The potential for cloud computing services in Australia

A Lateral Economics report to Macquarie Telecom

October 2011

LateralEconomics

CAPABLE, INNOVATIVE, RIGOROUS

Overview

Background

Macquarie Telecom asked Lateral Economics to develop a report on the opportunities for Australia to establish itself as a regional hub for the provision of cloud computing services.

This paper discusses the benefits and economic drivers for users of cloud computing services as well as the competitiveness factors that influence where the providers of cloud services choose to locate their facilities. We emphasise the legal jurisdictional risks and potential costs associated with the extra-jurisdictional nature of cloud computing. We also explore issues related to the regulatory and legal settings that are likely to encourage cloud computing services to locate in Australia.

A Regional Cloud Hub – The cloud computing opportunity for Australia

'Cloud computing' is a significant opportunity for Australian industry. Ibis World estimated Australian cloud revenues at over $1 billion for 2010 and employment at around 4,300 persons.

When it comes to cloud computing, can Australia reasonably aspire to become a regional hub for cloud computing? What will determine Australian industry's competitive position in offering cloud computing services and facilities? To what extent will Australian providers meet Australian demand for cloud services? Will Australia aspire to its usual back office role – with a few scraps badged as local content, or will it aspire to something more?

Activity to date suggests there is reason for some confidence. If we were destined to become a cloud computing backwater we'd have seen less investment in cloud infrastructure than we have – for example Macquarie Telecom, Fujitsu and Telstra combined have invested nearly $1 billion in Australian cloud infrastructure. What can and should we do to encourage the nascent cloud computing industry in Australia?

Experience tells us that for a nation to be a hub for any industry requires a combination of factors: a well designed regulatory and policy environment, some environmental advantages and a willingness to identify and remediate if possible any areas of disadvantage. As discussed below, the nascent international policy environment for cloud services has important features in common with the financial services market.

Australia's opportunity is to develop a world-leading regime for cloud services – a better, not equal, cloud ecosystem to that of other jurisdictions. We must understand who are our competitors and how we stack up against them.

Getting this right will be critical to not only encouraging Australian businesses to buy Australian cloud services, but also to maximising the extent to which overseas businesses and consumers will find such services attractive. It must finesse a range of important potential policy trade-offs in areas such as national security, copyright, organised crime and other problems of legal enforcement in the network.

Our 'intangible infrastructure' – our governance – is a major asset. Our political stability and the stability, transparency and integrity of our institutions stand us in good stead, putting us on a par with Singapore and Hong Kong.

But the key for Australia to become a leader and not a follower is to understand that many services are increasingly a *co-product* of competitive service providers (usually from the private sector) and government regulators. The United States Patriot Act brazenly declares the US Government's right to access anything it wants from any cloud infrastructure over which it can claim jurisdiction. That creates a demand for cloud computing services that are not subject to such capricious hazards.

Partly in response to the kinds of sovereign risks that this engenders, the Australian Government has prevented its own agencies from holding personal information offshore. Other countries have made similar decisions.

Suddenly the market for exporting cloud computing services starts looking quite like the market for exporting financial services. Apart from a handful of tax havens, successful exporters of financial services – like Singapore, Hong Kong, London, Luxembourg and even Ireland despite its current woes – are all characterised by a powerful combination of competitive efficiency and export-oriented regulation. Thus, amid vigorous domestic competition, regulation pays assiduous attention both to ensuring integrity and to advantaging exporters by harmonising regulatory regimes with export in mind.

The Australian government's prohibition of its own agencies storing personal information offshore makes it a valuable 'anchor client' for Australian cloud services providers. But just as Swiss banks are attractive to global depositors, in substantial part because of supportive Swiss regulation, so the Australian government should regulate the cloud so that we're a preferred provider for firms, governments and other users offshore. Indeed Australian governments should be prepared to import cloud services from any country that gives them similar confidence and that will mutually recognise our own offerings to them.

This type of solution does not necessarily imply heavy-handed regulation by government. The cloud computing industry is likely a good candidate for effective self-regulation. The general concern with self-regulation is that industries will maintain appearances but skimp on discipline and enforcement. In the case of cloud computing, however, trust and the minimisation of uncertainty are absolutely critical to the success of individual cloud service providers and the industry as a whole. This can be expected to provide a strong incentive for effective self-regulation.

The optimal outcome for regulation is probably a combination of government legislation and industry self-management with government setting the ground rules on issues such as privacy and industry handling things like standardisation of contract terms and security practices. This should be done in a way that is cognisant of the differences between its obligations to its domestic citizens and the needs of users in other countries who do not rely on Australian authorities to protect their interests (but who may wish, at a cost, to avail themselves of some such services).

Recent industry engagement has alerted us to the moves of a group of Australian-based companies that are looking to develop a self-regulatory approach to provide users with confidence regarding the integrity of their data. We believe that such moves, if they come to fruition, should be commended as providing the means for ensuring the regulatory environment keeps pace with the rapid evolution of cloud services.

That said, Australia does face significant challenges. Because of our remoteness and the capacity of undersea cabling to the rest of the world, we suffer from capacity, congestion, cost and latency issues that disadvantage us against other locations closer to large markets. In addition there's our high and volatile dollar and the rapidly maturing cloud services industry emerging in the US, particularly through vendors such as Amazon Web Services and Google. The US also has the world's largest and deepest market for Internet services of all kinds populated by relentless entrepreneurs and deep-pocketed venture capitalists. It regularly throws up companies like Facebook, Twitter and Flipboard. Governments have not been idle concerning the opportunities presented by cloud computing with initiatives by US, UK, European and Japanese governments to establish their own capacity in the cloud services sector. Singapore and Hong Kong have likewise identified the provision of cloud computing as a priority for their own development.

With the rollout of the NBN, Australia will have one of the world's best nation-wide infrastructures for fast onshore data transfer, which will promote business and consumer confidence in cloud solutions. A question mark remains, however, over the extent to which Australia's domestic backhaul capacity and international data links to points of interconnect with the NBN which will hold back communications performance and limit the development of our cloud computing industry.

Latency – the time it takes for signals to pass from user to server in the cloud and then back again – and the cost of undersea cables running thousands of kilometres to and from Australia, cut both ways for the future of a domestic cloud industry. On the one hand, they create substantial natural protection for Australian suppliers of cloud computing services. This creates strong incentives for capacity to be installed in Australia to service those domestic users who are disadvantaged by latency problems where they rely on the cloud infrastructure of other countries. But it can also be a barrier to Australia becoming an exporter of cloud services to the region and beyond.

Opinion leaders in the industry differ about how much cloud computing in Australia may be subject to the 'tyranny of distance' and over ways to manage and mitigate this. However much it is a constraint, this should not stop us from establishing the institutions that would facilitate the export of cloud computing services to the maximum possible extent. In any event, in those cases where latency is a potential issue there are a wide range of sophisticated options available for reducing delay. These include network route optimisation, caching of data and high performance transmission links. Smart application design is also increasingly used to keep latency effects to a minimum.

The Competitive Analysis: Some conclusions about cloud computing in Australia

The considerations outlined above and discussed in more detail in the body of the report below lead us to the following conclusions:

The Australian industry has natural protection and competitive advantage from two sources:

- Firstly, the 'tyranny of distance'. Like high transport costs in the 19th century, the relatively high latencies imposed by our distance from major digital markets mean that:
  - Australian industry has some strong advantages in supplying some parts of the domestic market (where low latency is critical) and
  - Australian industry may aspire to reasonable competitiveness in supplying parts of the export market particularly where low latency is not a critical requirement.
- Secondly, regulatory security.
  - We have strong regulation and high levels of government and regulatory integrity.
  - We have a good capability to develop and manage industry self-regulation (and the cloud services industry has a strong self-interest in effective self-regulation).
  - This gives local services some advantages – particularly in juxtaposition with some of the unattractive regulatory impositions of competing countries like the US (in particular the Patriot Act).
  - This is particularly true where Australian governments seek cloud computing services but wish to avoid exposure to risks arising from foreign regulation.
  - Superior regulation could help facilitate export growth in two ways:
    - Firstly we could pioneer a careful separation between the regulation of local supply and export so as to exempt foreign purchasers of Australian cloud services from any regulatory requirements that exist in Australia solely to protect Australian users.
    - Secondly we could allow foreigner purchasers of cloud services to 'opt in' to that regulation should they wish.

  These strategies of carefully discriminating between the regulation of domestic and foreign users are pursued both by Australia and other countries in areas such as the export of finance and education.

The cloud computing industry appears to face higher costs in Australia than in our major competitor countries due to:

- market immaturity
- lack of scale
- higher costs to and from offshore markets

With an open and vigorous strategy, Australia maximises its chances of growing the cloud sector domestically and 'owning' the local market. This would be a significant achievement in adding value through import replacement. Given the current state of our international and long-haul communications links and their high cost, the objective of export-driven growth remains a challenge, and there are actions for governments to consider if they wish to ameliorate these. But a large and competitive domestic industry will be well placed to seize export opportunities in specific niches where they can wrest some advantage against competitors should circumstances change – for instance where there is increased international communication capacity, a fall in the value of the Australian dollar or a favourable shift in relative energy prices.

Recommendations for Government

Governments can play a role in assisting the development of cloud computing in Australia by:

- being an anchor source of demand, though governments should direct their business to Australian providers on their merits, and on the merits of Australian supply, not in the form of purchasing preferences.
- facilitating and expediting government and industry collaboration to clarify and agree on the application of existing legislation to cloud computing, particularly in relation to privacy and data security.
- collaborating with industry to define a code for industry self-regulation that addresses issues such as standard terms in contracts and obligation to notify of security breaches.
- collaborating with industry to develop export-oriented legislative and self-regulatory settings for cloud computing. In particular, where they are servicing export customers, Australian cloud service providers should be able to opt out of certain regulatory strictures designed to protect Australian resident people and corporations.
- collaborating with industry to ensure its policy and regulatory framework promote Australia as a data centre hub in the same way that the Singapore government is proposing a general data protection law to strengthen Singapore's position as a trusted hub for data processing industries such as cloud computing.
- investigating the state of competitiveness and pricing in domestic backhaul communication links and international links with a view to optimising public expenditure on communications infrastructure.

