GAP Task Force on CLOUD COMPUTING Final Report

May 2011, Australia

This report details the discussions of the GAP Task Force on Cloud Computing - a cross-disciplinary group established in 2010 by public policy network Global Access Partners (GAP) in collaboration with the Australian Government's Department of Broadband, Communications and the Digital Economy

GAP Task Force on Cloud Computing

FINAL REPORT

May 2011

GAP - Global Access Partners Pty Ltd

ACN 000 731 420
ABN 74 000 731 420

53 Balfour St, Chippendale

Sydney NSW 2008
AUSTRALIA

T +61 2 8303 2420
F +61 2 9319 5754
www.globalaccesspartners.org

DISCLAIMER: This report represents a range of views and interests of the individuals and organisations participating in the Task Force. They are personal opinions that do not necessarily reflect those of the organisers and sponsors of the Task Force. Given the different perspectives of Task Force participants, the report does not reflect all the views of all members and it should not be assumed that every participant would agree with every recommendation in full.

COVER: The image is courtesy of Erika Szostak (UK), *PhotoMaldy®/Creative Commons via flickr*

TABLE OF CONTENTS

PREAMBLE

Task Force on Cloud Computing

This report details the discussions of the **GAP Task Force on Cloud Computing -** a cross-disciplinary group established in 2010 by public policy network Global Access Partners (GAP) in collaboration with the Australian Government's Department of Broadband, Communications and the Digital Economy (DBCDE).

The group was conceived following the Technology Foresight Forum *"Cloud Computing: The Next Computing Paradigm?"* held by the Organisation for Economic Co-operation and Development (OECD) in October 2009. This workshop discussed the growing usage of Cloud computing and the implications for consumers and small businesses. This workshop also canvassed thoughts on possible government regulatory approaches.

The primary purpose of the GAP Task Force was to enable the Australian Government to become better informed about Cloud computing.

The key objectives of the GAP Task Force were to address the potential impact of Cloud computing on the Australian economy, identify any issues of concern, consider policy measures adopted by other countries, and work with the Australian Government to develop appropriate policy frameworks for vendors, businesses and consumers. Its members included senior executives and thought leaders from the public, private and research sectors who were invited to offer a cross-section of views and perspectives, as well as a breadth of experience and knowledge. The Task Force was chaired by Mr Keith Besgrove, First Assistant Secretary, Digital Economy Services Division, DBCDE. A full list of the participants in the Task Force is at Attachment 8.

Members met on four occasions, under the Chatham House rule of non-attribution, from August 2010 to February 2011. Proceedings emphasised openness and consensus building, however, the final report does not purport to reflect all the views of all its members. It should not be assumed that every participant would agree with every statement or recommendation.

The Task Force considers that there would be value in further research into the issues raised in this report. It also believes that it is time for some further discussions between industry, government and civil society and proposes further, on-going dialogue of the issues raised in the report. With this in mind, some members of the Task Force will be proceeding with the organisation of a larger-scale, policy-focused discussion in 2011, involving a broader group of contributors from Australian Government departments and industry bodies such as the Australian Competition and Consumer Commission (ACCC) and the Australian Communications and Media Authority (ACMA). Some members of the Task Force also considered assuming a role in the discussion of global industry standards, as well as the establishment of an ongoing online platform to facilitate future collaboration.

Regulation in Technology-Rich Environments

The pace of development and deployment of Cloud computing[1] is such that over half of the world's IT activity may occur "in the Cloud" within the next decade. There are many commercial and strategic reasons for Australia to encourage greater access to Cloud services in a drive to develop a competitive digital economy.

The adoption of Cloud computing will be driven by its promise of radically improved choices, attractive cost savings, seemingly limitless flexibility, fresh potential for collaboration, multi-layered resilience and instant scalability. Like the Internet itself, Cloud computing may affect almost every field of human endeavour, from boosting the computing power available to individuals and small businesses through monitoring complex ecosystems and urban traffic flows to streamlining many forms of government services. The Task Force believes that when Cloud computing is coupled with high speed broadband -- for example, via the National Broadband Network -- then major opportunities will be created to assist in transforming the efficiency and competitiveness of the Australian economy and to enhance the quality of life of ordinary Australians. Cloud computing can generate a range of major new business opportunities for Australia, but only if the regulatory environment succeeds in protecting consumers from abuse, while not constraining the introduction of innovative service solutions.

Cloud computing constitutes a shift in the way computing resources are sourced and delivered. Its rapid growth offers significant benefits, but also challenges existing business and regulatory models. Cloud computing demands flexibility, adaptability and innovation in any public policy response.

So What Is Cloud Computing?

According to the widely-used US Government's National Institute of Standards and Technology (NIST) definition (*http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf*), Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. More details about this range of characteristics and models can be found in Attachment 1 of this report.

[1] Any reference to Cloud computing in this report focuses primarily on the public Cloud environment unless otherwise indicated.

While there are other definitions of Cloud computing, the GAP Task Force thinks of Cloud computing as essentially computing as a utility. In this respect, Cloud computing may be defined more simply as the use of third-party software applications and storage provision accessed by users over the internet.

A useful working definition for the layman is the Gartner definition which uses five criteria to define Cloud computing:

1. **Scalable and elastic**: Services that scale on demand
2. **Service-based**: Well defined service interface
3. **Shared**: Services share a pool of resources to build economies of scale
4. **Metered by use**: Services are tracked with usage metrics to enable multiple payment models
5. **Uses internet technologies**: Service is delivered using internet protocols, such as HTTP, IP via web-oriented architecture

All five criteria have to be present to represent Cloud computing.

Such services have rapidly expanded during the past two years and can significantly reduce transaction processing and technology management costs. Cloud computing revolutionises the online interactions of Australia's citizens, businesses and government but, as with any new technology, there are also potential downsides and risks, particularly in regard to data ownership and security.

Why Is Cloud Computing Important?

The Task Force believes that Cloud computing is important because it has the clear ability to significantly reduce the cost of establishing and operating computer and communications systems. It reduces the time to establish computer support systems for activities as diverse as a research project, a technology start-up company, or a new government service from months to days or even just a few hours. However, the real power of Cloud computing arises from developing new systems, rather than simply shifting legacy systems to the Cloud without doing any further work.

Because of the speed of establishment, and the ease with which Cloud services can be scaled up or down on-demand, Cloud computing is changing how people use computing and communications services. Cloud computing will make many aspects of communications better, faster and much cheaper than today. The Task Force considers that the cost advantages available under Cloud computing are so large that Cloud is probably unstoppable. The Task Force also believes that the combination of Cloud computing with the high speed connectivity that will become available under the National Broadband Network represents a combined force for transformational change of the Australian economy and society.

In some respects, the issues thrown up by the emergence of Cloud computing are essentially similar to those thrown up by the earlier growth in the internet. However, the combination of Cloud services and high speed broadband will invariably increase the scale, speed and complexity of both the opportunities and challenges which Australia must confront in moving towards a fully-fledged digital economy. The fact that much ICT is now globally interconnected with data sent and received across many different, and often unknown, jurisdictions means that existing regulatory processes can frequently be - or be perceived to be - inadequate.

It is important to understand that, while Cloud computing draws upon technologies which have been available for some time (e.g. virtualisation), it is the combination of elements of the services and the manner of their presentation, availability and scalability which is new. This is presenting significant interoperability challenges and the standards environment for Cloud computing will clearly take some time to stabilise. While a number of voluntary bodies have emerged to manage issues regarding the internet, such as the *Internet Engineering Task Force* (IETF), the *World Wide Web Consortium* (W3C) and the *Internet Corporation for Assigned Names and Numbers* (ICANN), they remain mechanisms for the self-regulation of standards and conventions. There is also some progress towards agreement on interface standards to allow different devices to communicate more seamlessly, including areas such as radio spectrum usage, device and peripheral interface standards, security standards and message structures, and so forth. The Task Force 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. Indeed, it may be unrealistic to expect agreement to emerge, since no international regulatory bodies oversee these areas and the issues involved are often highly specific to individual jurisdictions.

Cloud computing brings these challenges to a head: offering tremendous potential for improving the accessibility and depth of online experience while highlighting the unresolved risks that have long existed for online privacy, data protection and authentication.

If Australia is to capitalise on its opportunities in the new globalised digital economy, the regulatory debate must transcend the known issues of reassurance and risk. Regulation in technology-rich environments must also address the perspective of 'competitive advantage'. Australian regulators should identify and focus on areas offering the potential to generate global opportunities.

What Are The Opportunities that Cloud Computing Offers?

The Australian and various state governments are embracing Cloud computing and grow ever more cognisant of the issues and sensitivities involved in their utilisation. The Australian Government recently released its Cloud Computing Strategic Direction Paper (*http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html*), which outlines the steps for the Australian Government over the next few years. Additionally, many state bodies are developing appropriate protocols to deal with the different levels of risks associated with various manifestations of the Cloud.

Overseas, public and private sector groups are moving rapidly to embrace the use of Cloud computing. The US government has issued a series of statements defining Cloud computing through the NIST with this definition being widely accepted, not least by the vendor industry itself. There is a growing body of international work on privacy protection and regulation, including that generated by the OECD, Asia-Pacific Economic Cooperation forum (APEC) and other bodies, with applications to the Cloud. In addition, the Obama Administration has recently announced a US Government Strategy for the use of Cloud computing: the Cloud First Strategy.

Internet users in Australia have already adopted Cloud computing solutions in large numbers, although comparatively few will be aware of the fact. Web search, online mapping and social networking are highly popular Cloud solutions. However, a lack of operational standards and compatibility between different suppliers of the Cloud may hamper its progress if not properly addressed. Implementation errors and a lack of investment in “trust” and standards proved damaging during the much heralded e-commerce revolution of the 1990s, and similar mistakes may be repeated today. Large Cloud service providers are assuming ownership of their users' information in ways that may cause problems while governments keen to employ Cloud-based citizen interaction solutions may inadvertently widen the existing 'digital divide' by obliging citizens to use online access methods which they may not be in a position to afford.

There are a range of Cloud deployments being promoted by vendors, ranging from the internal or external aggregation of data to the use of complex brokerage systems. Server farms (servers located in disparate sites) can generate significant economies of scale for large corporate clients and create the infrastructure required to offer true Cloud computing to private consumers and small businesses. The operation of distributed server farms may generate privacy and security issues as data is transferred across national borders and a host of varying jurisdictions, but also allow business risk to be balanced across the globe.

Cloud service aggregators will become increasingly common in the market, but these companies may merely juggle existing capacity, rather than investing in the real infrastructure required to handle increasing loads, while service level agreements may involve complex re-selling arrangements involving ISPs or power companies and their failure could imperil information security.

Benefits and Challenges of Cloud Computing

Benefits

Depending upon the implementation, Cloud computing promises compelling efficiency, cost and scaling advantages delivering:

- *Lower upfront costs:* When introducing a new application, the cost of hardware and of software licenses are currently a major concern, but Cloud services allow the subscriber to pay the provider for usage alone, avoiding the need for up-front expenditure and allowing costs to be spread over time and managed more closely.
- *Reduced financial risk:* If a Cloud-based application proves unsuccessful for whatever reason, or its use within the business is for a limited time, it can be discontinued without the retention of useless infrastructure. The user also avoids the financial risk of technological obsolescence.
- *Faster time to market (agility):* It typically takes several months to achieve successful implementation of a traditional application, but Cloud applications can be deployed and scaled within days or hours.
- *No capital expense:* Cloud computing allows the user to pay for ICT as a service when consumed, turning capital expenses into operating (variable) costs.
- *Lower operational expense*: Given economies of scale, high levels of automation and self-service, Cloud providers can usually offer ICT services at a significantly lower cost than individual organisations can deliver themselves.
- *Clear ICT value for businesses*: ICT has always struggled to demonstrate its value to businesses, and there has been a seemingly constant disconnect between ICT spending and the perception of value it delivers. Cloud computing provides a direct connection between ICT spending and value – similar to domestic spending on phone bills or electricity.
- *Innovation*: Cloud computing can offer an almost infinite "ICT sandpit" for experimentation and innovation at low risk, low operating cost and with no capital expenditure. Experiments in the Cloud can be rapidly scaled up or abandoned depending on how they turn out.
- *Access to expanded expertise*: Given their economies of scale, Cloud providers can afford to offer more specialised services and deeper expertise in advanced security techniques, application performance optimization, tailored user support and business continuity services than many in house ICT departments.
- *Sustainability*: Most providers of Cloud services are facing pressure from consumers and governments to utilise facilities that consume less energy. There is a growing trend towards locating large data centres in locations where renewable energy is available.

