when using social networking sites such as Facebook and email services such as Gmail and Hotmail.

Other existing examples of cloud computing are present in data storage sites, video sites such as YouTube, personal health record websites and many more. Also, Google Apps uses a cloud computing model to provide government, business and educational institutions with access to web-based applications to utilise intranets, spreadsheets, presentations, hosted video sharing and Gmail. Macquarie University recently announced that it will be rolling out tailored Gmail accounts to all of its staff.

It is therefore not a question of if cloud computing will be adopted - it is already here - but rather how long will it be before it is adopted wholesale by business. As seen from the Gartner survey noted above, 2010 is the year CIOs will be seriously considering cloud computing. Are you ready?

WHY USE IT?

Substantial upfront and ongoing cost savings - generally the economies of scale that suppliers can generate through sharing infrastructure costs over many users can dramatically reduce the total cost of ownership (and users can almost eliminate the need to own a significant amount of hardware). In addition to reducing overall costs, the popular 'pay as you use' model means that you are not paying for unused capacity as your costs are aligned to your actual use.

Flexibility - using a common resource provides almost immediate elasticity and scalability which are not bound by the constraints and limitations of your particular hardware or current IT resources.

Time to market - compared to traditional forms of IT infrastructure roll-outs, adoption of many types of new technology or services can be almost immediate (often negotiating the right contract is the only thing slowing you down).

WHAT ARE THE PROBLEMS?

The most common concerns with the cloud models are:

- **Privacy** - in the cloud computing model data (including personal information) is often stored in the most cost effective location(s), which may be offshore.These locations may or may not have privacy protections that are the same or similar to those of Australia.

1. Gartner EXP CIO report "*Leading in Times of Transition: The 2010 CIO Agenda*"

- **Security** - cloud computing uses a decentralised model to deliver IT services and can take data out from behind the customer's firewall (a key part of the traditional IT security infrastructure). In moving to such a model, can appropriate levels of security be maintained?
- **Regulatory** - can cloud computing be used while still complying with any relevant regulatory (eg APRA) requirements?
- **Legacy** - how will moving to the cloud affect your existing IT infrastructure and software licensing arrangements?
- **Practical** - how should connectivity and disaster recovery issues be addressed when using the cloud.

But these concerns are not wholly new or limited solely to cloud computing. Similar concerns have been raised and dealt with in the past, particularly in respect of outsourcing and offshoring models, in particular.

Privacy

Privacy concerns and the loss of physical control over data are often cited as the major impediment to the growth of cloud computing and its wide adoption by business. However, there is nothing about cloud computing that is inherently incompatible with privacy protection or that raises issues which have not been dealt with in other contexts.

The Privacy Act 1988 (Cth) sets out ten National Privacy Principles (**NPPs**) which regulate the collection, use and disclosure of 'personal information' (being information or opinions about an individual whose identity is apparent or can be ascertained from that information) by the private sector. It is important to note that the Privacy Act only relates to 'personal information' - it does not apply to anonymous or purely statistical information.

NPP 4 (*Data Security*) provides that an organisation must '*take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure*'. As cloud computing is de-centralised and internet based there is a perception that it is inherently less secure than traditional IT models of data stored on hardware located at the premises of the customer (or supplier in the case of traditional outsourcing). However, a major cloud computer supplier will argue that their size and expertise allows investment and attention to security significantly in excess of what a normal in-house IT department (or small outsourcer) can deliver.

Regardless of one's view of this argument, it is common sense, when putting personal information into the cloud, to investigate and understand the mechanisms and protections your supplier will use to protect your information (including the personal information of your customers and employees). If you are not satisfied with the supplier's security standards, find another supplier!

You should ensure that your service agreement contains appropriate obligations on the cloud computing supplier so that security arrangements are implemented to ensure that all personal information is safeguarded and secure.

NPP 9 (*Transborder Data Flows*) regulates the transfer by an organisation of personal information about an individual to a different entity in an offshore location. Given that the internet is not bound by geographical boundaries, the issue of offshore transfers of personal information has special relevance to cloud computing. NPP 9 currently permits such transfers in a limited number of circumstances, including where:

- the organisation reasonably believes that the recipient is subject to a law, scheme or contract which upholds principles similar to the NPPs; or
- the individual consents to the transfer; or
- the transfer is necessary for the performance of a contract between the individual and the organisation or for the benefit of the individual.

In practice, these obligations are commonly dealt with by obtaining consents from the relevant individual and/or placing contractual obligations of privacy on the supplier.

Practical steps that you can take to manage privacy issues are:

- Ensure your customers are informed that their data may be processed and/or stored in the cloud.
- Ensure your contract with your cloud supplier has strong privacy obligations, and preferably, indemnities with respect to losses resulting from privacy related breaches.

Future developments: On 14 October 2009 the Government agreed to recommendations to significantly tighten privacy law with respect to offshore transfers and to now focus on the ongoing 'accountability' of the sender of the information (being a fundamental change from the current position of prohibition, unless exceptions apply).