- governments at higher levels might be able to constructively assist in the orchestration of demands for cloud computing services from governments at lower levels. For instance the Cloud Computing Task Force report talks about the scope for local government to use the cloud, and the cloud should be a powerful source by which successful innovation in one government can be taken up by others. Federal or State governments might be able to help by rewarding councils and/or vendors with the most attractive proposals for common cloud services perhaps through competitions with set prizes attached – including advance purchase undertakings.

Table of Contents

1 What is cloud computing and what are its benefits, costs and risks?

There are many definitions of cloud computing. Three examples serve to illustrate the range of definitions:

According to IBM (2009):

> *Cloud computing can be loosely defined as using scalable computing resources provided as a service from outside your environment on a pay-per-use basis.*

Microsoft (2011) offers a narrow definition:

> *just-in-time provisioning and scaling of services on shared hardware.*

The U.S. National Institute for Standards and Technology defines cloud computing as:

> *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

At this stage there seems to be little consensus about the definition of cloud computing. The term 'cloud computing' is in vogue recently in Australia and now encompasses many different types of services sometimes including traditional web hosting services.

Cloud services are typically divided into the following categories:

Software-as-a-Service (SaaS): complete business applications delivered online. For example, Salesforce.com, Microsoft Live, Oracle CRM On Demand, Google Apps.

Platform-as-a-Service (PaaS): delivery online of an application development or deployment environment in which applications can be built and executed. For example, Force.com, Microsoft Windows Azure, Google AppEngine, Sun Project Caroline.

Infrastructure-as-a-Service (IaaS): online delivery of virtual infrastructure components such as server processing, Internet, and storage capacity. For example, Amazon EC2, GoGrid, Rejila.

In addition, there are further distinctions pertaining to the openness of the cloud service:

Private cloud: a pooling of IT resources by an organisation for internal use and access via a browser over IP protocol over an internal network.

Trusted cloud: pooled internal resources but accessed over a private link or secured public link to the service provider.

Public cloud: computing delivered using a pool of shared resources to any organisation over a public Internet connection.

1.1 Cloud computing: advantages and trade-offs

Cloud computing presents a number of potential costs, benefits and trade-offs:

Lower costs: lower unit capital and operational costs associated with delivering a particular set of IT services can be delivered under the cloud computing model because of the economies of scale and scope available to cloud providers. These economies include not only the expected scale economies in capital equipment, but also those in expertise and any intellectual property used by the provider, typically in the form of proprietary software.

Scalability: cloud computing offers customers the ability to start small and increase the scale of operations in a very smooth manner without the need for large capital outlays. The cloud service provider, in effect, outlays the capital and then passes the service onto the customer on an incremental fee for capacity basis. This ability of cloud service vendors extends to concepts such as flexibility and customisability whereby users can change the services they purchase as their needs change with the myriad indivisibilities being handled within the cloud, which can aggregate the demands of many users.

Security: in the cloud, security needs to be considered from two perspectives. First, there is vulnerability to hacking attacks from outside. On average, we might expect cloud service providers to have more expertise at securing facilities from external attack than any particular corporate entity (although generally speaking the larger the entity the less true this may be). Nonetheless, the cloud services user faces risks associated with data misuse by the cloud provider, which could be a matter of the provider's policy or disgruntled employees. Second, some security risks arise for users of cloud services from the fact that their data is held offsite by third parties. Security risks may arise because data is held in a foreign jurisdiction and subject to local laws, which may include rights to interrogate or seize data. Thus, jurisdiction-specific regulation and laws are an important consideration in determining the attractiveness of cloud computing facilities at alternative locations.

Availability: an important concern for users of cloud services is continuity of access to their data and applications. In moving to cloud services a user is exposed to the additional risk of the failure of Internet connectivity – if a user does not have Internet connectivity then the cloud services are not available. A counter argument to the significance of this risk is that organisations are now so dependent on network access that non-access to the Internet is incapacitating anyway. This is particularly so in the case of organisations with multiple sites. It can also be argued that, in any event, organisations also face the risk of *internally* provided IT services becoming unavailable due to internal failures. Third party cloud providers may be less subject to such failures.

As can be seen from the foregoing discussion, cloud computing offers clear cost advantages. However, these must be considered against a set of other trade-offs that complicate the decision to move into the cloud and which depend on the specific circumstances of individual firms. Also, firms do not face an all-or-nothing choice. Most firms will make incremental forays into cloud services and the data and applications that are most central to their operations may never be moved into the cloud.

1.2 Legal and jurisdictional risks

Recently there has been growing awareness that the use of cloud services presents firms with some new categories of risk.

A key new source of risk for users on cloud computing services is that associated with the storage of data and the execution of transactions in foreign jurisdictions. Cloud customers may be unaware of where their data is being stored. In fact, the location of any particular data set and the processes associated with it can be highly dynamic responding to providers' efforts to minimise costs, especially electricity costs. As Kien Le *et al.* (2010) put it:

> *Cloud service providers operate multiple geographically distributed data centers. These data centers consume huge amounts of energy, which translates into high operating costs. Interestingly, the geographical distribution of the data centers provides many opportunities for cost savings. For example, the electricity prices and outside temperatures may differ widely across the data centers. This diversity suggests that intelligently placing load may lead to large cost savings.*

At any point in time the data belonging to a particular cloud services customer could even be in several jurisdictions. The nature of the risks associated with this characteristic of cloud computing is that the data may be subject to the privacy laws (which may differ markedly from the privacy protection a customer enjoys in its local jurisdiction) and the powers of government in that jurisdiction. This could include the right to control, access and seize data. The material risk for cloud-using organisations is that such outcomes could result in legal action by their end customers and/or significant financial or reputational damage.

These risks are increasingly being brought into focus by industry commentators and Government experts. For example, The Hon Brendan O'Connor MP, Minister for Home Affairs and Justice, Minister for Privacy (2011), emphasised the need for businesses to ensure the security of their customers' information and the difficult jurisdictional issues arising from location of personal information in foreign jurisdictions.

Department of Defence (2011) recommended directly against outsourcing information technology services and functions outside Australia:

> *DSD strongly encourages agencies to choose either a locally owned or foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian border. A risk assessment should consider whether the agency is willing to trust their reputation, business continuity, and data to a vendor that may transmit, store and process the agency's data offshore in a foreign country.*

AGIMO's Draft Cloud Computing Strategic Direction Paper (2011) argues that the "legal/contractual, economic and security aspects of cloud computing are still relatively immature". Research undertaken for Macquarie Telecom (2011) on cross-jurisdictional risks concluded:

- regulatory compliance risks need to be addressed. For example, APRA guidelines require authorised financial services institutions to notify APRA of any transfer of data offshore to demonstrate the appropriate risk management procedures are in place;
- the disparities in the privacy regimes among, for example, Singapore, the US and Australia should be factored into any business case for offshoring data (Singapore lacks unified and comprehensive data protection and does not constitutionally recognise a right to privacy, although the Singapore government is working on a new data protection law in part to ensure Singapore is competitive in the International cloud computing market; the US lacks a national privacy regime);
- storing data in Singapore or the US could give rise to a tax liability even if no business as such is transacted in those markets (for example hosting a transactional website in the US could create a taxable presence in the US for both federal and state tax purposes);
- data stored offshore is subject to the laws of the jurisdiction. Singapore has more than 160 disparate, sector-specific laws regulating the use and disclosure of data in Singapore, and failure to comply with these laws may prove costly in fines, revocation of operating licenses as well as reputation risks;
- data transferred or stored in Singapore or the US may be at a greater risk of being accessed by government and law enforcement agencies than data stored in

Australia (data stored in the US is subject to the US Patriot Act or in Singapore exposed to police investigative power granted under the Computer Misuse Act).

Box One: Australian cloud investment

Major telecommunications operators and technology providers have been committing to significant investment in cloud computing services in the Australian market. Growing demand from industry sectors for access to these services is the main driver behind additional investment.

Macquarie Telecom (MT) has been making substantial investments in cloud computing infrastructure. In FY 2010-11, an additional AUD $ 60 million was committed to data centre expansion. MT's Aidan Tudehope described the reasons underlying his company's investment. "70 per cent of services . . . are deployed in an in-house environment . . . . Customers have real issues at the infrastructure layer particularly around power and cooling and with the global financial crisis… there is no access to capital to improve facilities."

MT is in the process of constructing its second Sydney data centre, 'Intellicentre 2'. The company hopes to capitalise on demand for hosting services. It believes that cloud computing, 'a natural extension of managed hosting, will increase the trend of selective outsourcing of information technology and provide new market opportunities'.[1]

In early 2011, HP announced that it was placing greater emphasis on cloud computing as a core business. In early 2011, it announced that it was developing differentiated cloud services for both the public and private sector and was aiming to corner the market as a provider of cloud computing services to the Government sector with its 'Government Secure Cloud Service'. It has spent AUD $ 119 million on its newly built Eastern Creek data centre. HP stated that its primary goal was to cater to small and medium agencies. The company identifies 'a significant shift in the marketplace' (regarding the importance of cloud computing) as being one of the reasons behind their greater emphasis.[2]

Fujitsu made a recent foray into Australian cloud computing services by offering Infrastructure-as-a-Service (IaaS), which originally served only a niche market. This product, inter alia, provides customers with enhanced support services and enables the self-selection of data storage. In early 2011, the company outlined plans for the deployment of two new data centres (from the existing 10). CEO Mike Foster said that this continuing AUD $ 100 million data centre investment was driven by growth in the financial, government and resources sector. Last February, Fujitsu announced that Toyota had selected it to provide cloud services for its 'TUNE Dealership Management System'.[3]

[1] http://www.theaustralian.com.au/australian-it/macquarie-telecom-jumps-on-cloud-computing-bandwagon/story-e6frgakx-1225995533505

http://www.macquarietelecom.com/about_us/investors/FY11_Annual_Report/Full%20Year%27s%20Directors%20Commentary%20FY11.pdf

http://www.macquarietelecom.com/about_us/investors/FY11_Annual_Report/Management%20Briefing%20to%20Analyst%20FY11.pdf

[2] http://www.theaustralian.com.au/australian-it/cloud-computing-offers-silver-lining-after-hps-poison-tablet/story-e6frgakx-1226124840808

http://www.cio.com.au/article/371575/hp_private_cloud_moves_local/#closeme

[3] http://www.cloudtweaks.com/2011/02/fujitsu-lifts-toyota-into-the-cloud/

http://www.computerworld.com.au/article/384960/fujitsu_ramps_up_data_centre_investment/

Over time, firms will try to develop a view on the trade-offs between risk, performance and cost and how they wish to make them. We would expect that, over time, contracts would evolve to allocate these risks between the various providers and their ultimate customers and that the prices of services would reflect the perceived riskiness of various providers' offerings. It is reasonable to assert, however, that the market still has significant learning and development to undergo and that while this is occurring heightened caution is appropriate. There is the risk that this type of industry maturation may take too long in Australia and lead to an erosion of our long-term competitive position.