- *Continuous enhancements:* Instead of facing occasional, disruptive and costly upgrades of ICT, the Cloud can deliver incremental improvements and enhancements on a continuous basis.
- *Decreased downtime and delays (improved resilience):* Since Cloud workloads can be spread across many facilities, and even across different Clouds, redundant applications can be used to avoid downtime. In addition, data distribution strategies can help address disaster recovery and business continuity issues. Larger Cloud providers can also afford to build 'hardened' facilities with reserve power supplies and cooling equipment.
- *Standardisation:* Over time, the use of Cloud services is likely to drive standardisation among users which in turn facilitates the simplification and alignment of business processes, yielding further savings and enabling the scaling of processes within an enterprise.

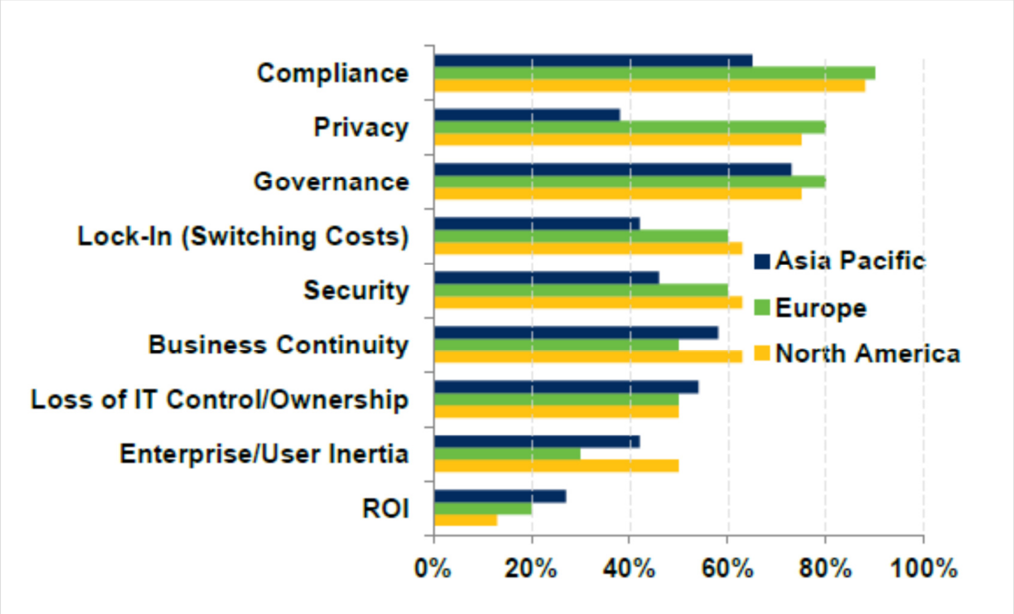
Challenges

- Lack of customisation
- Integration with existing systems
- Business continuity
- Data portability and interoperability issues
- Data sovereignty
- Legal and privacy issues from a cross-jurisdictional perspective
- Performance and conformance
- Changing skills requirements
- Government and business reputation
- Cyber security

What Is It About Cloud Computing that Worries People?

As with any evolution in technology and service, Cloud computing brings with it new challenges, both real and imagined. Cloud computing depends on fast, low-delay, highly reliable networks which may not always be available and, though the Cloud computing can be seen as a further evolution of outsourcing, some companies and industry sectors are uncomfortable with any increased reliance on outside providers or off-premise data storage.

Figure 1. Public Cloud Concerns in the Public Sector
(Source – World Economic Forum 2009 Cloud Computing Survey)



Further challenges include assessing the role, importance and impact of government involvement, education, portability, open source solutions, privacy, consumer protection, reliability and identity theft, security, consumer sovereignty and awareness and lawful interceptions. Such concerns can involve a disparate range of bodies, including law enforcement organisations and industry regulators.

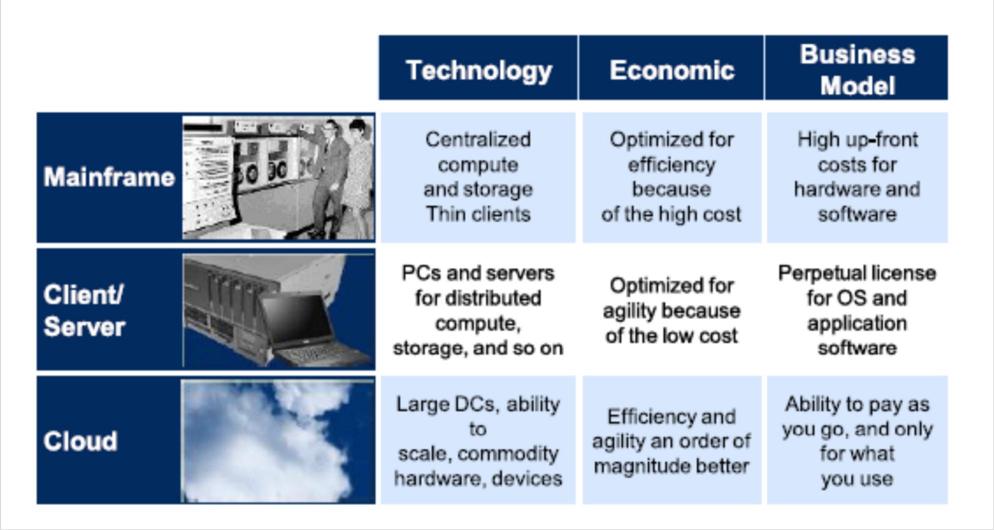
As previously alluded to, there is a lack of clarity regarding "the rules of engagement" on the internet in general and in Cloud computing in particular. Although a *Cloud Trust Protocol* is being developed among businesses, involving 24 different recommendations or stipulations, such agreements may have limited application to individual consumer choices.

Economic Drivers of Cloud Computing: an Industry Perspective

Cloud computing represents a major departure from previous industry practice and may fundamentally change the nature of computing. While mainframes required expensive upfront capital investments and later client servers optimised agility for end users, the Cloud offers the advantages of both approaches without the disadvantages of either and can improve efficiency by a factor of ten.

A recent Microsoft report *"The Economics of the Cloud for the Public Sector",* released in November 2010, examines the possible economic drivers for the adoption of Cloud computing, with a specific focus on 'private' Clouds.

Figure 2. Cloud Opportunity (Source – Microsoft)



	Technology	Economic	Business Model
Mainframe	Centralized compute and storage Thin clients	Optimized for efficiency because of the high cost	High up-front costs for hardware and software
Client/ Server	PCs and servers for distributed compute, storage, and so on	Optimized for agility because of the low cost	Perpetual license for OS and application software
Cloud	Large DCs, ability to scale, commodity hardware, devices	Efficiency and agility an order of magnitude better	Ability to pay as you go, and only for what you use

Cloud computing requires large, expensive data centres, but these can offer economies of scale, for example, in the area of power consumption. While separate applications are commonly run on separate servers today, Cloud computing allows usage to be aggregated through handling the peaks and troughs of demand across different time zones. Businesses are often uncertain of the extent and type of their future computing needs and Cloud computing may offer the cost effective flexibility they require.

Recent separate analyses by Microsoft and National ICT Australia (NICTA) have reached similar conclusions that the potential cost savings of using public Clouds could be around ten times greater than the savings which could be achieved by the use of private Clouds.

Microsoft sees the cost savings offered by Cloud computing as certain to change computing practices in the near future. Cloud computing will allow large Central Processing Units (CPUs) to be rented for large but occasional tasks, and so more computing will be done in real time in the Cloud, rather than over a long time by in-house computers of much lesser capability. Computing will continue to grow as a percentage of GDP as the integration of digital technologies into people's lives continues. Cloud computing will also facilitate the future use of artificial intelligence with simple user interfaces.

IMPLICATIONS OF THE CLOUD FOR DIVERSE USER GROUPS

Government

The Task Force considers that Cloud computing brings substantial benefits for government that no other IT model can provide in terms of simplicity, cost, security, flexibility and pace of innovation. Adoption of Cloud services by government will increasingly see applications delivered over the Internet and accessed in a web browser. The applications and the data are stored centrally and are designed to be served from highly scalable, secure and reliable multi-tenant infrastructures. Devices like notebooks, tablets and smartphones are portals to the data that help people be productive from anywhere, at any time. Upgrades are not necessary to get access to the latest innovation - a simple browser refresh will suffice. Business and governments would no longer own or manage servers and client software; rather, they will purchase integrated applications and development platforms from others, and can devote their time to improving internal processes and service delivery.

Cloud computing is already delivering benefits for government agencies here and around the world. The Task Force believes there are tremendous opportunities for "quick wins" in the short/medium term across the levels of Australian government and huge potential for an evolution to Cloud computing by government. Private sector members of the Task Force expressed a strong willingness to partner with governments in this process.

Australian government agencies are moving rapidly to embrace Cloud computing. At a national level, agencies as diverse as the Department of Immigration and Citizenship (DIAC), the Australian Taxation Office (ATO) and DBCDE are all moving into the Cloud environment. At the state level, take up of Cloud computing is also underway. Queensland, for example, is looking at a significant, state-wide use of Cloud computing to streamline government services and achieve substantial savings. At a local government level, take-up has commenced in some councils, but is generally less advanced. However, the Task Force considers that the use of Cloud computing, combined with high speed connectivity, offers major opportunities to dramatically improve the speed, quality and availability of services across all levels of government, but particularly for local governments based in regional and remote areas. The Cloud has great potential to improve efficiency in local government as it will allow sophisticated solutions to be used by small and cash-poor local government organisations.

Cloud computing can allow government to source computing services in a more efficient and cost effective manner. Cloud computing can offer government agencies the ability, for instance, to deal with unexpected bursts of enormous demand experienced shortly before lodging deadlines or in times of civil emergencies. Existing systems have not been built with the redundancy required to handle such rare, but massive peaks in usage and Cloud computing offers an obvious solution.

However, when considering Cloud computing, agencies must address a host of issues beyond those of service cost and flexibility. These include risk and privacy, performance and security, and the inherent latency caused by the routine channelling of Australian internet traffic through servers on the other side of the planet. Interoperability, reliability, standards, 'locked in' contracts, service standards and performance, exit strategies and legislative and regulatory constraints must also be considered.

The Australian Government's security requirements for the Cloud outlined in the Department of Defence's Cyber Security Operations Centre paper on Cloud Computing Security Consideration (April 2011) recommends against sourcing ICT services and functions outside Australia. There is also a danger that if, for example, data is hosted on a server in the United States (US), the US Government would have the right to access it under the terms of its Patriot Act, although there is a protocol that the US Government would consult with other governments before any such action was taken in regard to public information.

Most government departments have clearly defined capital and expense budgets, and Cloud computing will tend to blur the boundaries between them because these solutions normally involve little or no capital expenditure. Cloud computing could deliver some services at a fraction of the current cost, while in other areas the savings would be less dramatic, but in all cases the information service accounting procedures of departments would have to change. Furthermore, Cloud vendors presently tend not to be compliant with accessibility standards mandated by government regulations.