One of the key changes relates to the offshore transfer exemption which permits offshore transfers where the recipient is subject to a law, scheme or contract which upholds principles similar to the NPPs. In the Government's view, placing contractual obligations of privacy on a supplier, in itself, will no longer be an adequate protection of privacy.

These reforms will lead to increased focus on which non-Australian jurisdictions the data may be sent to. Customers will want to place obligations on their cloud computing suppliers to only store their data in nominated countries which they believe have privacy protections compatible with Australian privacy law.

The Government has recommended guidance be prepared by the Privacy Commissioner explaining which circumstances constitute an offshore 'transfer' for the purposes of NPP9. This guidance will be highly relevant to cloud computing. The Government has noted that the data transfer principle is intended to apply to personal information accessed or stored outside Australia but not to any personal information that may be routed or temporarily stored outside Australia. It may be that certain types of cloud computing, with infrastructure primarily in Australia, will not constitute an offshore transfer!

Security

Moving to the cloud inevitably means relinquishing a degree of control over your IT infrastructure and relying on your cloud provider to ensure that your information is kept secure.

Many of the major IT providers are starting to offer alternate forms of cloud computing such as 'private clouds' and 'shared private clouds' (in contrast with the more common 'public cloud').

Adopting the concept of private networks, suppliers can design solutions to deliver some of the benefits of cloud computing while keeping key IT infrastructure within the customer's physical or virtual control or within a specified geographical boundary. In the case of shared private clouds, customers that share similar security requirements can become 'tenants' within a private cloud that meets their particular collective security and operational requirements. An example is the UK Government's proposed G-cloud in which Government Departments will be able to obtain on-demand IT services from a number of different IT suppliers through the G-cloud.

You should ensure that all required security arrangements are reflected in the cloud services contract and that you have access and audit rights to verify that the promised security mechanisms and standards are being complied with.

Regulatory

Certain regulated entities, such as APRA licensees, have additional IT security and operational requirements under their applicable licences. Of particular relevance to cloud computing is the new Prudential Practice Guide 234[2] (**PPG234**) which provides high level guidance for regulated entities as to how they should address the issues of IT security. PPG234 recommends that disaster recovery arrangements should seek to ensure that an Australian regulated entity maintains control over assets that relate to the Australian operations through:

- Documentation identifying the relevant assets.
- Sufficient segregation to allow separation of assets if required.
- Contractual protection to ensure access to assets.

A regulated entity should ensure that using a particular cloud computing services model will meet their license obligations.

Legacy

Save for wholly new IT requirements, moving to the cloud can require transitioning away from existing physical IT infrastructure and migrating existing data and licensed software into the cloud.

Your appetite for the cloud may depend on the position in the life cycle of your existing infrastructure. If you have just completed a major hardware refresh, you may be reluctant to make your brand new hardware redundant. However, as noted below, the cloud is not an 'all or nothing' proposition and you could transition parts of your business into the cloud as and when existing IT hardware / infrastructure needs replacing.

If your intention is to put existing legacy applications into the cloud then, apart from satisfying yourself as to any security and performance issues that may arise, you will also need to consider whether the terms of the relevant software licence permit and/ or are compatible with the cloud.

2. *PPG 234 - Management of security risk in information and information technology.*

Where the licence fees are based on the number of servers the software is installed on, for example, some software vendors may view your move to the cloud as an opportunity (although presumably short sited) to derive additional licence fees. However, software vendors are increasingly recognising the importance of the cloud and are, accordingly, offering more flexible terms to their customers. When moving to the cloud you should review your existing software licence terms and, if necessary, raise any concerns you have directly with your software vendors. If no resolution can be reached, at the next break-point you may choose to move to a software vendor whose licensing models do support the cloud.

Practical

A key function of an IT contract is to describe the supplier's service performance obligations and set out a mechanism to ensure such performance. Cloud computing contracts are no different. However, as cloud computing services are delivered primarily through the internet, particular attention needs to be paid to exclusions of liability due to internet unavailability.

You should also seek to confirm with your supplier that your retained IT and communications infrastructure will be appropriate to 'connect' to the supplier's cloud.

Disaster recovery processes and infrastructure are also important to help ensure service continuity and protect against data loss. For many types of IT contracts this means building resilience into IT infrastructure and having a main IT centre being supported by a remote back up location. Given that cloud computing is based on a variety of de-centralised models, traditional forms of disaster recovery are not always possible or appropriate. When negotiating with a supplier, ask them to explain their disaster recovery and business continuity processes and infrastructure and ensure your contract places appropriate obligations on the supplier as regards these matters.

BEFORE YOU JUMP INTO A CLOUD!