In fact, this is recognisably a situation that is difficult for the private sector – as navigating this level of complexity and risk requires a good deal of collaboration between different parts of the system – for instance sellers of cloud services must aggregate a sufficient number of buyers with whom to share the risks of investment, skills need to be built up and standards need to be arrived at. Governments will have some role in this process as their own regulation will have implications for many of these developments (see discussion in Section 3.1 below).

There is also the prospect that government involvement and the complexity of government regulation cranks up risk. Some governments' heavy-handedness, particularly, for instance, the US with its Patriot Act and its assertion of extraterritorial jurisdiction, could offer competitive advantages for the cloud computing suppliers in smaller countries with nimbler approaches.

These considerations have important implications when assessing Australia's potential role as a cloud computing hub.

- As the awareness of cross-jurisdictional risks grows, it is likely that Australian users of cloud services will increasingly prefer Australian providers who store their data within Australia's borders. Having said this, a distinction needs to be made between corporate users that are outsourcing to the cloud significant subsets of their IT functions and consumers who are using cloud services somewhat inadvertently because they are using services such as Gmail, Dropbox and Facebook. In the former case, we can expect corporate users to increasingly prefer Australian services if they judge cross-jurisdictional risks as significant. Consumers, on the other hand, show little sign of objecting to the multi-national cloud services currently on offer. Given this, it is unlikely that those who are concerned will have much choice about where their application-specific data resides.
- To the extent that Australia's legal and regulatory regime for cloud computing is perceived to be less risky than those of other countries, providers of cloud services to the international market may tend to locate their facilities in Australia. This will

depend, however, on the extent of risks and exposures that arise for overseas buyers from taking their data offshore. These may extend to complete prohibitions in some cases – several national Governments have prohibited government departments from letting any personal data offshore.

Box Two: Australian users of cloud services

One large women's retailer, Anthropologie, decided that it was best to outsource its e-commerce platform to a third party as 'the process of building a website in-house can take a very long time...' This platform, provided by Venda, includes a payment system, product database and website design. Larger retailers typically host their own in-house IT system due to pre-existing infrastructure, but the benefits from cloud-based systems for SMEs are obvious. Cloud systems can dramatically reduce cost and improve quality, for instance in the management and analysis of data.

The Australian Information Industry Association (AIIA) observed that investment in cloud computing is crucial if firms in finance desire to maintain the patronage of a generation that will make up approximately 42 per cent of the working population by 2020. This is because Gen-Y values direct/Internet banking over the traditional retail branch system. They appreciate marketing and interaction over social networks and use the web for more complex financial services such as home loans.

In response, local firms such as Westpac have begun to invest in cloud technologies. Westpac does not envisage taking its entire network into the cloud, but instead uses Cisco UCS technology with 300 virtualised services and 40 terabytes of storage for its mid-range platform. The Bank has since deployed Microsoft's Azure platform. When discussing the firm's decision to utilise cloud technology, Ward Britton of Westpac indicated that productivity concerns were significant. Westpac needs data analysis in greater detail than can be easily managed on existing in-house systems. The cloud service model enabled staff to "take the application [Numerix] and the job running on the analyst's desktop, plug in HPC [High Performance Computing] and Azure and 'make it run way faster' and more reliably". The staff member is able to use a mathematical and pricing library that is held via the cloud to aid in calculations.

Healthcare services would greatly benefit from cloud-based solutions, but adoption is stymied by concerns regarding patient confidentiality and fragmented and obsolescent IT systems throughout the sector. Within the context of healthcare, cloud computing would enhance the information sharing on an inter/intra-organisational basis.

Austin Health, a Victorian private healthcare provider has more than 6,000 staff and three hospital sites. The steady increase in patient numbers put significant strain on a dated in-house IT network. Fiona Webster, Austin's strategy, quality and redesign executive director, observed that the company desired improved accessibility, reliability and quality for its data. Microsoft subsequently deployed a cloud system using 4,000 PCs across three sites and two 64-bit servers. The $175,000 network uses a performance dashboard consisting of SharePoint 2007, SQL Server 2008 and Microsoft Office 2007. As a result of this new system, doctors and management are delivered automated consolidated reports on an at-needs basis, and they are able to chart progress against management and Government KPIs.

2 Cloud computing: economic perspective

In many ways, the cloud computing model mirrors the centralised computing architecture model from the ’60s and ’70s that was based on the mainframe computer. In that model both the mainframe computer and the network were internal to the enterprise. The mainframe computer itself was accessed via ‘dumb terminals’ over local enterprise network. An essential characteristic of this system was that end users were separated from the computing resources. In the cloud computing model, warehouse-sized data centres replace the mainframe and the local enterprise network is replaced by the Internet.

A critical enabler for the evolution of cloud computing has been the massive increase in the penetration of IP networks into corporate and consumer markets over the last 15 years. Allied with this have been the falling costs increasing performance and reliability of high-speed Internet connectivity. These changes have created the economic pre-conditions to create centralised computing resources that are remote from end users.

Economics, almost invariably, explains shifts in platforms, management techniques, and technology as driven by changes in the costs of inputs and opportunities to improve the quality of outputs (which are driven by technological and management innovation). In essence, corporate users face a set of tasks and processes involving information acquisition, storage, management, analysis and dissemination, which can increasingly be achieved at lower cost under the cloud computing model.

Therefore, in essence, cloud computing is essentially the effort to lower the costs of information processing and storage by achieving scale and specialisation in hardware and software at centralised facilities.

Cloud computing is typically thought of as a corporate or enterprise phenomenon, and notwithstanding services such as Gmail, Dropbox etc, the introduction of iCloud by Apple in June 2011 crystallises the growing importance of cloud services for individual consumers. In effect, the information management requirements of consumers are analogous to those of corporate users. Particularly useful to the individual user are cloud backup and replication services. Consumers increasingly have multiple devices and need to synchronise files between these devices and to ensure their data is backed up, and this is often best done in the cloud. The very rapid growth of smart phones and tablet computers will also drive cloud growth and consumer awareness of cloud services. These mobile devices typically have small solid state storage (rather than large disk drives) and they will rely on the cloud for storage per se as well as replication.

While the cloud computing industry appears to be on a trajectory for rapid growth, there is a range of factors that may impede that growth and, in the context of this paper, there are factors that may constrain Australia's ability to export cloud services.

2.1 Complexity and coordination

Markets are at their most miraculous when individual firms are able to compete with one another and to innovate in relatively well-defined areas of endeavour. They can be not so good where something new is emerging but requires widespread cooperation, both between firms and with government. This is the situation in which the nascent cloud computing industry finds itself. The industry is still in relatively early stages of growth and has numerous 'chicken and egg' dilemmas. For example, business users will be reassured as technical standards develop that give them confidence in such things as the continuity, competitiveness and security of service and protection from vendor lock in. Yet this requires a great deal of cooperation between both individual firms here and in other countries, among voluntary industry standards bodies and also governments.

Where a firm is contemplating some major innovation, it is likely that the innovation in itself will involve major technical risk. In addition, the firm must have some confidence that the many suppliers it will need will be tolerably competent, knowledgeable and competitive compared with suppliers that might be available to competitors elsewhere. It must believe that it will be able to secure adequate skills in the labour market if it wishes to expand to capitalise on its innovation. And the innovation must be compliant with existing government regulation or the innovator must be confident that regulation at all levels of government will respond to accommodate the innovation where necessary.

The tallness of this order goes some way to explaining why industries so often develop in 'clusters' around pioneer firms that pave the way for others. The Economist Alfred Marshall (1890) explained this phenomenon in terms of external economies of scale. A cluster of skills may grow in a region around pioneers. Manchester had metalworking skills, cotton working skills and trading links and other technical skills, which saw linen and cotton mills established in Manchester. Their existence created a deep market of skilled labour, supplier firms and a growing awareness among the suppliers of capital into which other firms could tap. More recently Paul Krugman (1991) has explained similar phenomena in economic geography.

Hidalgo *et al.* (2007) have documented this phenomenon at the same time as highlighting the ways in which industries and capabilities within regions and countries are dependent on one another's health and competitiveness and also showing how greater interdependencies typify more prosperous, developed economies.