Sir Peter Gershon's *Review of the Australian Government's Use of Information and Communication Technology* (2008) made a number of recommendations (which were accepted by the Government) concerning the Government's use of Information and Communication Technology (ICT). Those recommendations included developing a whole-of-government strategic plan for data centres, tightening the management of ICT spending, including exploring options for shared services, and developing a whole-of-Government ICT sustainability plan. In the report, a number of agencies indicated that they are already using virtualisation technologies with others citing plans to adopt these technologies. By extension, the adoption of Cloud-based services by the Australian Government may offer opportunities in its consideration of: whole-of-government data centre needs; improving standardisation across agencies; reducing ICT spend; maximising resources and improving sustainability.

The need to fully address issues such as privacy, security and the entry of citizen data into the 'public Cloud' means that widespread adoption of public Clouds by government agencies may take from six to ten years. However, opportunities to use private Cloud or 'data centres using advanced virtualisation' techniques to store citizen data behind government firewalls will arise in the short term.

Major opportunities present themselves in terms of data already in the public domain, be it in regard to 'citizen-facing' services or public information. The use of the Cloud for such information would aid the opening up of government data recommended by the Gov 2.0 Task Force report. Public data need not to be hosted on government servers, and many departmental websites could also be hosted in the Cloud. This is already happening with the Australian Government's Cloud Computing Strategic Direction paper encourages the transition of public-facing websites to the Cloud environment. Sites such as *www.data.gov.au* are already being hosted in the Cloud.

Coincidentally, the more widespread availability of government data in the Cloud could also spawn the creation of new businesses based upon the manipulation and presentation of such data.

In April 2011, the Department of Finance and Deregulation (Finance) released the *Australian Government Cloud Computing Strategic Direction Paper*. In the short term, the paper encourages agencies to adopt public Cloud services for public facing, unclassified services. In the medium to long term, the paper proposes a whole-of-government approach integrated with the data-centre strategy. Finance, through the Australian Government Information Management Office (AGIMO), has also established a Cloud Information Community comprising both agency and cross-jurisdictional representatives and a reciprocal arrangement with the Australian Information Industry Association's (AIIA) Cloud Taskforce. The Defence Signals Directorate (DSD) has released an interim Cloud computing security considerations paper to assist agencies when undertaking a threat and risk assessment to assist in making an informed decision as to whether Cloud computing is meets their business requirements with an acceptable level of risk.

A commitment by the Government to use open systems (based on open standards) would be useful in encouraging the Cloud market to develop in Australia. In January 2011, the Australian Government updated the Open Source Software Policy which requires agencies to consider open source software in all ICT software procurements.

The Taskforce is aware that a single agency has been appointed to coordinate software licences from Microsoft to deliver significant cost and contractual savings, for instance, and such arrangements may point the way forward to dealing with similar software licensing issues with the Cloud.

Governments should address the potentially anti-competitive elements of digital rights management as well as issues of software interoperability. Major suppliers such as Microsoft are already moving towards interoperable open standards and a set of voluntary principles could be adopted by major players to ensure that evolving Cloud computing solutions employ open systems to reduce unnecessary technological inconvenience and transaction friction for consumers.

Cloud computing poses few issues which have not already been successfully tackled in other areas. Data has been routinely hosted on outside services for years in other guises and a range of terms and conditions can be offered to customers, from large corporations to individuals, to suit different security needs and preferences. Whole-of-government solutions may overlook the fact that different agencies require different terms and conditions to suit their individual circumstances. Cloud computing can actually overcome the problems found with traditional outsourcing through offering more flexible arrangements.

The private sector members of the Task Force believe that there is clearly an opportunity for government agencies to be utilising many of the technologies to gain large benefits. Government agencies should actively consider adoption in the short term and should review risks and benefits on a case-by-case basis. The trialling and early adoption of Cloud computing models in appropriate circumstances will have the wider benefit of building up of the government's knowledge base regarding the technical deployment and management issue associated the adoption of Cloud computing solutions

The Australian Government has recognised the benefits of a strong and vibrant digital economy in Australia. Its investment in the National Broadband Network is a key part of this commitment. A primary goal of the NBN is to use this investment in nation-building infrastructure to pay a dividend to the Australian people through enhanced productivity and innovation in the long-term. Ubiquitous availability of high speed broadband should spur the adoption of Cloud-based computing solutions by business and government alike.

Larger Businesses

Major companies are increasingly seeking Cloud computing and exploring the development of private Clouds. While obviously mindful of potential pitfalls, anecdotal evidence suggests that many would embrace Cloud computing solutions for data storage and retrieval they could trust.

It is fair to say that the Task Force discussed a wide range of large business responses to the emergence of Cloud computing. The rapid development of a wide range of Cloud service providers within Australia certainly implies an escalating demand from both public and private sector users. While some large businesses are moving quickly into the use of Cloud computing, others -- including some of the banks -- are proceeding cautiously at this stage. This is partly a response to the unsettled nature of the market for Cloud computing (including the absence of widely adopted standards), combined with concerns about the potential reputational risks which could arise if something goes wrong with client data in the Cloud. Indeed, several of the major banks have recently been calling for more work on the establishment of Cloud computing standards to ensure that they are able to retain control of any outsourced IT. This is particularly related to the question of vendor lock-in.

Banks operate in a complex regulatory framework regarding their handling of customer data, with the various privacy acts being a major consideration. However, such legislation does not pose the primary barrier - the wider question of customer trust remains the stumbling block. Customers have to trust their financial institution, which in turn should not expose their customers to unnecessary risk. The scope of bank services is far wider than merely financial transactions however, and customer relationship management is an area thought amenable to Cloud computing. It was noted that the Australian Prudential Regulation Authority (APRA) has been counselling caution in the adoption of Cloud computing.

Legal advice offered to one major banking concern regarding the possible use of Cloud computing focused on privacy considerations and the US Government's Patriot Act, and allowed for a range of options including asking customers to opt-in to the scheme. The failure of any Cloud-based arrangements could risk the reputation of the company and questions of confidentiality, reliability and security remain. Domestically-based Clouds are considered more secure than international Clouds, but service providers must build trust with their banking clients, just as banks must earn the trust of their customers regarding the handling of their financial assets.

Unfortunately, contracts with Cloud providers have proved difficult to negotiate with insufficient protections for privacy, data backups and data segregation offered by vendors. The business model of Cloud service providers tends not to intersect with the more conservative framework that banks must adhere to. Vendors tend to offer a promise of 'best endeavours' to maintain services, rather than actually guaranteeing the continuity and security of provision demanded of them. Pitfalls experienced with other much-hyped revolutions in computing and the internet have underlined this tendency towards caution. The use of IT outsourcing raised similar considerations, for instance, and many problems were encountered with its deployment. The co-location of data in Cloud computing solutions also poses new challenges and creates the perception of new risk asymmetries.

The Research Community – Federated Access Management

The research community in Australia appears to be well aware of the significant advantages which Cloud computing can offer, particularly in terms of enabling the rapid scale-up of small, purpose-built research teams which may often exist for only short periods while a single research task is conducted. The recent release of *"Cloud Computing: Opportunities and challenges for Australia"* by the Australian Academy of Technological Sciences and Engineering (ATSE) demonstrates a growing realisation of the value of Cloud-based solutions for the public and private research communities, both in Australia and overseas. Once again, security remains one of the greatest barriers against its widespread adoption with academic institutions wary of the liabilities which participation in the Cloud might incur.

The Australian Access Federation (AAF) offers the research community a system through which security, at least in terms of identifying those attempting to access information, can be better assured. It allows participating institutions and service providers to trust the identity information they receive from other member bodies, so allowing students, scientists and academics seamless access to resources and collaborative communication avenues. The system uses federated access management to give authorised people a single "sign in" to access data and share computing capacity and scientific instruments from a range of Clouds for short term projects, so encouraging collaboration and data dissemination. Users' credentials are managed at the home institution, which then passes information to other institutions as required. The AAF uses a combination of Shibboleth and Public Key Infrastructure (PKI) to allow fine grained control while enabling short term relationships with a minimum of bureaucracy and delay.

The AAF relies on an agreed set of rules among the universities involved, including the terms of the Privacy Act. There are four levels of identity assurance ranging from self-presented credentials through to fully vetted security credentials. Each organisation can determine the number of attributes it collects from users, who can in turn choose whether to release their information or not. Trust federations can have applications in "darknet" networks. This approach will allow researchers from around the world to use data from the square kilometre array, for example, in conjunction with worldwide federated trust organisations.

The AAF Project is sponsored by the Australian Government's Department of Innovation, Industry, Science and Research, through the National Collaborative Research Infrastructure Strategy Platforms for Collaboration (e-Research) capability.

The AAF model is based on the existing EU data access in a federated system.

Small Business

Small business will embrace Cloud computing to reap the cost savings promised by vendors, but in many instances may be ill prepared to do so in an informed and considered fashion. Government could therefore play a useful role in raising awareness and educating the small business community about the possibilities of Cloud computing, as well as its possible risks.

The potential of Cloud computing to solve a firm's specific problems could be demonstrated through the generation of practical scenarios which could also examine issues which might arise regarding privacy and security. Public seminars, workshops and 'concept exercises' might also prove useful in helping small and medium enterprises understand Cloud technology.

Cloud computing can offer a much wider set of solutions than simply aggregated data services. It facilitates new ways of collaborating and working and can drive increases in productivity as well as saving costs. It allows information and communications capacity to be bought as needed, offering flexibility and innovation to businesses which wish to free themselves of expensive and cumbersome in-house IT solutions. Cloud developments could also encourage employment by reducing IT start-up costs for small businesses. Secondary brokerage is a growing market, with infrastructure aggregators becoming a major factor in the market. Cloud computing allows identities to be obscured online to an even greater degree than before, with small organisations able to appear much larger than they are, and vice versa. This has obvious risks as well as potential for small players to penetrate larger markets.

NICTA has developed advanced tools and techniques for evaluating Cloud computing platforms (*www.soasymposium.com/pdf_berlin/Anna_Liu_10_Things.pdf*) and is leading research projects with engineering architects and project management professionals in examining the Cloud from an enterprise perspective. Its research shows that many of the opportunities, challenges and risks of the Cloud can be addressed through the development and use of improved technology. The latency period for Australian data to travel to data centres on the West Coast of America, for example, is a fraction of that to data centres in Singapore and so a blanket assumption of Australia's place in the Asian internet sphere may be misplaced. There are a range of new businesses involved in this area, particularly second-tier system integrators offering backup services to the major providers, such as Amazon and Google, but the market is still at an early stage of development. Issues range from managing the large sums processed by online gambling companies to denial of service attacks run by organised crime syndicates in Russia. Other problems include the auditing of Cloud services and the liability of sales taxes across state boundaries.

Service-oriented computing may prove to be the future of business computing and Australia could have an advantage in developing the sophisticated and flexible work flow services it requires, rather than hosting physical data centres.

Consumers

Australian consumers have already embraced a host of Cloud-based data storage solutions, from web-based mail to video and photograph storage, with great enthusiasm and seemingly little concern for data privacy issues. There are surprisingly low expectations of online rights and remedies, for example, if information should be lost. Email itself was an early Cloud solution, with many customers unconcerned where their messages were held or which jurisdictions they crossed. Many customers automatically trusted the providers not to leak or lose their information. However, as Cloud computing grows in scope and influence, so does the potential for criminal exploitation.

Many people feel that future Cloud vendors may engage in fierce competition, backed by minimal capital investment, and providers may seek to reduce costs at the possible expense of security. In practice, it seems that most Cloud providers take security very seriously, and offer high levels of data security as a matter of course. A more critical issue for consumers is the question of what happens to private information if the consumer seeks to change Cloud provider, if that provider goes out of business or if the Cloud provider wishes to exploit the data for its own (sometimes poorly disclosed) purposes. There is enough anecdotal evidence already available to suggest that this is an issue of real concern. Given the number of potential business failures in such a new and dynamic market, there is the need to ensure the ability of users to transfer information from one Cloud solution to another. Examples of current problems include the difficulty of transferring address book data from Blackberry to Apple platforms and network locks on mobile phones.