Do your homework! Take time to investigate and understand:

- The types (eg personal information, sensitive information, confidential information) and sensitivity of the data you want (and do not want) to put into the cloud. Understanding the data in question is key to the privacy and security issues.
- What obligations (e.g. contractual, privacy, regulatory, business confidentiality) you have with respect to the data.
- Do the terms of your existing software licence permit moving the software into the cloud? What consequence would a move to a cloud model have on the licence fees?
- Where your supplier's infrastructure and data centres are based and where (i.e. which country) will your data be stored? Will your data be subject to potential access by foreign governments (under laws such as the US Patriot Act).
- What security protections will the supplier use to protect your data.
- The reputation and track record of your supplier - how reliable are they.

When negotiating your agreement with the supplier try to include:

- A specific provision under which you retain ownership of the underlying data.
- Rights to audit and access the data.
- Rights to audit the supplier's security arrangements.
- Return of the data when the agreement is terminated / expires.
- Meaningful service level agreements and maintenance obligations.
- Disaster recovery obligations.

Your ability to negotiate contractual measures and protections will depend, as usual, on your relative bargaining position, the contract value and the type of services. If, in the circumstances, it is not possible to have key provisions included in the contract then you will need to assess the risks of proceeding without these protections against the benefits you will receive.

CONCLUSION

What cloud computing offers to customers is choice (a very cost effective choice!). In most cases, cloud computing can provide users a compelling mix of security and privacy safeguards, cost effectiveness and service performance. However, it is not an all or nothing proposition - cloud computing allows a user to dip their toe in the water and to choose which toe to dip!

Of course there are data, security, regulatory and practical issues that need to be addressed and managed, as there are in respect of all IT services. However, cloud computing is not totally new (ie the issues have been seen and dealt with before).

The flexibility and scalability of the cloud allows customers to balance any issues and perceived risks against the significant benefits of using the cloud and to create a particular cloud model which is most appropriate for the requirements of their specific business.

IN SUMMARY:

- While commentary on cloud computing has raised concerns such as privacy and security, no wholly new risks arise in respect of clouds that have not already been identified and successfully managed in other IT models.
- When considering moving to the cloud, identify and raise all potential issues early on in the process. Work with your supplier to see what cloud model, or mixture of models, is most appropriate for your data and particular circumstances. No 'legal issue' is insurmountable.
- The service agreement with your cloud provider should address all of your particular concerns including issues such as data security, privacy and service performance.
- Australian privacy law will soon undergo significant reform and impose stricter controls on the use and overseas transfer of personal information. When enacted these reforms will impact on the legal requirements when placing 'personal information' into the cloud. These reforms should be considered now when determining your cloud strategy to minimise the need to substantially revise your arrangements once the reforms are enacted.

For further information, please contact:

Alec Christie, Partner
Tel +61 2 9286 8237
alec.christie@dlaphillipsfox.com

Richard Smith, Senior Associate
Tel +61 9286 8605
richard.smith@dlaphillipsfox.com

DLA Phillips Fox's lawyers are at the cutting edge of the legal issues relating to cloud computing and ensure our clients comply with best practice and applicable privacy and related legislation.

ABOUT DLA PHILLIPS FOX

DLA Phillips Fox is one of the largest legal firms in Australasia and a member of DLA Piper Group, an alliance of independent legal practices. It is a separate and distinct legal entity. For more information visit www.dlaphillipsfox.com

DLA Phillips Fox offices are located in Adelaide Auckland Brisbane Canberra Melbourne Perth Sydney and Wellington. A list of DLA Piper offices can be found at www.dlapiper.com

SUSTAINABILITY

In line with our commitment to sustainability, our paper is produced using processes that conform to ISO14001 and EMAS.

COPYRIGHT

www.dlaphillipsfox.com

RNC01/DPF2084/0310

MORE INFORMATION

Contact your nearest DLA Phillips Fox office:

ADELAIDE

Level 14, 100 King William Street
Adelaide SA 5000
Tel +61 8 8124 1811
Fax +61 8 8231 0014
adelaide@dlaphillipsfox.com

AUCKLAND

209 Queen Street
Auckland NZ 1010
Tel +64 9 303 2019
Fax +64 9 303 2311
auckland@dlaphillipsfox.com

BRISBANE

Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
Tel +61 7 3246 4000
Fax +61 7 3229 4077
brisbane@dlaphillipsfox.com

CANBERRA

55 Wentworth Avenue
Kingston ACT 2604
Tel +61 2 6201 8787
Fax +61 2 6230 7848
canberra@dlaphillipsfox.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
Tel +61 3 9274 5000
Fax +61 3 9274 5111
melbourne@dlaphillipsfox.com

PERTH

Level 32, St Martins Tower
44 St Georges Terrace
Perth WA 6000
Tel +61 8 6467 6000
Fax +61 8 6467 6001
perth@dlaphillipsfox.com

SYDNEY

201 Elizabeth Street
Sydney NSW 2000
Tel +61 2 9286 8000
Fax +61 2 9283 4144
sydney@dlaphillipsfox.com

WELLINGTON

Tower Centre
50 - 64 Customhouse Quay
Wellington NZ 6011
Tel +64 4 472 6289
Fax +64 4 472 7429
wellington@dlaphillipsfox.com