Dani Rodrik has written of the implications of this for economic development in less economically developed countries. For Rodrik, though he would concede the necessity for basic macroeconomic responsibility and the importance of some basic market disciplines,[4] these interdependencies explain why simply freeing up markets is unlikely to produce rapid transformation in less developed economies. In addition to pragmatic attempts to create the conditions where 'clusters' of capability can be established, Rodrik and his collaborator Ricardo Hausmann (2003) write compellingly of economic development as self-discovery of nations, regions and indeed of firms. In so doing they illustrate the potential for deep market failure:

> *Neither economic theory nor management science is of much help in helping entrepreneurs (or the state) choose appropriate investments among the full range of modern-sector activities, of which there could be tens of thousands, once one moves beyond broad categories such as "labor-intensive products" or "natural-resource based products." Yet making the right investment decisions is key to future growth, as it determines the pattern of specialization. In these circumstances, there is great social value to discovering that cut flowers, soccer balls, or computer software can be produced at low cost, because this knowledge can orient the investments of other entrepreneurs. But the initial entrepreneur who makes the "discovery" can capture only a small part of the social value that this knowledge generates. . . . Consequently, entrepreneurship of this type – learning what can be produced – will typically be undersupplied, and economic transformation delayed.*

There are some similarities between the situation for cloud computing services in Australia and this difficult development scenario sketched out by Rodrik and Hausmann. The Cloud Computing Task Force (Global Access Partners, 2011, p. 6) "was advised that as many as 24 different international groups were currently seeking to develop standards relating to aspects of Cloud computing. However, universal agreement on standards for privacy, data protection and authentication remains elusive." There are no 'magic bullets' that can quickly solve these problems – which are natural problems of market development. On the other hand they disclose a situation in which there is a strong collective interest in widespread learning and coordination among different firms and between them and government. One of the things that stands out about cloud computing is the extent to which it is enmeshed with collective disciplines such as industry standards and government regulation. Further, government is a major potential purchaser of cloud

[4] More precisely arrangements that ensure that economic decision making is decentralised to those with the appropriate knowledge and incentives throughout the economy to make the right decisions. Rodrik has written about how incentives on Chinese local government officials have effected very worthwhile transitional changes without privatisation or deregulation.

services. This suggests it has a role to play as a strategic purchaser and valuable early client for a growing industry and also as a leader helping to foster market development by supporting skill development. It should also be sensitive to opportunities it has to facilitate the coming together of potential buyers where they have common interests. Thus, for instance, a government might help facilitate joint purchasing by a number of its own agencies or of governments at lower levels. Federal and/or state governments might encourage local governments to become cloud services users in a strategic and coordinated way.

2.2 The different funding, service and regulatory needs of domestic and export markets

To an increasing extent the market for sophisticated services is dominated by regulation. For this reason, areas like global markets in banking, funds management, health and education are highly balkanised with intense national regulation and in the latter two areas strong government subsidies and service delivery in most countries. Yet there is substantial international trade in all these industries. As a result, countries seeking to expand exports in these areas have found that they can only do so by quarantining many of the regulatory, tax, funding and service delivery underpinnings to domestic consumers and in effect building separate regimes for foreign purchasers of these services.

Australia has become an exporter of education by allowing foreign students full fee paying access to our educational institutions that are not available to Australian domestic students. Other countries have specialised in becoming services entrepot exporters by assiduously crafting regulatory and tax regimes around the needs of exporters of financial services. Australia has attempted to play this game – for instance with offshore banking unit legislation – though not with marked success. We have also made a range of changes to our tax laws to try to ensure that they function as intended to facilitate domestic tax collection and to prevent personal tax avoidance by domestics while at the same time not taxing foreigners who have their money managed in Australia but who pay income tax on their earnings in another country. Some, usually small countries, such as Ireland and Luxembourg, have gone to great lengths to facilitate such trade – which is not typically intended to assist tax avoidance (as tax havens are) so much as tax 'pass-through' or the facilitation of a tax-payer paying tax in one jurisdiction only. The convention by which exporters are exempted GST and pay it in the country of their destination is inspired by a similar principle.

If we are to become an exporter of cloud computing we should think about the very different needs of domestic and foreign users of our cloud computing services. Australia has an interest in a range of regulation that protects its citizens' rights – in areas such as privacy and security. But it has no particular interest in protecting the privacy or security of citizens of other countries. Accordingly it should contemplate a situation in which a foreign user could purchase cloud services from Australian suppliers without a range of Australian privacy regulation attaching to it.

Again there is an analogy with Australia's approach to financial exports. One substantial pension fund managed from Australia on behalf of an Asian Government agency gave that agency the choice of setting up an entity subject to ASIC's regulatory control (together with the higher costs this would entail) and a lower cost entity without ASIC supervision. The holder of the funds plumped for ASIC supervision (Lateral Economics, 2007). This illustrates both why there should be no compulsion on foreign buyers to comply with our regulation (because it is there for the protection of Australians), and also that Australia can in effect sell 'regulation as a service' to offshore buyers who value it. This is essentially the model that drives entrepot services exporters like Ireland and Luxembourg in finance and Delaware, among US states in corporate domicile, regulatory, judicial and other legal and corporate services. Later in this report we suggest that the issue of latency imposes some constraints on our ability to become a major exporter. But this should not stop us from establishing the institutions that would facilitate the export of cloud computing services to the maximum possible extent.

3 An overview of the cloud computing services industry in Australia

Several recent reports point to an acceleration in the adoption of cloud services in Australia. “According to a report by technology service provider Avanade, 71 per cent of Australian companies are using some form of cloud services. This represents an increase of 31 per cent since a similar survey in 2009” (The Australian IT, 2011, p. 1).

Ibis World reports the industry metrics reported in Table One below.

Table One: Key Industry Statistics

Key Industry Figures	2010
Industry Revenue	$1,049.1m
Revenue Growth	1.8%pa
Industry Gross Product	$458.2m
Number of Establishments	726
Number of Enterprises	578
Employment	4,305
Total Wages	$293.4m

Source: Ibis World
http://www.ibisworld.com.au/industry/default.aspx?indid=555

A recent report from Frost and Sullivan states that Australia leads other Asia Pacific countries in adopting cloud computing. In 2011, 43 per cent of enterprises are now using cloud computing in some form and 41 per cent of IT decision makers agreed that cloud computing will continue to be a top priority (International Business Times, 2011).

The Australian Government has recently recognised the need for a data centre strategy for its data-hungry agencies. At present, there is not a unifying strategy and an *ad hoc* approach is taken. The Australian Government Data Centre Strategy 2010-2025 has outlined a unified approach to this emerging issue. It is seeking to harness its bargaining power in order to reduce the prices it pays by making centralised bids for data centre space (AGIMO, 2010; Computer World, 2011).

4 Drivers of competitiveness in cloud computing and Australia's competitive positioning

What are the factors that drive competitiveness in cloud computing – what factors influence how efficient a particular country is in providing cloud competing services?

We will assess Australia's competitive position with reference to three sets of factors:

- Environmental factors – relative cost conditions for cloud computing within Australia
- Business efficiency and innovation in cloud computing in Australia relative to the rest of the world
- The legislative and regulatory environment in Australia.

4.1 Environmental factors

4.1.1 What drives cloud computing competitiveness?

There is a range of other environmental factors that drive competitiveness in jurisdictions in general. These include:

- the cost of electricity
- the cost of hardware
- distance from markets – this is important because of latency and long-distance capacity issues
- cost of telecommunications services usually driven by the scale, regulation and competitiveness of the domestic telecommunications industry
- the cost and capacity of national telecommunications links relative to demand (the probability of congestion)
- ambient temperatures at various locations
- the availability of skilled labour required to design, build and maintain cloud facilities.

The cost of internal (national) data links is also important. In our discussions with industry participants it was suggested that the very high cost of very high speed data links in Australia (as much as 20 times the cost of similar services in the US) is retarding the development of cloud computing in Australia. The NBN, to the extent that it builds better, faster and cheaper backhaul and backbone links, will potentially assist, but the real test will be the delivery of significant improvements in both performance and price once the NBN is deployed.

In discussions with industry participants undertaken for this paper, Lateral Economics was informed that a 1 Gbps link between Auckland and Sydney costs approximately $75,000 per month whereas a similar link between Los Angeles and Vancouver would cost about $10,000 per month.

This level of cost disadvantage is significant when considering Australia's capacity to export cloud computing services. In addition, the quality of cloud service offerings from Australia may be constrained by congestion in Australia's international telecommunications links. It is arguable that upgrading the capacity of these links needs to be factored into the Government's plans for the NBN. The NBN, if widely adopted, is likely to increase significantly the demand for content from overseas and this will place significantly greater capacity demands on our international links.

The Australian Task Force on Cloud Computing Report (2011, p. 25) made the following comment on the issue of international links:

> *While the NBN will greatly increase internet speed and capacity within Australia, some Task Force members, having noted Australia's ranking in the World Economic Forum's Global Information Technology Report 2010-2011 (page 335) which placed Australia at 41 out of 138 countries evaluated, considered that its benefits will not be fully realised until more capable and cheaper international cable access is available to enable participation in the global public cloud. An increase in investment in submarine cable protection and resilience, combined with the NBN roll-out and supportive regulatory framework, could encourage major industry players to invest in constructing global cloud computing capacity in Australia.*

While improving international connectivity will certainly improve data throughput and reduce congestion, the problem of latency can be addressed but not eliminated.

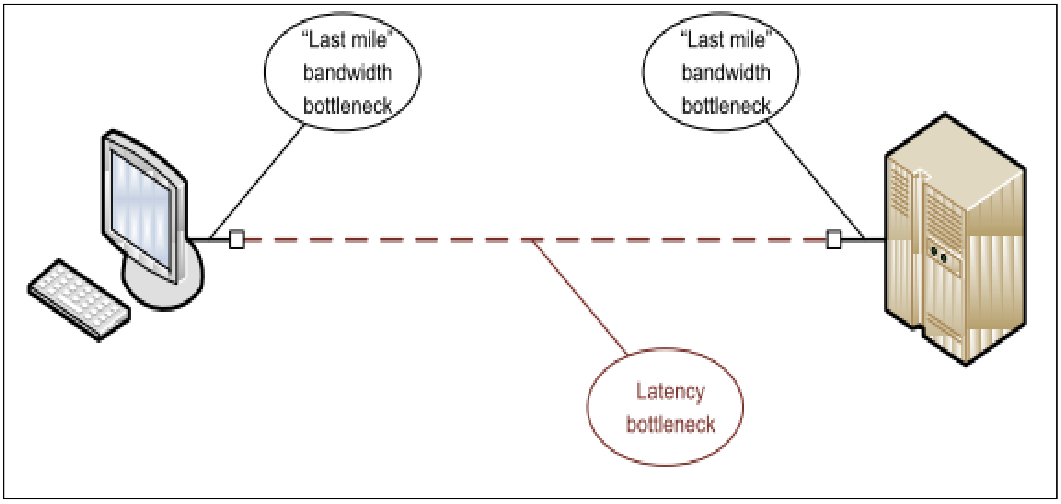
4.1.2 Latency: The tyranny of distance in the world of cloud computing

Latency is a synonym for network delay and connotes the speed of light transmission plus processing times through physical devices such as switches and routers. In many cases, longer latency does not hugely undermine competitiveness and there are plenty of cloud computing services provided to Australia from cloud based services in Asia or beyond.