The spread of Cloud-based solutions does not necessarily pose new challenges for consumers, but it does have the clear potential to amplify problems arising from the provision of services by overseas suppliers who may have little or no physical presence in Australia. Any reluctance by consumers to employ wider Cloud computing solutions may be driven in part by uncertainty as to where important or sensitive information would be held and by uncertainty over secondary use of personal information (although only partially a 'Cloud' issue, the recent debate over re-use of geolocation data is an example of the concerns that are arising from this uncertainty). People tend to care greatly when their privacy is actually and demonstrably invaded, even if they had not manifested any concern prior to the event.

A key issue which arises when considering the potential vulnerability of users of Cloud computing is the nature of the contractual terms and conditions which apply. Two recent University of London studies of Cloud contractual terms and conditions have revealed a wide range of approaches. Cloud suppliers routinely seek to specify that their contracts are governed by the laws of a particular country (usually the supplier's home jurisdiction) or, in the case of many US suppliers, a particular state in the USA.

Contractual terms often seek to gain the agreement of consumers to waive some or all of their rights. In many jurisdictions (e.g. the UK, EU and Australia), such contractual waivers are likely to be unenforceable and consumers seem likely to enjoy the same theoretical protections as in a non-Cloud environment. As is often the case in matters related to the internet, the challenge for regulators is enforcement of multi-jurisdictional cases. In this respect, Cloud computing has not produced a new issue, but is certainly adding impetus to an existing problem.

The successful light-touch regulation of e-commerce through the 1990s, both domestically and internationally, might provide a roadmap regarding discussions of Cloud computing in the future. Many of these transactions came with no price to the consumer and so old notions of contractual obligations and informed consent struggled to apply. Agreements of principles and verification systems have encouraged trust in e-commerce to develop over time, and similar principles should exist to encourage the use and development of Cloud computing.

Privacy principles are commonly adopted around the world, as are e-commerce standards, despite a lack of legal backing. A similar combination of standards, principles and protocols could be adopted to drive Cloud computing in the future. Progress is already being made on this front. A draft discussion paper of possible principles was presented to ISO council members in November 2010 and, if accepted, this will be passed on to relevant regulatory and consumer groups for incorporation into local agreements.

As has been noted elsewhere in this report, the standards base for Cloud computing is not yet stable. However, there is considerable activity under way around making standards.

POTENTIAL AREAS OF ACTION

The following key areas were identified by the GAP Task Force as crucial for the development of Cloud computing in Australia.

Critical Infrastructure

The Cloud is likely to quickly become part of Australia’s critical national infrastructure. However, its widespread utilisation raises questions about economic sovereignty. In addition, the practical risks of relying on foreign servers and the undersea cables which link Australia's internet to the rest of the world are likely to absorb increasing attention by government. If the Government becomes reliant on Cloud services, the question of how it would continue to operate if access to those services were subject to geopolitical pressures or lost to natural calamity becomes an important strategic consideration.

Australia as a Cloud Host for the Region

There were strongly differing opinions within the Task Force as to whether Australia could realistically expect to adopt a major role in the hosting of Cloud computer solutions for this region. Some asserted that it would require an increase in national capacity by a factor of 'a thousand', particularly given the limits of the undersea cable connections to the rest of the world. Others pointed to the rapid emergence of a host of nationally and regionally focussed Cloud services which are emerging in Australia right now. But the larger companies considered that Australia may be too remote from major markets in America, Europe and Asia. In addition, concern was expressed that Australia has neither the natural or contrived advantages of things such as cheap green energy (and low ambient temperatures) offered by countries such as Iceland and the large government subsidies of Singapore.

A major data centre costs between 200 and 500 million dollars to construct. It was suggested that Australian capacity is poorly placed to provide capability for Asian markets due to the inherent latency caused by its geographical distance from them. Latency periods of 150 milliseconds have been acceptable in the past, but improved technology is reducing such delays to 50 and 25 milliseconds, currently leaving Australian-based services out of the calculations of South East Asian customers. However, recent significant investments in Australian data centres by Fujitsu and Macquarie Telecom, amongst others, suggest that the jury is still out on this question.

A recent report suggested that a growing number of Australian Software-as-a-Service (SaaS) providers are now moving their applications to the US, according to figures from US-based Cloud provider, Hosting.com. That company currently generates 12% of its revenue from Australian companies. The number is even more pronounced, given the fact that Hosting.com have *“no one on the ground in Australia and we actually do nothing special for Australia.”*

The reason for the high proportion of companies from outside the US now seeking to use the company's Cloud offering appears to be performance, with 20% of its business now being organisations not based in America trying to service the North American market and wanting to move their applications to North America to overcome latency issues.

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.

Industry Exploitation

Australia's diverse, medium-sized economy provides advantages for both Cloud providers and users, especially around SaaS and Platform as a Service (PaaS).

- Australia is one of the world-leaders in the use of virtualisation, with twice the adoption rate of any other country, according to VMware. Australian enterprises are 'ready for the Cloud' and have the right skill sets.
- The NBN will be the catalyst/enabler of broadly distributed Cloud computing solutions.
- Australia offers an environment in which industry, research communities and government can collaborate relatively easily when compared to more complex locations of Europe or larger land masses such as North America.
- The country has a medium-sized yet very sophisticated economy, in which challenges can be undertaken with less risk and cost than in larger, more complex economies
- Australia currently hosts a healthy economy, rather than one in which public sector spending is being cut dramatically or industry is struggling to grow.
- Australia is well placed to tackle the same challenges facing many developed economies; e.g. the rising costs of health care, an aging society, long term sustainability, boosting productivity and innovation and adapting education to the technological age.

Australia will build on its advantages if government, industry and the research community can collaborate on exploiting the NBN for solutions delivered by SaaS to consumers and companies. Promising areas include education, health, aged care, funds management/retirement investment, natural resources, eco-tourism, sports management, agri-business, medical research and other vertical sectors, none of which depend on international links. Australia can take the lead in developing its own solutions and market the resulting "know-how" and IP around the world. Such Cloud-based solutions would highlight the foundational role of the NBN in transforming the economy. Sustainable technologies may be another selling point, as may tools for carbon emission calculation and management.

As previously mentioned, apart from insufficient and expensive internal capacity and the cost of carriage, potential inhibitors may also include the perception of security risk, rather than its reality. Education has a strong part to play in alleviating these fears. Solutions flagged as Cloud-based tend to raise warning flags among customers, while if exactly the same services are termed 'additional features', they pass without comment. Risk management strategies need to be discussed with regulators such as the APRA.

The majority of potential Cloud adopters in Australian industry are still confused about what Cloud computing is, what it can accomplish and how its various models differ - particularly in terms of local 'Hosted Utility Services'. The key lies in emphasising its elasticity and its potential for driving down costs through shared economies of scale. CSIRO and NICTA as Australian Government-funded research organisations, coupled with their capabilities in Cloud computing research areas, are well placed to clarify these matters. In addition, initiatives such as the Australian Centre for Broadband Innovation and the Institute for a Broadband Enabled Society can contribute to clearing confusion about Cloud computing and encourage uptake.

Standards

When information is placed in the Cloud, customers have very little idea where their information is, what is happening to it and what risks might be involved. Such concerns can best be addressed by the adoption of common open standards by Cloud vendors to improve transparency, trust, data portability and interoperability.

There is an ever more diverse range of Cloud computing solutions offered to companies seeking to move away from in-house IT provision. Commonly agreed open standards will allow platforms to share a range of infrastructure across different service providers. Management and functional standards are under development, while infrastructure standards are already advanced, particularly in the US. There are at least 23 standards development organisations in the world, sponsored by various organisations.

Network Communication

Setting Cloud computing within the regulatory reform agenda, both at a state and national level, is emerging as a priority. Newly installed independent systems at a federal level tend to duplicate the information they hold and Cloud computing offers a possible solution to such expensive redundancy by offering the potential for legacy systems to communicate with each other.

If state and federal systems can be connected economically and efficiently through Cloud computing, they could create a single portal for business interaction with state government. There is also a scope for 'hybrid' Clouds – i.e. the use of a Cloud solution in conjunction with an in-house departmental service. Such plans lay at the heart of the public policy discussion but also have the potential to generate attractive business opportunities.

Control Over Data

While some Task Force members consider that Cloud computing will allow supply chains to become fragmented and widely distributed, others felt that Cloud computing enables transition to more flexible supply chains. Either way, Cloud computing requires the generation of new risk profiles and introduces complicating issues of control.

Cloud computing may exacerbate fundamental asymmetries in information, and therefore power, between service providers and small consumers. Large customers could demand high levels of control denied to individual consumers and small businesses, whose information could be mercy of the service providers. In this context, the content and quality of contractual terms and conditions will become paramount.

Privacy

Cloud computing is increasingly used as both a weapon and defence against global, cross-border cyber-attacks. The need to protect the privacy and security interests of consumers and businesses is emerging as a significant issue, particularly in light of past difficulties in building consumer trust in e-commerce transactions.

The term 'privacy' spans a continuum between all information being entirely open to view through to it being completely closed in terms of access. The increasing fragmentation of data storage in the Cloud creates new security and privacy issues. Technical solutions to improve privacy in the Cloud exist, but phenomena such as Facebook, which are 'semi open', complicate the environment. Consumers do not know where their Facebook information is held or what their privacy protections may be. Recent controversy regarding Facebook's use and ownership of personal information has raised concerns in some quarters.

While it is important for consumers to be informed about the implications of using Cloud-based services for their ability to control their personal information, and for those controls when exercised to be effective, businesses considering adopting Cloud computing also need to be aware of their privacy obligations. Businesses should review the privacy and security protections offered by Cloud vendors and ensure that they are able to continue to meet their privacy obligations. These include the ability to retrieve information and ensure that all back-up copies are deleted.

Most privacy laws around the world are applied at a national level only and follow a similar pattern. They attempt to address privacy concerns by applying principles to the collection, use and disclosure of personal information by an organisation. These principles are usually complemented by ensuring access by individuals to that information, and have relied heavily on individuals being:

- informed about these practices
- able to understand the consequences of them
- able to make sensible decisions as a result, and
- acting as the first line of enforcement (through complaints etc.)

The explosion of personal information collection by ever more complex supply chains that operate over ever more jurisdictions has meant that these underlying assumptions no longer hold. The individual is not in a position to undertake appropriate handling of personal information and single jurisdiction legislation is being rendered irrelevant. Moreover, organisations that wish to comply with all the laws that impact them are finding it increasingly difficult to do so, while organisations that wish to ignore them seem to be able to do so with impunity.

In the first instance, existing international security and privacy frameworks, such as they are, could be applied to the Cloud, rather than generated separately. Security problems facing the Cloud, such as digital forensics, the regulation of computer records and the threat of malware and other security concerns have already been tackled previously with varying degrees of success. Privacy challenges in the Cloud, especially when multi-jurisdictional, are much less resolved. The initiatives by APEC, including the Cross Border Privacy Enforcement Arrangement between privacy regulators and the Cross Border Privacy Rules framework, are a promising start, but more is likely to be needed.

The role of Cloud computing in data service provision across diverse sites is increasingly important, with commercial providers currently outstripping scientific and academic resources in terms of capacity and capability. There must be assurances that sensitive data can be extracted at the end of a contract without confidentiality being jeopardised.

In Australia, over the last decade, public concern over privacy has seen a plethora of privacy laws, some general such as the Privacy Act, and some quite specific such as the Do Not Call legislation. As is the case elsewhere in the world, almost all of these laws have had a strong focus on protecting personal information within a single jurisdiction.

Public policy makers on both sides of the Atlantic Ocean are contemplating new privacy frameworks that respond to these developments by calling for privacy frameworks based on

- 'Privacy by Design' principles,
- Development by organisations of Binding Global Codes that meet minimum criteria
- Backing by credible accountability by the organisation to credible third party accountability agents
- Backstop enforcement by a government regulator only when the effort of accountability agents has not led to satisfactory resolution.