Further, there is a range of strategies to minimise the effect of latency and in those cases where latency remains as a potential issue there is also a range of options for reducing latency. These include network route optimisation, caching of data and high performance transmission links. Smart application design is also increasingly used to keep latency effects to a minimum.

"Latency" is relevant both to human users and their tolerance for delays but also from the perspective of machine-to-machine communications where thousands or even millions of interactions could occur within the timeframe of minutes or hours. Though digital signals travel at close to the speed of light through fibre optical cable, transmission across the world requires numerous ‘repeaters’ each 40 to 70 kilometres at which point the light signal is converted to an electric signal, put through electronics and converted back into light for the next leg of the journey. The average time taken for a round trip of data from the antipodes to the centres of cloud computing in the US is 150 to 200 milliseconds, Asia 100 to 150 milliseconds and Europe is typically over 300 milliseconds. By contrast the worldwide average round trip time (RTT) to Google services is slightly over 100 milliseconds but within the United States is between 60 and 100ms (Belshe, 2010).

Figure One: Three bottlenecks throttling our speed of access to the Internet


“Last mile” bandwidth bottleneck
“Last mile” bandwidth bottleneck
Latency bottleneck

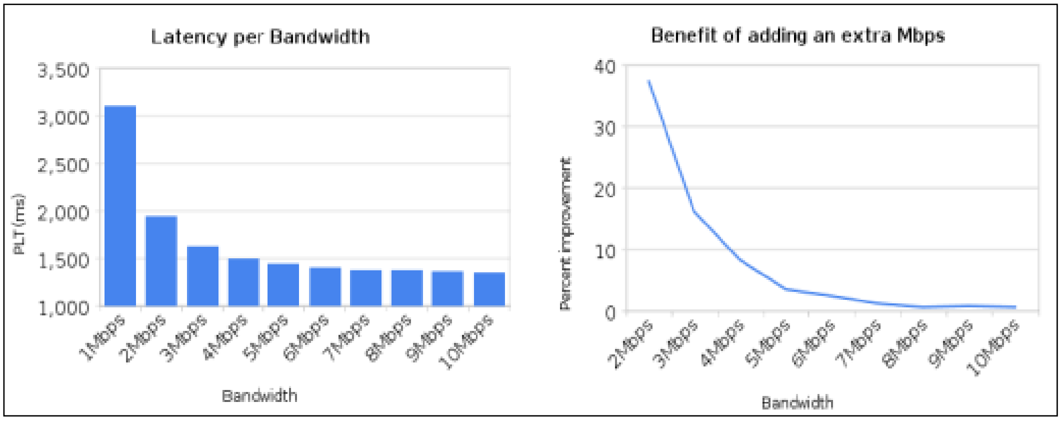
Source: Obren and Howell, 2010.

Belshe 2010 shows that even for fast RTTs of 60 milliseconds, the latency bottleneck imposes heavy diminishing returns on additional bandwidth in the mode of transmission.

Minimising the effects of Latency is a well-understood issue with software application developers. The most common techniques used to minimise the effect of Latency include caching of data, and local processing of data in the browser, not on the host. SaaS applications such as Salesforce.com are hosted in the US, but used globally without latency impacting their adoption.

Given this, and given the importance of latency in the technical capability of systems and in the user experience on websites, it is likely that Australia’s distance from the major centres of cloud computing will be a major source of natural protection for Australian cloud computing. Indeed it is analogous to the natural protection provided by long supply lines for fresh produce. It improves the competitive position of Australian-based suppliers servicing their domestic market because higher quality can be delivered from domestic sources of supply. Supplying cloud services from an Australian base can reduce latency to about 100 milliseconds or less for most round trips. On the other hand it is a handicap for Australian cloud computing providers seeking to compete in offshore markets.

Figure Two: Diminishing returns to bandwidth in delivering speed

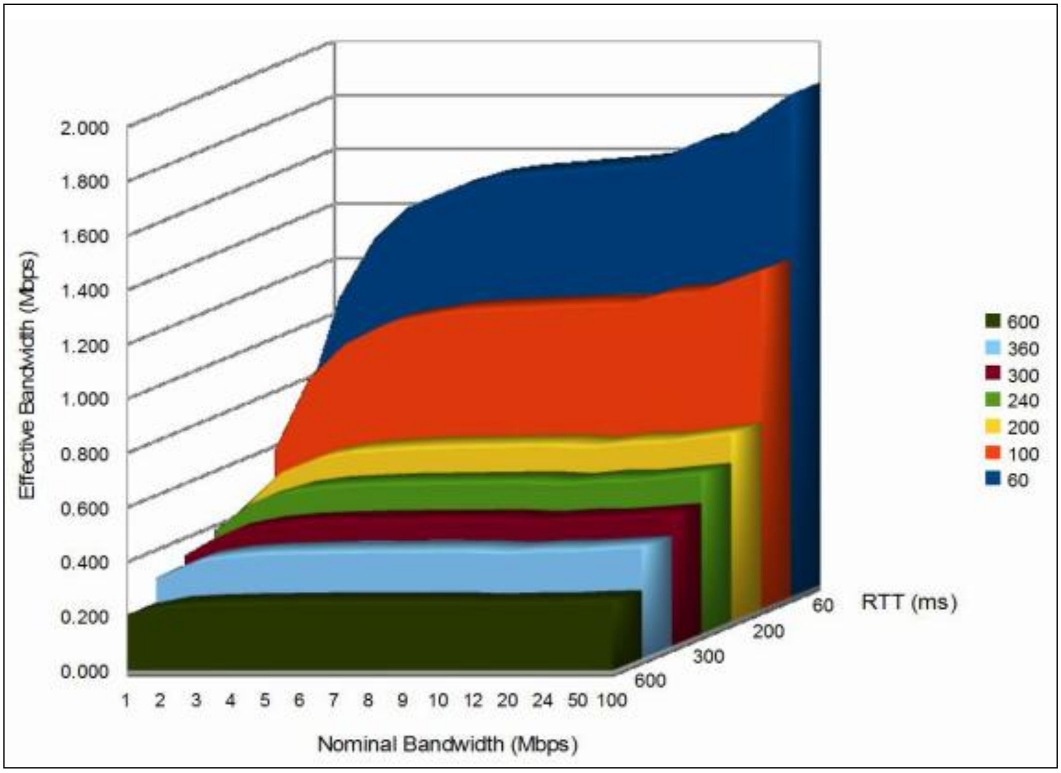


Source: Belshe, 2010, pp. 2-3.

Indeed, as Obren and Howell point out (2010), latency appears to be the most important bottleneck in the speed with which those in Australia and New Zealand access the Internet, making it harder for us to achieve high speeds than most other places that are closer to major cloud capacity. In examining the three potential bottlenecks, they find that the main bottleneck is not ‘last mile bandwidth’ or the speed with which the end user is connected to the Internet so much as the total latency bottleneck as users wait while their signal goes on its round trip to the server (often overseas) and back again.

Obren and Howell then extrapolate these figures to show that stronger diminishing returns set in substantially earlier with RTTs above 200 milliseconds.

Figure Three: Diminishing returns to bandwidth as function of RTT



Source: Obren and Howell, 2010.

While Obren's and Howell's analysis reflects on the likely net benefits of faster broadband speeds, it is also of relevance to Australia's future as a cloud computing hub. For the antipodean distance from the central hubs providing cloud computing means that the gain from faster broadband is likely to be greatest where Australian users of cloud services are serviced from cloud facilities located in Australia.

While decreasing congestion and, to the extent possible, latency would improve Australia's cloud competitiveness, some disadvantages of distance will remain, but these do not preclude Australia from developing export-oriented cloud services in a range of areas. For example, on the demand side, a user of cloud services whose requirements were driven by a need for a particular set of regulatory conditions and for whom low latency was not a key driver might find Australia a relatively attractive provider of services. For example, a provider of mass storage would be more concerned with capacity and less concerned with latency than a provider of online games.

Box Three: A low latency application

Tele-surgery provides a clear example of an application that is highly intolerant of latency delays. Tele-surgery brings surgical expertise to remote areas and underserved populations, helps healthcare providers make better use of expert surgeons, improves surgical outcomes and reduces costs. However, network bandwidth, network latency and jitter are obstacles to the widespread use of this technology. Of great importance to the success of tele-surgery is the round-trip latency from the issuing of a robotic control signal to the resulting video displayed at the surgeon's site. This essentially determines the safety of tele-surgery. If the robotic control signal gets delayed, it will result in a delayed action of the surgical robot (Ciena, 2011). By contrast some other areas of medicine require high bandwidth but are not sensitive to latency – for instance remote and 'round the clock' diagnosis of CAT scans, MRI and radiography.

Another example of how Australia might be competitively attractive is where Australian entrepreneurs develop specific expertise and assets (most likely in the form of proprietary software) in supplying specialist services in particular niches. For example, one industry participant we spoke to exports animation rendering processing where the competitive advantage resides in the ability to complete massive processing throughput in the minimum time.

Box Four: A high latency application

An example of an application for which high latency is not a significant problem is the 'rendering' of high-resolution animation. Rendering involves taking the models of animation and producing final images – in this case, the sequence of frames that will be used in the final version of a movie. This requires very large processing resources. A method for 'off site rendering' is to replicate all of the model data from the site at which it is created to the processing site. All the computation is undertaken at this site and then the finished files are shipped back. Using this method, latency is more or less irrelevant, the primary communications consideration being throughput. This method was used by cloud processing specialist SteamEngine (based in Sydney) to render models for animation firm Rising Sun (based in Adelaide) for the latest Harry Potter film.

4.1.3 Addressing latency and congestion

It is likely, given the magnitude of investment required, that government will need to become involved in the upgrading of Australia's international links. This might be undertaken on the basis of public goods characteristics or the existence of insufficient competition in this market.

It should be recognised, however, that improving the quality and capacity of Australia's international telecommunications links cuts both ways – improved links will also improve the experience of Australian users of cloud services located overseas. In addition, significant cable investments are occurring in the Asia Pacific region and Australia will likely need to invest if it wishes to remain competitive.

While Google has publicly stated that it is not going to enter the submarine cable business in competition with telecommunications operators (2008), its current activities would suggest that in Asia at least it is making significant investments in submarine cable capacity. It has now invested in two major Asian cable projects. In February 2008, Google invested in the Unity submarine cable (value US$300 million) from Japan to the US, which provides 7.68 Terabit/s. Its partners are Bharti Airtel, Global Transit, KDDI, Pacnet and SingTel. It is soon to commence commercial service.

In December 2009, Google announced it was a partner in the Southeast Asia Japan Cable (SJC), which is a 23 Terabit/s cable linking Singapore, Hong Kong, Indonesia, Japan and the Philippines. It is scheduled to be completed in Q2, 2012. Google is working with Globe Telecom in the Philippines; Japan's KDDI; Network i2i, a subsidiary of Bharti; Reliance Globalcom and Telemedia Pacific on this investment. SingTel announced it had also joined in January 2010.

The Federal Government has embarked on an enormous upgrade of Australia's communication infrastructure in the NBN. The ground for this intervention appears to be a mixture of addressing structural competition defects, the existence of positive externalities and public good characteristics. These rationales could equally be applied to Australia's domestic long haul and international communications links.

4.2 Other issues for Australia's competitiveness in cloud computing

One area where Australia has a comparative advantage for cloud computing is in relation to the cost of energy. The cost of energy will be a key competitive driver for Australia as the market evolves, specifically the cost of reliable, base-load electricity. Australia is a net exporter of energy, but much of this is carbon-intensive. Australia, however, has vast potential for renewable energy generation and has enormous supplies of relatively low carbon natural gas.

Data centres are prodigious users of electricity. If in future, as many predict, the relative price of energy increases significantly, Australia could be well placed to capitalise on its cost advantage in this key input for cloud services. Indeed, as the management and technical sophistication of cloud facilities increases we can expect highly dynamic geographic assignment of computer processing and other services in response to minute-by-minute changes in the price of electricity at various locations. Such developments will likely make the distinction between base load and non-base load less important. We can imagine future scenarios where South East Asian regional processing demand shifts to Australia on its many sunny days as the deployment of large-scale solar generation capacity increases. Geo-thermal (hot rocks) generation offers the prospect of not only low environment impact energy, but also good base load characteristics. In fact, the combination of solar and geo-thermal may be a winning combination for powering cloud infrastructure. Realising these scenarios would require investment in fibre optic connectivity to the remote locations. Because it is cheaper to transport photons (information) than it is to transport electrons (energy) and because data centres will always be big users of energy, such scenarios, although seemingly improbably now, may become attractive in the future, especially if world energy prices increase relative to Australia's.

Australia may have some advantages in the quality of its entrepreneurs. Certainly some Australian businesses and entrepreneurs believe that cloud services can be successfully operated from Australia. What is yet to be determined is the extent to which such services will ever be supplied as exports to overseas rather than domestic buyers.

Chief Commercial Officer of SteamEngine (which does export services) Stefan Gillard comments that "Technology and private enterprise will find a way to meet a business need".[5] He believes that a lack of competition in the provision of international data links to Australia is resulting in excessively high prices.

As a general conclusion it seems that the industry is capable of innovating in the provision of cloud services and competing for import replacement and exports. The balance between export and import replacement, and the specific types of services where Australia can be most successful, will reflect the balance between the advantages we presently enjoy and can enhance further (e.g. a favourable and far-sighted regulatory regime) and constraints (the relatively high telecommunications costs and the extent to which they can be reduced to more competitive levels). It is this balance that will determine whether it is too ambitious for Australia to achieve status as a regional hub, but clearly there are factors within the control of the industry and governments that can ensure the most favourable balance is achieved.

[5] Consultant's discussions of this report

Box Five: Cloud computing in Singapore

Infocomm Development Authority of Singapore has been investigating cloud computing opportunities since July 2008 when it engaged Yahoo!, HP and Intel to create a research initiative (Open Cirrus Cloud Computing Testbed). IDA recognises cloud computing as an important paradigm in ICT but is cautious, identifying data security and regulatory compliance as key issues that still need to be improved.

IBM houses a cloud computing laboratory at Changi Business Park (as part of a network of labs in HK, Ireland, Vietnam, China, South Africa, Japan, Brazil, India, Korea and the US) to help business, government and research institutions to take advantage of the benefits of cloud services. IBM is investing a further $38 million into a new cloud data centre for IaaS in Singapore servicing the market in the Asia Pacific region, the size of which is expected to grow to $5 billion by 2014.

Singapore is politically stable, is a centre of finance and trade for Asia Pacific and has access to a skilled workforce. On the negative side, land is scarce and expensive in Singapore.

It is also likely that these high bandwidth costs impact negatively, not only on large firms, but also on smaller innovative technology companies and, in particular, start-up companies that offer consumer-facing web applications. These types of companies form an essential component of the cloud ecosystem in the United States. Companies such as Google and Facebook and a plethora of others started life on an almost experimental basis and were able to scale up their services and run quickly based on the wide availability of low-cost telecommunications services as well as, of course, the deep venture capital markets of the US.

Through innovation policy and competition policy, governments have a role in responding to these issues, which if it is addressed successfully will be important to the growth of cloud computing in Australia.

4.3 The legislative and regulatory environment

As we have emphasised, a key factor driving the demand for cloud services is the confidence and trust that users have in the providers of these services. The track record of the industry will have a significant impact on users' evaluation of its trustworthiness, but, in addition, the adequacy of legislative and regulatory arrangements will also be important.

Over the past 20 years or so, Australia has developed a reputation as a leader in economic reform, regulation and policy design both in terms of government practice and industry self-regulation. In order to provide for the safe and rapid growth of cloud computing in Australia, there is no need for cloud-specific legislation or regulations and such actions could impede the potential of cloud computing. That is, government legislation is not required to address a range of consumer concerns associated with cloud computing – Australia's positive regulatory experience in fact includes industry self-regulation. As the Task Force (2011, p. 32) put it:

> *Australia has benefited from the economic expansion facilitated by the internet, and cloud computing can further boost productivity. However, heavy-handed regulation might compromise future growth, even as it attempts to bolster its foundations. On the other hand, 'smart' regulation can facilitate, enhance and accelerate commercial opportunities, particularly if it is well informed and 'soft' in nature. There was strong support across the Task Force for the development of industry codes of conduct to cover aspects of cloud computing. Light-touch codes of conduct, rather than prescriptive legislation, are the way forward, but there needs to be some mechanism for complaint and remedial action against a breach in contractual agreements. This could be facilitated through links between an established peak body and the national legal system.*
>
> *The success of Australia's ISP code of practice on cyber security regarding the eradication of malware on infected computers is a good example of effective self-regulation initiated by the Government. It involves educating consumers and encouraging ISPs, in their own interest, to adopt a common approach and so offers a model for cloud regulation. However, such codes need to form part of a coherent framework based on principles to avoid fragmentation or a plethora of confusing schemes.*

Perhaps one of the clearest areas in which the relative immaturity of the industry is evident is in the development of contracts for cloud services. Eric Clemons, professor of operations and information management at the Wharton School of the University of Pennsylvania (who visited Australia in June), argued that the cloud computing industry would benefit from the standardisation of contracts to protect customers and suppliers – "this would provide much needed assurances about the rights of both parties if there was a services disruption, in billing disputes, when privacy was breached or when a contract ended" (Australian Financial Review, 2011).

> *One of the things that magnifies the size of the market is the safety of that market. Australia would be an ideal location for resolving contractual disputes. Most large cloud companies including Amazon.com, Google and Microsoft are based in the US and enjoy home court advantage in legal battles. A standard contract has to be drawn up in a place that is not the home of a bigger player and has the predictable tradition of British common law. There is a very small set of possible places and Australia would be my first choice. Ultimately, disabling any particular vendor's home court advantage is good for vendors everywhere (Ibid).*

This comment emphasises the importance of setting up a regulatory environment that improves Australia's export prospects. An example is the success that Delaware has achieved as a favoured location for business incorporation in the US because of its focused development of a facilitating regulatory environment.

More generally, Australia's high level of political stability makes it relatively attractive to a cloud provider because of the very large investments in capital equipment required for large-scale cloud sites. Providers want to avoid exposure to the loss or damage of such assets.

Box Six: Cloud computing in Hong Kong

IBM has also established a cloud computing lab in Hong Kong's Cyberport complex, primarily a global hub for web-based messaging services to support IBM's LotusLive cloud service portfolio. Telstra subsidiary CSL Limited has signed an agreement with HK's SIMtone to develop groundbreaking cloud computing services for delivery across CSL's Next G Wireless network. Telehouse recently chose Hong Kong as location for its first Cloud Computing Complex due to its reputation as 'network hub' of Asia. Hong Kong offers regional access across Asia, including India.

Hong Kong is a very mature and competitive telecommunications market, with high grade services, especially mobile. Hong Kong is one of the few places where the telecommunications market has been fully liberalised so that many players offer very good quality infrastructure and very competitive pricing. Hong Kong is very well served with overseas cable and satellites and has good data pipes into mainland China.

It is one of few places with both attractive electricity tariffs and high levels of stability and reliability. Two power companies taking care of each side of the harbour back each other up, cover a small geographic area and register very high uptime.

There is a high level of economic freedom in Hong Kong with virtually complete freedom of trade and no restrictions on importing technology. Highly trained personnel are available in Hong Kong, which means access to high-calibre ethical staff. Hong Kong also has a mature legal system, very good data protection and privacy laws.

In terms of shortcomings, again, land is scarce and expensive. However, many vacated industrial buildings (factories that have moved to mainland) can be rezoned and repurposed; the Hong Kong Government is getting more proactive in this regard.

A critical mass of 'cloud parks' will bring in additional operators and brand Hong Kong as a cloud computing or data centre hub. Costs of telco infrastructure and utilities can be shared if cloud activity is concentrated and centralised. This lowers setup costs and lead times, in turn encouraging utility operators to enhance infrastructure. However, cloud parks do not address the need for redundancy which is a critical requirement for the success of cloud computing.[6]

[6] A failure of power, water or transmission connectivity to a data centre can be catastrophic and some users choose to hedge against this by backing up their data in remote data centres with separate utility services. Centralisation of data in cloud parks runs counter to this measure.