The Hunton and Williams paper '*A New Approach to International Transfers In Response to the European Commission's Communication on "A comprehensive approach to personal data protection*"' of January 2011 is a very credible attempt to set out such a framework. However, it is important to note that such a framework depends on credible, effective international cooperation between government regulators.

Consumer Trust

Trust is a vital enabler of commercial interaction on the internet, and will become even more important as Cloud computing become ubiquitous. Individual and company reputations are easily besmirched and hard to restore.

A distinction can be drawn between "sophisticated" and "unsophisticated" purchasers of Cloud computing. As in the field of financial services, "unsophisticated" consumers may need protection and benefit from 'trust-marks' not relevant to "sophisticated" larger players. However, transparency regarding privacy, data accountability, openness and conformity to standards has the potential to generate trust and therefore encourage use of Cloud computing to the benefit of everyone.

The GAP Task Force felt that the use of such 'trust-marks' might help build consumer confidence provided they are supported by "backstop" privacy enforcement authorities such as those set out by APEC for Cross Border Privacy Rules. If all Cloud providers signed up to a credible, enforceable agreement to maintain a certain level of procedures and standards, public trust in them would increase to the benefit of all concerned.

The issue of trust needs to be discussed from both the perspectives of suppliers and consumers. It is necessary to define the elements which demand trust and could be 'trust-marked' accordingly. Data exists at varying degrees of value and privacy, but many providers do not manage access to and verification of their customers' data in such differentiated terms.

A trust mark system such as the use of “star ratings” should be applied to Cloud providers with some caution, however. If a five-star rating site went down, confidence in the system as a whole would be undermined, while if a large provider was awarded a low star rating, an undue level of controversy might ensue.

Another approach could be a requirement to every Cloud provider to make explicit statements on a common set of policies, procedures and standards such as, for example, who owns the data and what third party has right of access to data and under what circumstances (e.g. Patriot Act). Such a mandatory requirement to inform the public and industry could be used by the Cloud providers as a business differentiator – or lead to changes based on consumer/business pressure.

Given the move from hardware to software in terms of network provision, Australia needs to be flexible in its approach. Exclusive, security-bound contracts between government bodies and providers are becoming outdated in the face of Cloud computing solutions but effective mechanisms for building and maintaining trust are fundamental to the formation of more flexible solutions. The World Economic Forum is now beginning to explore this space and there is an opportunity for Australia to take the lead.

ENCOURAGING CLOUD COMPUTING IN AUSTRALIA

The Task Force considers that the four main questions facing government in relation to Cloud computing are:

1. How to protect “unsophisticated” users? (e.g. by protecting privacy)
2. How not to hinder “sophisticated” users? (e.g. major commercial customers)
3. How to encourage development? (e.g. drive open standards)
4. How to exploit the technology? (e.g. make best use of infrastructure and encourage profitable solutions)

These four considerations have influenced the Task Force’s views about what it should propose to Government.

Leadership and vision

As Cloud computing can be seen as a continuation of internet evolution, rather than a revolution in itself, governments which have already embraced e-solutions should adopt a pro-Cloud stance and integrate preparedness for its employment in forthcoming infrastructure investment, particularly as Cloud computing can turn fixed capital costs into variable costs.

At the national level, a clearer vision is required for Australia's computing future. Through its investment in the National Broadband Network, the Australian Government has already clearly recognised the benefits of a strong and vibrant digital economy. A key objective of this investment in the NBN is to pay a dividend to the Australian people through enhanced productivity and innovation in the long term The Australian government needs to also now embrace Cloud computing as a key complement to its investment in the NBN. The Task Force believes that Cloud Computing services will be the key element in enabling the NBN to be a success. Consequently, the Australian government should assume a leadership role both as a user of Cloud computing and also as a facilitator of the uptake of Cloud computing across the Australian economy and society.

It is important that the Australian Government adopt a strong leadership role in stimulating the digital economy and realising the economic and productivity benefits which will be enabled by the NBN. As part of the Government’s broader digital productivity agenda, the adoption of Cloud computing represents an important opportunity for the Government to not only work more efficiently and save money in its own ICT administration, but to lead the way in encouraging the use of innovative and productivity-enhancing technologies by Australian businesses more generally.

Engagement with industry

Greater engagement with Cloud providers needs to be encouraged. A number of bodies are already considering the issue of Cloud computing and need to cooperate to create a strategic approach. Major computer companies have expressed their interest in successfully exploiting this expanding market while avoiding potential consumer pitfalls. The need to collaborate across the industry and with government bodies to achieve these goals is paramount. The Australian Information Industry Association (AIIA) can play a strategic role in encouraging such collaboration and has commenced this through the recent establishment of an industry Cloud Taskforce.

Given Australia's local advantages and constraints, one approach could be to encourage collaboration among government, industry and the research community on the back of the NBN. Specific initiatives could include case studies, reference architectures, joint proofs of concepts, workshops, and demonstrations.

Global influence

Australia is one of a small group of countries which show intellectual leadership on digital policy and associated regulatory issues. It has already, for example, led the way in legislating against such internet annoyances as spam. Australia should continue to build upon its influence in existing multilateral bodies to help to develop global standards and policy frameworks to encourage the further development of Cloud computing in Australia and overseas. It should also seek multilateral agreement on mechanisms to deal with the multi-jurisdictional issues which are thrown up by the widespread adoption of Cloud computing services including issues relating to privacy, information security and dispute resolution.

In regard to the need for regulation, however, it must be acknowledged that, as with some environmental concerns, local solutions may prove ineffective in the face of global challenges. In the end, the role of government is to protect the nation and the interests of its citizens. The government could add value in the market, but should not be dictating to users which standards to adopt. The Australian Government will not be able to influence such global markets directly, and previous attempts to set prescriptive standards in ICT have proved counterproductive.

Improvement of critical infrastructure

The Task Force considers that government should explore measures to enhance Australia's international connectivity. There are two key advantages in upgrading Australia's international capacity:

1. It makes it more likely that major Cloud infrastructure is built here, and that services not currently available to Australian consumers will become so, and
2. It makes it more likely Australian businesses will get world-class Cloud services developed for the international market

Cloud computing in Australia has to be part of a global Cloud. Improving and expanding the undersea cable connections to Asia and America would both reduce the risk of undersea cable disruption and improve capacity and speed. More capacity from the West and North Coasts, via the large and growing market of Indonesia, would make Australia a more attractive proposition for data centres.

'Smart' and 'soft' regulatory approaches

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.

An approach that is based on risk and principles would be beneficial, not least because this has proven successful for the Australian financial industry and has helped Australia weather the global financial crisis in comparatively good shape. This model has the advantages of being clear, relatively simple and effective.

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.

The National Broadband Network (NBN)

Advantage should be taken of the NBN's topicality to expand the range of the debate as 'pipes alone will not be enough' to make full use of the capacity. The business case for the NBN is based on growth which will in turn be boosted by the Cloud. The real future value of the NBN will be generated from the web applications which arise from it.

The Cloud will allow domestic users to fully realise the potential of the NBN without having to upgrade their computing devices while the NBN should help independent suppliers of services challenge the existing major players in the market. Government should work to remove barriers to entry and ensure that small service providers offer assurances on security and privacy. More critically, however, government should be exploring now the opportunities for utilising the NBN connectivity and Cloud computing services in a wide range of sectors such as education, healthcare, the not for profit sector and the various levels of government itself.

Australia should be profoundly interested in encouraging use of the NBN to meet local needs, particularly those of disadvantaged groups in society. Whatever the success of the NBN domestically, the latency caused by Australia's geographical position may limit its consideration as a major host of global Cloud data servers. However, the creation of an efficient domestic network system and 'safe harbour' provisions for service providers will encourage foreign interest in itself.

There will clearly be some significant Cloud infrastructure in Australia in the future to overcome the latency problems caused by its position, not least in the serving of advertisements. Greater cable connectivity between Australia and Asia and the USA should reduce, although not eradicate, latency problems in the future.

Education and awareness

Government officials, business leaders and senior politicians will require educating regarding the exciting possibilities of Cloud computing, as well as its possible risks. For example, the issue of Cloud computing was not raised in the 2010 election debates regarding the NBN.

Education and cyber safety campaigns by the government could be applied to the Cloud. Such campaigns should target not only individuals, but also business and government agencies, to raise awareness of the obligations in the areas of privacy and security that such entities must meet when adopting Cloud-based services. A tool, so far underexploited by Australian Governments, is media exposure. Other countries, including the United States, have taken the opportunity to enhance public awareness of Cloud computing through media address with some success.

Government initiatives such as the Australian Centre for Broadband Innovation and the Institute for a Broadband Enabled Society can contribute to clearing confusion about Cloud Computing and encouraging uptake.

Government as a major Cloud customer

Recognising its power as one of the largest customers of computing services in the country, government has an opportunity to act as an 'anchor tenant'. It could help the Cloud develop by tackling the major issues it faces on the domestic front, in the hope that such solutions could then inspire similar action around the world. An understanding of the amount of infrastructure needed to deliver cost effective services is important when calculating its costs and benefits to the economy. The industry will tend to be dominated by a small number of vendors as it matures, and the government should not try to pick technological winners, but instead help encourage trust and the adoption of open standards to maximise customer flexibility and market innovation.

Self-regulation

The purpose of regulation should be to regulate the “behaviour” of technology providers, as much as the actions of individuals and corporations. This can be done through government legislation and administrative processes regulated by appointed bodies, but also by self-regulation by interested parties acting in concert, with the threat of exclusion as its most effective sanction.

The scope for self-regulation of Cloud service providers in Australia should be explored further by industry and government.

Privacy protection and security

Safeguarding the personal information of Australians is a continuing issue, particularly in protecting people from malware whose threat continues to act as a disincentive to some people fully using the internet. Consumer electronics are regulated to ensure their physical safety, and similar approaches to Cloud computing and other internet activities may achieve a degree of cyber-security in the future.

The risk associated with Cloud computing is currently spread among a wide range of vendors. However, if the industry becomes more concentrated as it matures, then the risk posed by the failure of a major provider increases.

Security concerns should be seen as ICT issues, rather than ones which affect only the Cloud. The Australian Government can play an international role by encouraging the adoption of common open global standards . Such standardisation of privacy principles in nation states would encourage more cross border activity and experience has shown that regulators influence expectations and responsibilities beyond the narrow terms of legislation. One point for domestic legislators to note is that Australian small businesses are currently not covered by the Privacy Act 1988 (Cth) and this may cause problems with accreditation with the EU.

Standards and protocols

Many of the concerns expressed in regard to Cloud computing are similar to those raised previously with outsourcing and other issues and have already found solutions. Cloud providers could be encouraged to sign up to a series of protocols and be certified with a range of “badges” to help consumers decide on which package best suited their needs. New organisations will emerge to offer such certification, and past experience suggests that, in general, they provide a trustworthy service as long as fraudsters are quickly dealt with by the authorities. The OECD and other international bodies have an important role to play in driving this process. Current developments in Britain could be significant to Australia and the international perspective should not be ignored.

Recommendations to Government

CENTRAL RECOMMENDATION - Statement of Support for Cloud Computing by the Australian Government

In recognition of the importance of Cloud computing to the positioning of Australia as a leader in the global digital economy, the Government should publicly acknowledge its support for Cloud computing.

This should be issued by the highest levels of Government and should:

- Recognise the potential benefits of Cloud computing to Australia's digital economy
- Acknowledge the Australian Government's strategic direction paper, which recommends that *"Agencies may choose Cloud-based services if they demonstrate value for money and adequate security."* The paper's phased approach includes early trials and the appropriate adoption of Cloud computing solutions by government departments and agencies.
- Recognise the opportunity for national government agencies including the Department of Broadband, Communications and the Digital Economy and the Department of Finance and Deregulation to work co-operatively to drive the consideration and adoption of Cloud computing, both domestically and internationally.
- Recognises legitimate concerns of end users that they may lose control over their personal information unless Cloud-based service offerings are constructed appropriately and are covered by effective, enforceable, easy-to-access help and complaint resolution services that address the challenge of services operating in multijurisdictional circumstances.