5 What regulatory conditions are required for Australia to develop a world-leading cloud computing services sector?

While cloud computing offers tremendous potential for improving IT productivity, its rapid growth highlights the unresolved risks that have long existed for online privacy, data protection and authentication. Putting aside infrastructure and environmental considerations, one of the key factors in making locational decisions for cloud computing facilities is the prevailing regulatory framework in which they must operate.

As noted elsewhere, one of the most precious assets for cloud service providers is client trust and reputation. Visible compliance with governmental regulation regarding the provision of cloud services is one way in which cloud service providers can demonstrate their trustworthiness. On the other hand, governments must be cautious not to create overly burdensome regulation that would stifle the development of the cloud services sector. On an operational level, client trust depends on client data not being lost or corrupted and being protected from unauthorised access or use (whether by the cloud service provider, innocent third parties, hackers or government).

As discussed above in Section 2.2, opportunities may exist to tailor regulatory settings for foreign users of Australian cloud services in a way that encourages the export of these services that draws on the experience of countries such as Ireland and Luxembourg that have achieved success in financial services exports.

It is also arguable that, in the case of cloud computing, industry self-regulation may be a necessary part of the overall regulatory solution. A legislative approach to regulation may simply be too slow and unable continuously to adapt to the rapid technological change that characterises the industry. Another factor in favour of industry self-regulation is that each firm has a strong incentive to build and maintain its reputation and to build a regulatory structure that promotes trust and confidence in the marketplace. In fact, imposing cloud specific legislation or regulations could impede the potential of cloud computing instead of encouraging the safe and rapid growth of cloud computing. For example, a unique privacy regime for cloud computing is not required given that cloud computing merely presents a new method of storage, consumption and delivery of traditional IT services rather than a unique context or sector. Instead, the successful light touch regulation of e-commerce might provide a roadmap regarding regulation of cloud computing in the future, and smart regulation can facilitate, enhance and accelerate the commercial opportunities of cloud computing. Australia has two significant pieces of legislation that regulate issues relevant to cloud computing, albeit in a peripheral manner. These are the *Privacy Act 1988* (Cth) (Privacy Act) and the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA

Act). In the broadest terms, these acts respectively regulate the manner in which an individual's personal information may be handled by certain organisations, and the responsibilities of telecommunications carriers and carriage service providers to provide access to communications they carry to government authorities for law enforcement purposes.[7]

5.1 Privacy implications of cloud computing

As in other jurisdictions, privacy law in Australia attempts to address privacy concerns by applying principles to the collection, use and disclosure of personal information by an organisation. Australia in fact has strong regulation determining how and where private data is stored.

In an attempt to better coordinate the joint needs of privacy, and freedom of information, the Office of the Privacy Commissioner was folded into the Office of the Australian Information Commissioner (OAIC) in November 2010. This shift in focus should be welcomed but should also be backed up by a shift in policy and legislation in relation to the treatment of customer data and information. 'Information' is the currency of the network economy, and establishing an appropriately secure and flexible regulatory environment for dealing with information is a key building block to the establishment of a strong local cloud services sector.

For the purposes of this report, the relevant focus of the OAIC is the Privacy Act,[8] which regulates how an organisation collects, uses and discloses private information and how it vouchsafes its accuracy, its security and rights to access it. While the Privacy Act doesn't address cloud computing per se, it does protect 'personal information', namely anything that can be used to reasonably ascertain the identity of an individual (name, date of birth, address, phone number, email, passwords, bank account details, photos, videos). It also includes a subset of even more 'sensitive information', the collection and use of which is put to an even higher standard, including medical records, opinions or preferences (including sexuality, political views).

[7] In addition, the Australian Competition and Consumer Commission has recently issued a discussion paper for public inquiry into a final access determination for the Domestic Transmission Capacity Service in June 2011, which applies to the regulation of cloud computing.

[8] There are additional privacy laws applied at state level in respect of certain types of information (for example, health records) and organisations (such as government agencies or health service providers). While there are moves to consolidate and make privacy laws consistent across the country, these have yet to take full effect. In most circumstances, the relevant legislation applying to cloud service providers will be the Privacy Act, but there may be circumstances in which state legislation will also apply.

Naturally a client's cloud data is likely to contain personal information. That information may have been collected with the consent of the individual(s) concerned; however, they may not have consented (explicitly or implicitly) to all of the various transactions that personal information may undergo in the course of typical cloud computing service activity (such as disclosure to third party service providers or transfer across national borders). There have been a number of moves to reform the Privacy Act in order to adapt to the network economy, but these have yet to crystallise in legislative form.

The Privacy Act itself is not prescriptive about types of conduct that are prohibited; rather, it sets out 'National Privacy Principles' (NPPs) that should be applied by organisations to guide their behaviour. In addition, the Privacy Act provides for the recognition of industry codes that supersede the NPPs, though none are currently registered in the ICT sectors. Media organisations are also exempt from the NPPs if they are publicly committed to observing published standards that deal with privacy in the context of their activities as a media organisation.

Further, the Privacy Act applies to only governments and their contractors and large commercial organisations, but not small businesses (namely, those with an annual turnover $3 million or less who aren't in the business of providing health services or specifically collecting personal information about individuals). Exempt organisations may nevertheless choose to opt in to the NPPs. The small business exemption is the main difference between Australian privacy laws and the European Directive on privacy. This distinction could be removed to allow Australian privacy laws to be 'deemed equivalent' to European privacy laws for better cross border transfers of information from Europe to Australia and vice versa and it is difficult to understand why consumers storing information with small businesses should have any less protection for their personal information.

Most of the NPPs relate to the processes of collection, use, disclosure, access, correction and identification of personal information. However, the most relevant NPPs to cloud computing are NPP 4.1 (data security) and NPP 9 (trans-border data flows). In addition, a number of the NPPs have indirect consequences for cloud computing service levels.

5.1.1 Data security

NPP 4.1 requires organisations to take 'reasonable steps' to protect personal information they hold from misuse, loss and unauthorised access, modification or disclosure. Among other things, this includes network and communications security. The definition of 'reasonable steps' depends on the sensitivity of the information being held, the harm that is likely to occur if there is a breach of security, the manner of information storage and the size of the organisation itself.

When applied to cloud computing, one has to assume that a cloud service provider may not know what information is stored in a client's data, or the gravity of unauthorised access or use. Accordingly, one would again have to assume that high standards of security would prevail. At a minimum, this would include some sort of risk assessment procedure, an implemented security policy, staff training, regularly monitoring and reviewing compliance, and possibly independent third party expert audit.

5.1.2 Trans-border data flow

NPP 9 prevents the transfer of personal information (without consent) to a country in which equal or better standards for information privacy do not exist, except in certain circumstances where it is likely that the relevant individual would have implied consent. However, NPP 9 does not prevent the transfer of personal information across borders where it is being moved to another part of the same company (but not to a related entity), in which case the Privacy Act is deemed to act extraterritorially.

Without rigorous (and possibly impractical) service contract provisions, organisations that use cloud services will almost certainly be ceding control over their data to their cloud service providers. As such, to the extent their data comprises personal information of individuals collected without their consent as to any trans-border data flows, they may be liable for breaching NPP 9 if their cloud service provider transfers or hosts such data overseas. This restriction highlights the importance of having a strong cloud service sector in Australia, as organisations may simply be unable to take advantage of cloud services where NPP 9 places too great a burden on them in terms of ensuring they have the necessary consent of all individuals whose information is affected by trans-border data flows.

5.1.3 Service levels

While the remainder of the NPPs does not raise specific concerns in relation to cloud computing, they may indirectly influence the service levels that client organisations collecting personal information of others would need to have in place with their cloud service provider.

For example, NPP 6 relates to an individual's ability to access or correct personal information collected by an organisation. If that organisation stores its information in the cloud, it would need to ensure that its cloud services were sufficiently reliable in order to fulfil such requests. It may be that the cloud service provider would need to have backup capacity to meet reliability targets, which in turn would require the organisation to ensure that any client data stored on redundant capacity networks was disclosed to the client and maintained with equally rigorous security. Furthermore, organisations may need to ensure that there is some degree of compatibility or standardisation between their cloud service provider and other similar suppliers, in the event that they wish to migrate their networks or data to another supplier at a later stage.

All such transfers would naturally require the express or implied consent of the relevant individuals in order to comply with NPPs 1 (collection) and 2 (use and disclosure), which raises the related issue of organisations ensuring that their privacy and data collection policies or agreements with individuals are rigorous enough to contemplate the possible movement of personal information using a cloud service.

5.1.4 Issues with implementation of privacy law

While the Privacy Act itself provides a useful framework for guiding organisations dealing with cloud data that may contain personal information, there are a number of issues with the existing privacy regime that may need to be addressed to create an appropriate framework for building a cloud services industry.

Despite the provision for industry to create its own codes to replace the NPPs, these are not widespread and (other than the current application by the Internet Industry Association) have not been adopted in the ICT sector. A report by KPMG (2009) advised that if Australia is to have a vibrant cloud services sector, more attention should be given to, and more action must be taken in respect of effective self-regulation.

The Task Force (2011, p. 32) stated:

> *There was strong support across the Task Force for the development of industry codes of conduct to cover aspects of cloud computing. Light-touch codes of conduct, rather than prescriptive legislation, are the way forward, but there needs to be some mechanism for complaint and remedial action against a breach in contractual agreements. This could be facilitated through links between an established peak body and the national legal system.*

There are no obligations in the Privacy Act for organisations to notify OAIC or their customers in respect of a breach of the NPPs. While this has the benefit of allowing breaching organisations to preserve their reputations (for the duration that such breaches remain unnoticed), it significantly undermines trust in such suppliers. For example, the recent attack on Sony's PlayStation network was exacerbated by Sony's decision not to publicise the details of the attack until well after it had occurred. Given our identification of trust as a key factor in building successful cloud services, it may be appropriate for some sort of notification framework to exist in respect of data security breaches. A house committee has identified this lack of a notification regime as an issue that needs to be remedied in respect of privacy law, and any changes in this regard should also be considered in respect of cloud services generally.