RECOMMENDATION 1 - Leadership and Vision

This report finds that the cost savings offered by Cloud computing are already encouraging their adoption by a host of Australian domestic and business users, regardless of remaining regulatory challenges (page 12). The Australian Government should not lag behind business and consumers, but should adopt a leadership role in driving the uptake of Cloud computing solutions in Australia.

The Australian Government (through the Department of Broadband, Communications and the Digital Economy and the Department of Finance and Deregulation) should assume a joint leadership role in encouraging Australian Governments, business and consumers to harness the benefits offered by Cloud computing by:

- Recognising the ability of the Australian Government to stimulate the Australian digital economy by acting as an 'anchor tenant' to encourage the adoption of Cloud computing solutions in Australia

- Recognising that the rate of adoption of Cloud computing by Australian Government agencies will be influenced by business requirements, risks to privacy and security in the public Cloud, maturity of the domestic Cloud services market, and the requirement for development of standards to support the portability of data/information held in public or private Clouds.
- Reviewing the recommendations of the report of the GAP Task Force on Cloud Computing
- Setting forward-looking targets and timeframes to encourage the trial and (appropriate) adoption of Cloud computing solutions by appropriate Government departments and agencies. As indicated in the Australian Government's Cloud Computing Strategic Direction paper, proof of concept trials have already commenced and will commence through 2011 and onwards.
- Reviewing and adopting where appropriate policy instruments developed by other Australian Government agencies, e.g. DIISR, the Attorney-General's Department (AGD), the Office of the Australian Information Commissioner (AOIC), etc. This includes recognition in policy instruments of any guidance documents published by other agencies, for example security guidance published by the Defence Signals Directorate (DSD).
- Establishing processes and procedures for assessing the risks of adopting Cloud computing solutions and the allocation of those risks between Cloud computing platform providers, businesses built on those platforms and end consumers.
- Setting time frames for developing industry, regulatory or policy solutions to minimise these risks. These processes and procedures should actively seek input from both business and consumers. Particular attention needs to be paid to structuring of contracts and the way that they allocate risk, either by vigorous application of existing consumer protection law or specific amendment to it.

RECOMMENDATION 2 - Establishment of a Cloud Computing Task Force

The Department of Broadband, Communications and the Digital Economy should establish a standing Cloud Computing Task Force, with membership made up of relevant Government departments, regulators, industry and consumer representatives. The Task Force should perform an active role in assessing and communicating the results of Cloud computing trials, commissioning research, undertaking case studies and joint proof of concepts, and providing a thought leadership role to encourage the adoption of Cloud computing solutions in Australia.

This Task Force should work closely together with the Government-only Cloud Information Community (CLIC), which was established by the Department of Finance and Deregulation and the AIIA Cloud Taskforce.

RECOMMENDATION 3 - Engagement

The report recognises that widespread adoption of Cloud computing solutions will be facilitated by ensuring best practice privacy protection and security as well as the development of standards and protocols by Cloud computing vendors. It will be essential that Australia's approach contributes to and is consistent with global developments and avoids isolating Australia through special rules and standards.

The Australian Government should take a central role in the domestic and international fora developing these standards, protections and protocols, including:

- Working with relevant Australian Government agencies, industry, consumers and leading international authorities such as NIST, ENISA, ISO and internet standards bodies (such as W3C, OASIS etc.) to develop best practice guidance, standards and protocols for Cloud computing
- Engagement with leading jurisdictions and authorities internationally on data protection and privacy, clear rules for the allocation of jurisdiction, responsibility and liability, and consumer protection
- Engagement with the international dialogue already under way between leading US and EU authorities and global businesses on developing an efficient and effective multi-jurisdictional accountability process
- International work on trust marks for Cloud computing solutions
- Formulation of the APEC Cross Border Privacy Rules
- World Economic Forum work on developing security standards for and trust in Cloud computing solutions.

RECOMMENDATION 4 - Assessing Australia's Cloud Readiness

The report recognises that many major companies involved in Cloud computing do not yet have a presence in Australia Cloud. The Minister for Broadband, Communications and the Digital Economy should consider establishing an inquiry to investigate:

- The economic, geographic, market, or regulatory reasons why this is the case and propose recommendations designed to encourage the increased availability of Cloud computing infrastructure and international data capacity in Australia.
- The appropriate regulatory framework for encouraging the adoption of Cloud computing to advance the Australian digital economy, including consideration of the appropriate industry and legislative structure to support a self or co regulatory framework for Cloud computing.
- How best to increase consumer and business awareness of, and trust in, Cloud computing solutions.

This inquiry should take into consideration that Finance, in conjunction with DSD, is currently assessing the requirements for an accreditation program for Cloud computing services providers.

RECOMMENDATION 5 - Education and Awareness

The Department of Broadband, Communications and the Digital Economy should be given a specific role (and appropriate funding) to educate Australian business and consumers on how best to harness the benefits and manage the potential risks of adopting Cloud computing solutions. For example, the Government's Business Online website - *http://www.business.gov.au/BusinessTopics/Onlinebusiness/Pages/default.aspx* - could provide information for small business on adopting Cloud computing solutions.

RECOMMENDATION 6 - Development of self or co-regulatory approaches to Cloud Computing issues

There was widespread support within the Task Force for government to proceed cautiously before leaping into any regulatory responses to the range of issues of concern created or exacerbated by Cloud computing. This was in recognition of the rapidly changing nature of the technology, combined with a view that some issues could be addressed by a combination of education and awareness, development of trust marks and the further development of standards. Nevertheless, the Task Force also believes that there is the clear opportunity for industry to take the lead here and to work with government and consumer agencies to explore the scope for industry codes of practice to address many of the issues of potential concern to consumers and government.

IN CONCLUSION

What does Government need to know?

- The growth of Cloud computing is inevitable and inexorable. The Cloud changes the way in which computer services are purchased and managed, and can deliver a range of benefits and considerable savings
- There is a significant symbiosis between the Cloud and the National Broadband Network (NBN) – in practice, the combination of NBN connectivity with increasing use of Cloud computing holds the key to a vast range of productivity improvements in the Australian economy.
- Cloud computing will aid the development and use of applications which will drive benefit from the pervasiveness, speed and low delay of NBN infrastructure. The Cloud and the NBN can deliver large productivity and efficiency gains for large businesses, SMEs, and all levels of government. The potential improvements for small business and local government services are especially significant.
- Concerns regarding privacy, security, identity management and jurisdictional issues remain, although if approached in the right way, security may be enhanced by Cloud computing. Some types of data and application are inherently not suitable for Cloud deployment.
- While the risks associated with Cloud Computing are largely the same as those already being faced by the wider community, the significant increase in the number of links in any supply chain and the number of jurisdictions involved means a much stronger focus on end-to-end risk management, 'risk/return' investment profiles, compliance and enforcement will be essential.

What should Government do?

- Proposed information law reforms in Australia, including privacy law reform and APRA-related legislation, should take into account the nature of Cloud computing and what is needed to facilitate its adoption, in order to provide effective compliance and consumer protection even when more than one jurisdiction is involved.
- Government should seek ongoing dialogue with Cloud providers and users, both to understand concerns and to raise awareness among different types of Cloud users (business users, consumers, etc).
- Government should seek a collaborative government approach as COAG processes and State and Federal ICT investments are in danger of wastefully duplicating solutions, while the use of Cloud approaches could offer a cheaper, more unified approach.

- Policy makers and decision makers should be educated about the issues associated with Cloud computing, specifically the opportunities, risks and current best practice.
- Organisations researching the potential of Cloud applications facilitated by the NBN should receive adequate funding.
- The Government needs to engage in international discussions of Cloud and related issues.
- Government should recognise that in an area of rapid technological change, 'soft' regulation is more useful than restrictive regulatory strictures. A 'clearing house' approach to issues would be attractive.
- Cloud computing should form part of cross jurisdictional government discussions to reduce costs and improve services.
- Australia's high cost structure, reliance on carbon-intensive energy, physical location and restricted international connectivity make it difficult to establish a business case for locating a major public Cloud server in Australia. Government might therefore investigate what incentives could be provided to encourage establishment of Cloud infrastructure in Australia. This may take the form of direct incentives, strategic arrangement of Cloud services for government at all levels to form a large aggregate customer, and improvements in international connectivity.

CONTACTS

Mr Keith Besgrove
First Assistant Secretary
Digital Economy Services Division
Department of Broadband,
Communications & the Digital Economy
Telephone +61 2 6271 1811
Email *keith.besgrove@dbcde.gov.au*

Global Access Partners (GAP)
53 Balfour Street
Chippendale NSW 2008
PO Box 978
Strawberry Hills NSW 2010

Ms Olga Bodrova
Senior Research Analyst
Global Access Partners
Telephone +61 2 8303 2420
Fax +61 2 9319 5754
Email *obodrova@globalaccesspartners.org*

ATTACHMENTS

NIST definition of Cloud computing

Peter Mell & Tim Grance
National Institute of Standards and Technology, Information Technology Laboratory

NB: Cloud computing is still an evolving paradigm. Its definitions, use cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time. The Cloud computing industry represents a large ecosystem of many models, vendors, and market niches. This definition attempts to encompass all of the various Cloud approaches.

Definition of Cloud Computing

Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models.

Key Characteristics

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service's provider.
- *Ubiquitous network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- *Location independent resource pooling.* The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for rent often appear to be infinite and can be purchased in any quantity at any time.
- *Pay per use.* Capabilities are charged using a metered, fee-for-service, or advertising based billing model to promote optimization of resource use. Examples are measuring the storage, bandwidth, and computing resources consumed and charging for the number of active user accounts per month. Clouds within an organization accrue cost between business units and may or may not use actual currency.

Note: Cloud software takes full advantage of the Cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

Delivery Models

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email). The consumer does not manage or control the underlying Cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g., java, python, .Net). The consumer does not manage or control the underlying Cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).

Deployment Models

- *Private Cloud.* The Cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.
- *Community Cloud.* The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- *Public Cloud.* The Cloud infrastructure is owned by an organization selling Cloud services to the general public or to a large industry group.
- *Hybrid Cloud*. The Cloud infrastructure is a composition of two or more Clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting).

Each deployment model instance has one of two types: internal or external. Internal Clouds reside within an organisations network security perimeter and external Clouds reside outside the same perimeter.

The most advanced Cloud standards (mid 2010)

Standard	Description	Proposed by
OVF (VM portability)	Open Virtuaslisation Format for virtual machines (VM)	Distributed Management Task Force (DMTF)
OpenStack API	Open APIs to create OSS Clouds on any commodity hardware	NASA, Rackspace
AWS (EC2, S3) 'de facto'	Amazon Web Services (AWS) Cloud formats	Eucalyptus, Canonical
UCI	Unified Cloud Interface	Cloud Computing Interoperability Forum (CCIF)
CMDBf	Configuration Management Database Federation	DMTF
OCCI	Open Cloud Computing Interface	Open Grid Forum (OGF)
CDMI	Cloud Data Management Interface	Storage Networking Industry Association (SNIA)
Cloud Trust Protocol		CSC with CSA, CloudAudit (aka A6)
vCloud		VMware, DMTF

(Source: CSC Australia)

Australian Government Cloud Computing Strategic Direction Paper

Developed by the Department of Finance and Deregulation (Australian Government Information Management Office [AGIMO])

AGIMO has developed and released in April 2011 the Australian Government's Cloud Computing Strategic Direction paper, 'a whole-of-government' approach to Cloud computing delineated over three distinct stages. The initial enabling phase will see the establishment of a Cloud framework by agencies and the adoption of a set of principles and best practice documents. Stage Two will involve a transition to the use of public Clouds, and from 2011, the re-examination of Commonwealth procurement guidelines. Proof of concepts and pilots will also be undertaken. Stage Three will see the emergence of private, community and government Clouds and their widespread employment by government agencies. All phases are to run concurrently

AGIMO is consulting with other government agencies in the USA, the UK and elsewhere. User driven initiatives, such as the Open Data Centre Alliance, are developing codes of best practice and standards and their work may be of relevance to government entities although private and public organisations can face different issues in regard to security and privacy. Considerations of the fate of current technological investment if Cloud computing is widely adopted in the future have been factored into the calculations of its potential cost savings.

The Cloud Computing Strategic Direction paper positions the Australian Government to take advantage of the benefits of Cloud computing while not compromising the security of its operations or people's privacy or sensitive information. It strategy states that:

> *"Agencies may choose Cloud-based services if they demonstrate value for money and adequate security."*

The following summarises the specific activities that will occur as part of a three phase approach to increasing Cloud use by the Australian Government.

Stream 1: Enabling (2011)
Preparing to Adopt Cloud: Policy, Principles, Contract Guidance and Knowledge Sharing

1.1 Establishment of a Cloud Information Community

1.2 Whole-of-Government Cloud Framework

Components of the Government Cloud Framework may include:

- Cloud Principles
- Governance and compliance framework for community Clouds
- Guidance to agencies on issues associated with Cloud computing
- Service Provider Certification Program

Stream 2: Public Cloud (2011 onwards)
Tactical: Public Cloud adoption as offerings mature

2.1 Finance transitions AGIMO public-facing websites to public Cloud

2.2 Sourcing Model
Investigate sourcing model, e.g. Whole-of-Government (WofG) Public Cloud Service Provider Panel

2.3 Proof of Concepts / Pilots undertaken by agencies

Investigate - Agencies are encouraged to investigate opportunities to utilise Public and Hybrid Clouds

Adopt - Agencies are encouraged to consider the use of Public and Hybrid Clouds (subject to cost/benefit and risk considerations)

Stream 3: Private and Government / Community Clouds (Mid-2011 onwards)
Strategic: Whole-of-Government Approach integrated with the Data Centre Strategy

3.1 Data Centre Strategy Integration
The Data Centre Strategy program of work will undertake projects that will provide future Cloud capability:

a) The Data Centre as a Service (DCaaS) project will assess Cloud technologies in providing common data centre facilities and ICT solutions for the 50 smaller Australian Government agencies.
b) The Optimising Data Centre Use project will provide guidance to assist in pre-positioning agencies to use Cloud-type technologies.

At this time, it is not known whether the Data Centre as a Service will utilise Cloud services (indicative timeframe 2012-2013).

3.2 Government "storefront"
Finance will investigate a whole-of-government service / vendor catalogue or Government Cloud.

3.3 Investigation and adoption of private and/or community Clouds

- Investigation of Community Clouds
- Adoption of Private Clouds
- Adoption of Community Clouds

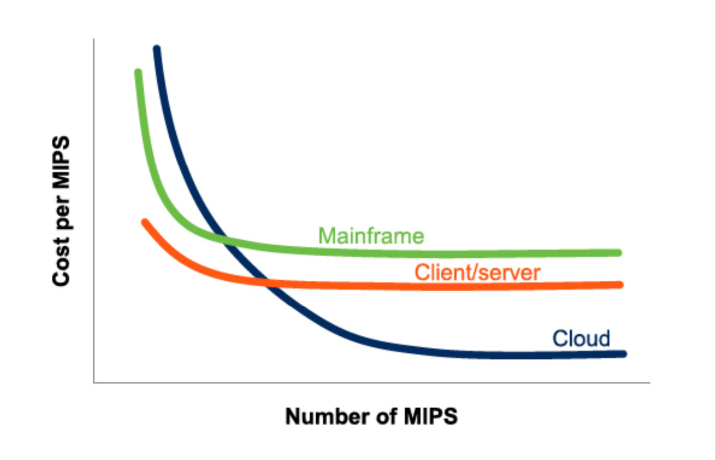
The Economics of the Cloud – an Industry Perspective

A recent Microsoft report *"The Economics of the Cloud for the Public Sector",* released in November 2010, examines the possible economic drivers for the adoption of Cloud computing, with a specific focus on 'private' Clouds.

Cloud computing requires large, expensive data centres, but these offer great economies of scale, not least in power consumption. While separate applications are commonly run on separate servers today, Cloud computing allows usage to be aggregated, so handling the peaks and troughs of demand from different time zones. Businesses are often uncertain of the extent and type of their future computing needs and whether Cloud computing solutions offer the cost effective flexibility they require.

Figure I. Economies of Scale (illustrative). (Source – Microsoft)

(NB. MIPS – million instructions per second)



Large data centres also improve service delivery. Cloud computing removes the need for single tenant applications – e.g. single customers running isolated copies of licensed software on individual computers. The management, patching and maintenance of these individual software packages is a major expense and security problem while multi-tenant applications allow a single instance of the application to service many clients in a public Cloud, greatly simplifying the procedures required to maintain it. As well as major cost benefits, this offers greater flexibility as each customer can potentially access an individually customised service depending on their requirements.

Some customers have welcomed the potential benefits of a globalised Cloud, but would prefer to use private, single tenant or 'in-country' Clouds for security reasons. In Australia, this seems likely to be true of many government agencies, for example. However, such private Clouds may prove to beconomically unsustainable and would not deliver the benefits and economies of scale offered by public, multi-tenant global Clouds.

Recent, separate analyses by Microsoft and NICTA have reached similar conclusions that the potential cost savings of such public Clouds could be around ten times greater than the savings which could be achieved by the use of private Clouds.

Microsoft sees the cost savings offered by Cloud computing as certain to change computing practices in the near future. Cloud computing will allow large CPUs to be rented for large but occasional tasks, and so more computing will be done in real time in the Cloud, rather than over a long time by in-house computers of much lesser capability. Computing will continue to grow as a percentage of GDP as people's lives become ever more 'digitised' while the Cloud will also facilitate the future use of artificial intelligence with simple user interfaces.

Figure II. Economies of Scale in the Cloud (Source – Microsoft)
NB. TCO – total cost of ownership

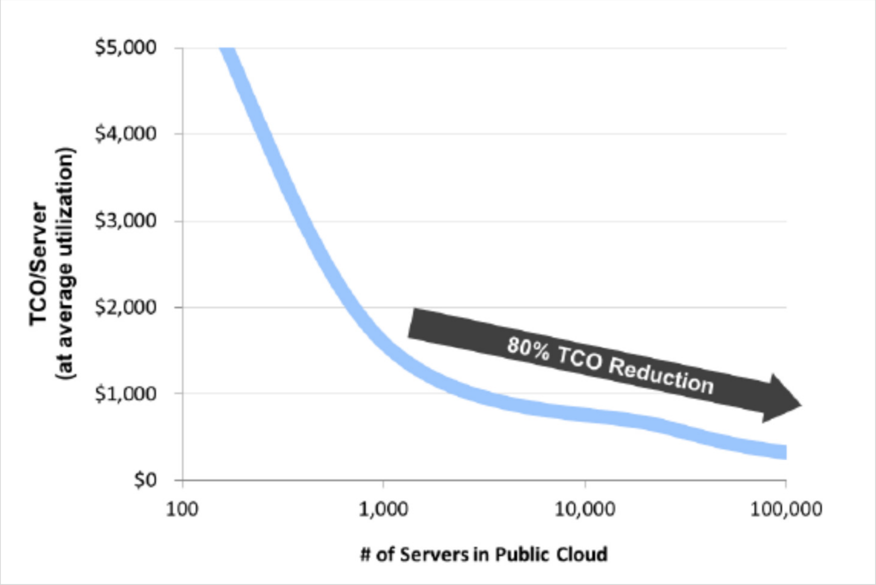
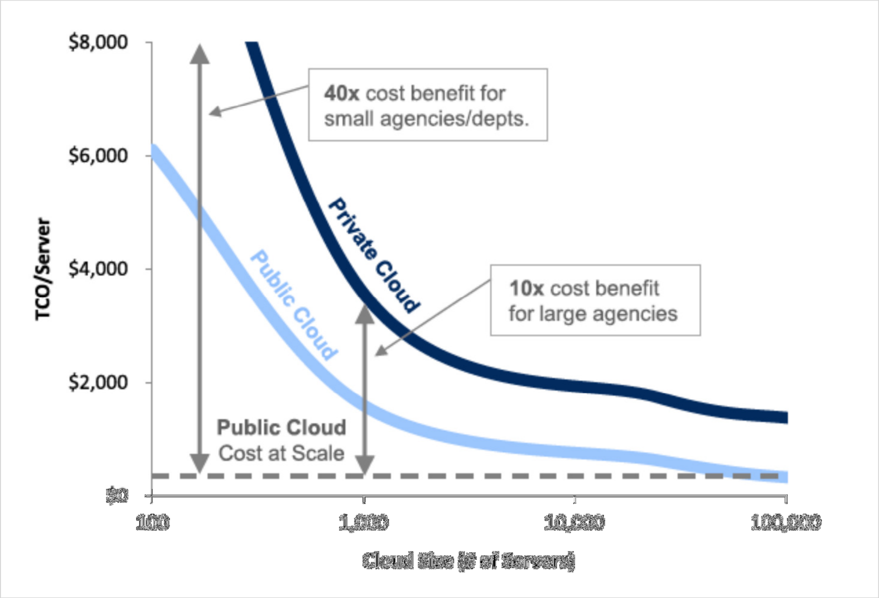


Figure III. Cost benefit of public Cloud (Source – Microsoft)



For certain situations, Hybrid Clouds will develop, in which private Clouds use public infrastructure to gain some of the benefits of the private Cloud while maintaining some of the benefits of the public Cloud. As it is impossible to build the infrastructure required for private Clouds while gaining the cost savings of public Clouds, such hybrid Clouds will tend to operate in 'virtualised' data centres, rather than dedicated data servers. Regulation of such provision must help public Clouds become a reliable framework, rather than prevent their usage for such purposes altogether.

There needs to be a rethink of information management by both clients and suppliers over the next five years. The paucity of Australia's internet provision currently mitigates against the use of Cloud computing domestically but this situation should change rapidly as the National Broadband Network (NBN) is rolled out. There is also a fear of malware compromising security and efficiency on a mass scale in a Cloud environment. However Cloud providers would also have the resources to protect themselves against attack. The perception of possible malware problems may more damaging than any current threat, and although the potential for damage through insecure browsers into company systems remains significant this can be solved, in part, through better mutual identification systems.

The cost savings offered by Cloud computing are already encouraging their adoption by a host of Australian domestic and business users regardless of remaining regulatory challenges. Improved information handling procedures will allow economies, businesses and individuals to interact through the Cloud while Cloud computing will also be driven by the major savings it offers in software licencing.

Critical Infrastructure Issues - Submarine Cable Resilience

Australia's dependence on submarine cables

Australia relies on submarine cables for 99% of its international communications connectivity, and there is no feasible alternative. It is estimated that existing satellite capacity can accommodate only about 1% of Australia's communications currently serviced by submarine cables. As an island nation, Australia is particularly dependent on submarine cables for its international communications as it cannot connect via overland cables as an alternate path. Given that the majority of electronic information is hosted outside of Australia, submarine telecommunications infrastructure enables Cloud computing.

Currently there are ten submarine cables connecting Australia to the rest of the world – eight off the east coast (Sydney) and two off the west coast (Perth and Port Headland). A major disruption to Australia's submarine cables would have severe consequences for the international transfer of data, including any Cloud computing services that use data outside of Australia.

Capacity constraint

As a result of Australia's reliance on submarine cables, the Taskforce recognises that there is a capacity constraint on Australia taking a major role in the hosting of Cloud computing solutions for the Asia/Pacific region. Performance latency will ultimately undermine the viability of Australia for this role.

Threats to and vulnerabilities in the submarine cable network

Submarine cables are vulnerable to a range of threats. Globally, natural hazards and accidents typically account for the majority of cable disruptions, and include natural events such as earthquakes and erosion of the seabed; and maritime activity or accidents such as bottom trawling, fishing, anchoring and dredging.