Given the relative geographical neutrality of cloud services, it is also important to ensure international cooperation of privacy and data security, in terms of regulations, standards and enforcement. Harmonising privacy and data security frameworks, as well as cooperation on enforcement against breaches, are critical in ensuring that privacy laws (and cloud computing services) are effective.

Having said that, we understand that the Australian Government Information Management Office (AGIMO) will develop a cloud framework incorporating the principles, governance, best practice guidance including security, privacy, portability and service provider certification requirements. It will do so in collaboration with the Cyber Security Policy Coordination Committee, Protective Security Policy Committee, the Australian Information Commissioner, the OAIC and other authoritative agencies.

5.2 Telecommunications interception

The TIA Act seeks to prevent the interception of communications (live or stored) over telecommunications networks. It also provides for circumstances in which Australian authorities can request that a communications carrier or carriage service provider intercept communications transmitted using its services for the purposes of law enforcement or national security.

Transactions involved in cloud services will inevitably involve the transmission of communications over networks, thereby triggering the TIA Act. However, the exceptions to interception of communications place obligations on telecommunications carriers or carriage service providers (namely, network providers or ISPs). At this stage, there are no similar obligations on cloud service providers who are not carriers or carriage service providers, so data stored out of the jurisdiction may not necessarily be subject to interception requests (though they may be to the extent they are transmitted or stored on the networks of Australian carriers or carriage service providers). However, to the extent that such laws are applicable now or in the future, the fact that Australian authorities can request access to such communications raises confidentiality concerns in respect of client data stored by cloud service providers.

5.3 Regulatory changes conducive to establishing a thriving cloud services sector

Australia’s competitiveness in cloud services requires the establishment of a strong local cloud services industry, which can subsequently add to regional capacity. As discussed above, there are significant regulatory gaps from the cloud consumer side and some unsuitable regulatory burdens from the cloud supplier side.

5.4 Guiding principles and self-regulated industry codes

In order to ensure that users are protected and encourage the economic benefits of cloud computing, it would be best to avoid cloud-specific rules and policies in favour of policies that apply broadly to a wide range of technologies and services, and those that maintain a level playing field for cloud computing and all approaches to remote computing and data storage.

Nevertheless, the Privacy Act itself provides an interesting insight into how a potential cloud service regulatory regime might work. Its resort to principles rather than rule-based regulation puts the onus on operators to determine how best to implement client protection measures. In addition, the ability for industry codes to supersede the NPPs should provide flexibility for an emerging cloud service sector to establish its own industry standards as well as to establish a firm point of reference for their customers. For example, in the United Kingdom, the Cloud Industry Forum (CIF) issued a Code of Practice in 2010 whereby cloud service providers must demonstrate accountability, transparency and capability to end users.

5.5 Even application of regulation

By virtue of their size and the nature of their services (less than $3 million annual turnover), some cloud service providers may fall outside the application of both the Privacy Act and the TIA Act. These gaps have already been identified by both government and industry and may be closed in time. Even if a cloud service provider falls outside the application of the Privacy Act, it may be in its commercial interests to opt in as it would increase customer confidence. However, to the extent that the application of privacy or other relevant legislation favours smaller organisations, regulation and policy should be adjusted to ensure an even regulatory burden and a level playing field.

5.6 Notification procedures and service levels

Although there are moves to enhance the notification regimes under the Privacy Act, data security breaches in respect of cloud service providers may also have substantial impacts on clients and is a central concern to the provision of cloud services. A cloud service sector would be wise to take the initiative and set out its own industry standard for prompt breach notification and remedial action. Similarly, it would be prudent for the cloud service sector to establish some sort of benchmark for key service levels (such as security, reliability, redundancy, continuity of service and compatibility) in order to attract a critical mass of customers for cloud services.

5.7 International cooperation and interception

Finally, given the problems raised by the trans-border flow of data (in Australia and elsewhere), there will naturally be a bias for companies based in any given country to use cloud services provided strictly within that country. In effect, this raises new barriers to trade that have been eliminated in many other sectors. To counter these, there needs to be significant international leadership and cooperation in harmonising privacy and data security laws, as well as transparent, uniform and cautious processes for dealing with cloud data. If Australia or other countries are unwilling to give up the right to demand that telecommunications carriers or carriage service providers (and, by extension, cloud service providers) intercept certain live or stored client communications, then cloud services should not be discriminated against in this regard – namely, the processes for obtaining such data must be brought in line with existing procedures for obtaining and executing warrants in respect of data that clients may store on their own secure networks.

5.8 Conclusions: regulation and Australia as a cloud computing hub

Cloud computing would benefit from an international privacy regime that allows for data transfers across borders. Having said that, when information crosses borders, the governing legal, privacy and regulatory regimes can be ambiguous and raise a variety of concerns. Against this background, requirements on data protection and constraints on trans-border flow of data become the subject of national privacy and security laws.

Australia has strong regulations about how and where private data is stored in comparison with other jurisdictions. As such, there has been limited take-up of offshore cloud-storage opportunities among Australian companies, particularly businesses that rely on a high level of data privacy protection and security. Going forward, the Australian Government's Exposure Draft on Australia's Privacy Principles issued in June 2010 will, if enacted, introduce even more stringent regulation of cross-border disclosures of personal information.

In order to foster the growth of cloud computing to seize the economic benefits and to protect citizens against potential harm, we believe that cloud-specific (or technology specific) rules and policies should be avoided in favour of policies that apply broadly to a wide range of technologies and services. Cloud-specific legislation or regulation could instead impede the great potential of cloud computing. In addition, Australia should seek interoperable privacy regimes in which countries recognise one another's privacy rules to the greatest extent possible.

References

Australian Financial Review, 2011, 21st June.

Australian Government Information Management Office (AGIMO), 2010, "Australian Government Data Centre Strategy 2010-2025", March, http://www.finance.gov.au/e-government/infrastructure/docs/AGDC_Strategy.pdf

AGIMO, 2011, Draft Cloud Computing Strategic Direction Paper, January.

Belshe, M., 2010, "More Bandwidth Doesn't Matter (much)", https://docs.google.com/a/chromium.org/viewer?a=v&pid=sites&srcid=Y2hyb21pdW0ub3JnfGRldnxneDoxMzcyOWI1N2I4YzI3NzE2 Accessed on 3rd August 2011.

Ciena, 2011, "Low latency more than just a financial market need", 17th March, http://www.ciena.com/corporate/blog/Low-latency-more-than-just-a-financial-market-need.html

Computer World, 2011, CeBIT 2011: Whole-of-govt panels slashing ICT costs: AGIMO, 1st June, http://www.computerworld.com.au/article/388579/cebit_2011_whole-of-govt_panels_slashing_ict_costs_agimo/?fp=4&fpid=78268965

Department of Defence, 2011, Intelligence and Security, Cloud Computing Considerations, April.

Dynamic Business, 2011, "Telstra to invest $800m in cloud services", http://www.dynamicbusiness.com.au/news/telstra-to-invest-800m-in-cloud-services-1762011.html

Global Access Partners Pty Ltd, 2011, GAP Task Force on Cloud Computing, May.

Google, 2008, "About the Unity bandwidth consortium", 25th February, http://googleblog.blogspot.com/2008/02/about-unity-bandwidth-consortium.html

Hausmann, R. and Rodrik, D., 2003, "Economic Development as Self-Discovery" Revised Mimeo, April, http://www.hks.harvard.edu/fs/drodrik/Research%20papers/selfdisc.pdf

Hidalgo, C. A., Klinger, B., Barabási, A. L. and Hausmann, R., 2007, "The Product Space Conditions the Development of Nations" *Science*, 27th July, http://www.sciencemag.org

Higgins, S., Wang, D. and May, T., 2011, "Australia's Trusted Infrastructure-as-a-Service Cloud Provider Market 2011", Longhaus, February.

IBM, 2009, "Cloud computing with Linux and Apache Hadoop", http://www.ibm.com/developerworks/aix/library/au-cloud_apache/

International Business Times, 2011, “Australia Leads in Adopting Cloud Computing”, 26th May, http://au.ibtimes.com/articles/152434/20110526/cloud-computing-australia.htm

Krugman, P., *Geography and Trade*, Leuven University Press and MIT Press, 1991.

KPMG, 2009, “Cloud computing: Australian lessons and experiences”, http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/Cloud-computing-Australian-lessons-and-experiences.pdf, Accessed on 4th July 2011.

Lateral Economics, 2007, Interviews with industry, January.

Le, K., Bianchini, R., Nguyen, T.D., Zhang, J., Meng, J. and Jaluria, Y., 2010, “Reducing Electricity Cost Through Virtual Machine Placement in High Performance Computing Clouds, Technical Report DCS–TR–680”, Dept. of Computer Science, Rutgers University, November, Revised April 2011, http://www.cs.rutgers.edu/~lekien/pubs/tr680.pdf Accessed on 16th July 2011.

Longhaus, 2011, “CloudViews: Part one of an interview with Stefan Gillard from Steam Engine”, http://www.longhaus.tv/ltv-network/299-cloudviews-stefan-gillard-part-1.html, 10th May, Accessed on 28th July 2011.

Macquarie Telecom, (2011) “An overview of the risks associated with hosting data offshore”, internal briefing paper.

Marshall, A., 1890, *The Principles of Economics: an Introductory Volume*, Macmillan & Co. (eighth edition, 1947).

Microsoft, 2011, “Get Cloud Empowered. See How the Cloud Can Transform Your Business”, http://www.microsoft.com/en-AU/cloud/reports/2784.aspx

Obren, M., and Howell, B., 2010, “The Tyranny of Distance Prevails: HTTP protocol latency and returns to fast fibre internet access network deployment in remote economies”, 21st November, http://www.iscr.co.nz/f609,17429/17429_The_Tyrant_Lives_v3_Nov21.pdf Accessed on 3rd August 2011.

O’Connor, B., MP, Minister for Home Affairs and Justice, Minister for Privacy FOI, 2011, April.

The Australian IT, 2011, 28th June.