Submarine cables also face the threat of malicious attack. These attacks could be in the form of physical attack to the cable itself, cable landing stations, network operations centres or other physical infrastructure. In addition, attacks could be in the form of cyber-attacks to the systems that manage and monitor traffic travelling over the cables.

Due to the global and interconnected nature of the network, a disruption to Australian communications connectivity could occur after an incident on the other side of the world. Any level of security provided at the Australian end of a cable needs to be coordinated with the security arrangements at the other end, or that cable will still be exposed, i.e. the cable is only as secure as the far end.

Submarine cable resilience strategies

There are a range of strategies in place to mitigate the risk of a submarine cable disruption, including the use of regulated exclusion zones around the cable landing points; awareness raising activities by the Government; telecommunications industry mitigation strategies; and increasing use of international collaboration measures.

Case Studies

Australian Government Information Management Office (AGIMO)

AGIMO uses a large Cloud computing service provider to host data for *www.data.gov.au*.

Australian Taxation Office

80% of the Australian Tax Office's internet traffic already uses Cloud computing to store citizen data behind government firewalls.

Department of Immigration & Citizenship

The Department of Immigration and Citizenship has run a highly successful hybrid Cloud pilot for people applying from Spain to work in Australia, using Google and CSC as the service providers. There are six phases to the processing of such visas and the pilot saw phase 1 and 2, which are merely exercises in data collection, employing the Cloud solution, while the subsequent steps took place on the Departments servers. The use of Google allowed the employment of its real time translation service, monitored by human operatives. Video conferencing and other 'vertical' services may also offer scope for low risk Cloud computing solutions in the next two years.

QLD Government

Queensland State Government has incorporated a $60 million Cloud provider into its remit and is currently investigating ways to fully utilise this capability in its operations.

Australian industry

Australian firms who have already transitioned to Cloud computing include Westpac Banking Corporation, Commonwealth Bank of Australia (CBA), Telstra, Wilson HTM Investment Group and Optus.
Westpac, for example, is using private Clouds for testing environments and is finding them an efficient and cost effective IT solution, while CBA Michael Harte's vision around Cloud computing, both in terms of its IT cost reduction potential and as an enabler of next generation business innovation, is widely cited and discussed in Australia and around the world.

Optus, Melbourne IT, and iiNet have established themselves as providers of Cloud services at the Infrastructure as a Service (IaaS) tier.

International Perspectives

NIST (National Institute of Standards and Technology) in the United States and RESERVOIR (Resources and Services Virtualization without Barriers) in Europe are currently the largest research projects examining matters such as Cloud standards and interoperability. ENISA (The European Network and Information Security Agency) has developed a useful body of knowledge related to the sharing of data between EU states.

In the UK, CSC is working with the National Health System on new applications in e-Health. It has created a 'solutions express', staffed with doctors and nurses, to demonstrate and "walk-through" solutions at centres of health care. This allows stakeholder to experience e-Health first hand, thereby promoting uptake of services hosted in the Cloud.

Cloud Computing Initiatives from International Jurisdictions

United Kingdom

Name of Initiative	*Details*
Government Agency shift to Cloud Solutions	***Government*** agencies have chosen **Composite's** (sole specialised data virtualisation provider) proven data virtualisation platform to fulfill critical information needs, faster and with fewer resources. Establishment of Cloud network set to save up to 3.2 billion pounds a year.
DirectGov	As part of its commitment to Cloud the Government established ***the DirectGov Portal,*** hosting data for all Government departments and agencies. Provides a one stop area for the public and businesses.
Establishment of major Data Centre	**International Business Wales**, the economic development arm of the Welsh Assembly ***Government****,* and Next Generation Data have established a $326 million data centre. The center is the largest of its kind in the UK, and one of the largest in Europe.
Intelligent Cost Reduction initiative	As part of the UK Government's commitment to lowering Britain's deficit, Cloud Computing has been officially adopted as a method of intelligent cost reduction.
Data.gov.uk	Allows authorised developers to find ways of making Government information available to the public. Acts as App store for publicly developed apps based around released data. Provides significant aid to improving transparency.

United States of America

Name of Initiative	Details
Utilisation of existing Social Networking Public Cloud Services	• Social networking services such as Facebook, Twitter, YouTube and blogs are being used across Government Agencies as part of a commitment to new **"Open Government" initiatives**.
Adoption of "Cloud First" policy	• The US Government has adopted a **Cloud First** policy in which federal agencies are required to default to Cloud-based solutions where "a secure, reliable, cost effective Cloud option exists".
Transparency initiatives	• Government data is being made available to the public through established **Dashboards** and in raw form providing a first step to placing public data "in the Cloud". • Takes advantage of lack of copyright on Federal Government data in US.
Joint Authorisation Board	• Provided a mechanism for granting government-wide approval for agency Cloud Computing applications that can then be adopted by other agencies.
Apps.gov	• Gives Federal, State, Local and Tribal Governments access to Cloud-based IaaS and SaaS offerings through a Government Cloud storefront. • This takes advantage of existing surplus server infrastructure developed by individual agencies. • Expected to reduce infrastructure, software development and procurement costs.
Government Information Apps	• Utilisation of Apps to improve awareness of government issues such as **The White House** app for iPhone.
GovLoop	• A social networking site aimed at improving connections between agency employees. • Currently has 25000 Government employees as members
Increased Government Spending on Digital Security	• Increase in spending on digital security to $13 billion ***a year to assist with viability of Cloud options.***
Public Media Forum	• In the US Cloud Computing is getting significant levels of media attention due to the Government's commitment to addressing the new paradigm in a public forum. • Has improved public education about opportunities and challenges of new technology.

Singapore

Name of Initiative	Details
Open Cirrus Cloud Computing Testbed	• A research initiative implemented in 2008 comprising of the IDA and private stakeholders including Yahoo, Intel and HP. • Aimed at a joint stakeholder evaluation of Cloud Computing opportunities
Market Access Partnerships	• Comprehensive market access partnerships with Singtel and trade promotion agency IE Singapore. • Assists SMEs with forming consortiums that will then meet with partners in markets including Australia, India, Indonesia, the Philippines, and Thailand.
Commitment to increasing access to broadband	• Significant public financial commitment to increasing access to broadband for all citizens • Has lead to a 26% increase in access since 2005.
Collaboration with IBM	• Collaboration with IBM to establish a Cloud Computing research lab in Singapore. • Others already exist in other countries including the US, Vietnam and Ireland.
Regulatory commitment to facilitating Cloud	• Singapore's government has embraced and facilitated Cloud technology development by avoiding stringent levels of regulation hindering development in other Asian nations. • Privacy and Security issues still remain.

References

Australian Government Cloud Computing Strategic Direction Paper: Department of Finance and Deregulation, April 2011
http://www.finance.gov.au/e-government/strategy-and-governance/Cloud-computing.html

Cloud Computing Security Considerations*:* Initial Guidance. Cyber Security Operations Centre, Department of Defence, Intelligence and Security, April 2011
http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

The Global Information Technology Report 2010-2011, Transformations 2.0: World Economic Forum, April 2011
http://reports.weforum.org/global-information-technology-report/

Independent Review of the Implementation of the ICT Reform Program: Dr Ian Reinecke, June 2010
http://www.finance.gov.au/publications/review-implementation-ict-reform-program/docs/Review-of-ICT-Reform-Program.pdf

Review of the Australian Government's Use of Information and Communication Technology: Sir Peter Gershon, CBE, FREng, August 2008
http://www.finance.gov.au/publications/ICT-Review/index.html

Cloud Computing and Public Policy: Briefing paper for the ICCP Technology Foresight Forum; OECD, 14 October 2009;
http://www.oecd.org/document/38/0,3343,en_2649_34223_43921574_1_1_1_1,00.html

"Cloud Computing: Opportunities and challenges for Australia": Report of a Study by the Australian Academy of Technological Sciences and Engineering (ATSE), September 2010;
http://www.egov.vic.gov.au/trends-and-issues/information-and-communications-technology/Cloud-computing/Cloud-computing-opportunities-and-challenges-for-australia-in-pdf-format-1367kb.html

"The NIST Definition of Cloud Computing"; Peter Mell, Tim Grance**;** National Institute of Standards and Technology, Information Technology Laboratory; July 2009
http://csrc.nist.gov/groups/SNS/Cloud-computing/

"Engage: Getting on with Government 2.0": Report by the Government 2.0 Task Force, December 2009; *http://www.finance.gov.au/publications/gov20Task Forcereport/index.html*

"A study of the privacy, security and identity management implications of Cloud computing for home users and small to medium enterprises": A report prepared by Convergent Communications Research Group, The University of Adelaide for the Department of Broadband, Communications and the Digital Economy, June 2010

"Proposed Security Assessment and Authorization for US Government Cloud Computing": White House, FedRAMP, November 2010
https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf

"Australia: Cloud computing – legal issues in the Cloud": Mark Vincent, October 2010
http://www.mondaq.com/australia/article.asp?articleid=113912

"The Economics of the Cloud for the Public Sector"; Report commissioned by Microsoft. November 2010

"Cloud Computing: Comments to the Task Force on Report Recommendations", Queensland Office for Regulatory Efficiency, Queensland Treasury, December 2010

Cloud Security Alliance Consensus Assessments Initiative (CAI);
http://www.Cloudsecurityalliance.org/cai.html

'A New Approach to International Transfers In Response to the European Commission's Communication on "A comprehensive approach to personal data protection": Paper by Hunton and Williams, January 2011

"Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services"; Simon Bradshaw, Christopher Millard, Ian Walden; Queen Mary University of London, School of Law, Legal Studies Research Paper No. 63/2010; *http://ssrn.com/abstract=1662374*

*"**Information "Ownership" in the Cloud";*** Chris Reed, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 45/2010, *http://ssrn.com/abstract=1562461*

Task Force Member List

Ms Deborah Anton
Assistant Secretary, E-Security
Policy & Coordination Branch,
Attorney-General's Department

Mr Glenn Archer
First Assistant Secretary
Policy and Planning Division
AGIMO, Department of Finance
& Deregulation

Mr Allan Asher
Commonwealth Ombudsman

Mr Alan Bennett
Industry Leader, Government & Defence,
Australia & New Zealand,
HP Enterprise Services

Mr Keith Besgrove (Chair)
First Assistant Secretary
Digital Economy Services Division
Department of Broadband,
Communications & the Digital Economy

Mr Malcolm Crompton
Managing Director
Information Integrity Solutions

Ms Gabrielle Davies
Senior Enterprise Architect
Genesys Laboratories Australiasia

Mr John Dunne
Program Director, Applications Best
Sourcing, CTO Office, Westpac
Technology, Westpac Banking
Corporation

Dr Dean Economou
Technology Strategist,
National ICT Australia

Mr Rob Forsyth
Managing Director, Asia Pacific
Sophos

Mr Peter Fritz AM
Group Managing Director
TCG Group; Managing Director
Global Access Partners

Mr Bob Hayward
Chief Technology & Innovation Officer
CSC Australia & CSC Asia

Mr James Kelaher
Director, Smartnet

Dr Anna Liu
Project Leader, Business Adaptation &
Interoperation, National ICT Australia

Mr Peter McKenna
Director, Queensland Office
for Regulatory Efficiency
Queensland Treasury

Mr John Morrissey
e-Research, Information Management
& Technology, CSIRO

Mr Alan Noble
Engineering Director
Google Australia & NewZealand

Ms Sabeena Oberoi
Assistant Secretary, Cyber Security
Department of Broadcasting,
Communications & the Digital Economy

Mr Andrew Solomon
Policy Director
Office of the Australian Information
Commissioner

Dr Matthew Sorell
Director, Convergent
Communications Research Group
Lecturer, School of Electrical
& Electronic Engineering
University of Adelaide

Mr Greg Stone
Chief Technical Officer
Microsoft Australia

Dr Darrell Williamson
Director, e-Research
Information Management
& Technology, CSIRO