ACS Cloud Protocol Consultation
Report on the outcomes of the ACS public consultation on Cloud Protocol

11 November 2013
## Contents

1. Executive Summary  
2. Background  
3. Consultations  
4. Written Responses  
5. Cloud in other Jurisdictions  
6. Conclusion  
7. Appendices  
   - Submissions received  
   - List of organisations who attended public consultation workshops  
   - ACS Public Consultation Discussion Paper
1. **EXECUTIVE SUMMARY**

In 2012 the National Standing Committee for Cloud Computing (NSCCC) recommended to the then Government that the industry develop a voluntary Cloud Protocol as a means of helping ensure potential consumers of cloud services are well informed about cloud products and services. The Protocol was seen as an effective means to help drive adoption of cloud services, particularly amongst SMEs and NFPs, by addressing a recognised uncertainty about cloud technologies. The then Government accepted this advice, included it as an action in its National Cloud Computing Strategy released in May 2013, and asked the ACS to conduct a consultation process to help develop the proposed Protocol. So between July and September 2013 the ACS conducted an extensive consultation process, receiving 23 written submissions and conducting Workshops involving more than 400 attendees across four capital cities.

The key conclusions from the consultation process are as follows;

1. The major global cloud suppliers, peak industry bodies and telecommunications providers who participated in the consultation process do not support a Protocol requiring a “sign-up” process, and including vetting of disclosures and a regulated complaints process. Their principle arguments against the Protocol are that there is no clear evidence that a lack of confidence in providers is the issue holding back the market, and any Protocol would duplicate already robust and effective regulatory protections and complaints mechanisms such as the ACL, ACCC, ACMA and the TCP.

2. On the demand side, the Australian Industry Group, which represents many thousands of small businesses, is similarly not supportive of a Protocol. It argues that there is no clear evidence that the problem a Protocol seeks to address actually exists in any material way, and that there are more effective measures which can be taken to drive adoption of cloud services amongst SMEs and NFPs.

3. Stakeholders who supported the concept of a Protocol, principally the consumer groups, argued that a mandatory regulatory process or mandatory protocol is necessary because a voluntary self-regulation will not be effective.

4. There was widespread support across all stakeholder groups for an education and awareness campaign directed at the target market to:
• define what cloud services are
• outline the potential benefits
• identify existing consumer protection measures
• provide users with information about cloud benefits and risks and,
• suggest key questions that should be directed at potential suppliers during the procurement process.

The advocacy for such a campaign reflects a widely held view that the largest problems for potential cloud consumers in the SME and NFP sectors are that they suffer from knowledge gaps, and they lack the time and resources to gather the information they need to address any contractual or poor performance issues with suppliers.

5. Further reinforcing the need for education and awareness raising is a recognition that the legislative and other consumer protections currently in place generally come into play to assist consumers after loss or perceived damage is suffered. They do not provide guidance or information pre purchase of the service about set-up mechanisms, cloud benefits and risks, costs and how to choose between suppliers.

Based on the findings of this consultation process therefore a Voluntary Cloud Protocol is not immediately viable. A Voluntary Protocol can only be effective if a high percentage of the suppliers by market share sign up to it. Whilst a Voluntary Protocol will be potentially attractive to smaller providers who could see it as a way to gain some marketing advantage, without the major suppliers on board a Protocol would be ineffective and potentially do no more than create confusion in a market where there are already a number of regulatory and consumer protection mechanisms in place.

However, whilst the ACS consultation process found no support amongst participating vendors or their representative bodies for a Voluntary Protocol, it is important to note that there are a number of cloud providers who did not participate in the consultation process. A notable example is Amazon. Therefore we cannot claim to know the views of the entire vendor industry on the value and merits of a Protocol. All we can do here is accurately reflect the views of those organisations that did contribute to the process. Were a major cloud provider to form the view, in the future, that a protocol was useful then this position could rapidly change.
Other arguments made during the consultation process against the establishment of a Protocol were:

- New Zealand, where a Cloud Code has just been launched and which prompted NSCCC consideration of a Code or Protocol in Australia, does not have the same economy-wide consumer and privacy legislation and regulations as Australia and as such does not provide the same level of buyer protections that exist in Australia. Hence while a Code or Protocol might be right for New Zealand it does not mean it is necessarily right or required in Australia at this early stage.
- Establishing a Protocol before the proposed regulatory stock-take announced in the Cloud Strategy is undertaken and before the proposed cloud working group is established would be putting the cart before the horse.
- Cloud is evolving so rapidly any Protocol would need constant review and change to remain relevant. And if it did not remain relevant and current, it would potentially stifle innovation and the delivery of new cloud products and services to consumers.
- A protocol for cloud and no other IT services and platforms potentially sends a signal to the market that cloud is a relatively more risky product than other storage-management systems. This would be at misleading and damaging to the industry.
- It would be prudent to observe the NZ Cloud Code experience and outcomes over the next 6-12 months before we consider doing anything similar in Australia. If there were to ultimately be a Cloud Protocol in Australia, it would be wise to do so taking into account the undoubted learnings that will come from the New Zealand experience.

Based on the consultation process findings therefore, the ACS suggests that rather than immediately introduce a Protocol, the strategy should be to focus initially on an extensive education and awareness campaign, monitor and review the impact of that campaign over the following 12 months and then, based on the outcomes of the campaign, determine whether further initiatives need to be taken to help address perceived market failures. It would also be useful to regularly review this position, particularly if one or more of the large cloud providers were to indicate support for a voluntary protocol.

Specifically ACS recommends;

1. A comprehensive education and awareness campaign be conducted through a
combination of

a. leveraging existing government programs such as Digital Business Kits and Enterprise Connect and using tools such as online tutorials, published materials, media campaigns etc.

b. a grass roots campaign through a program of national, targeted Workshops done in conjunction with industry groups such as Ai Group, AIIA, COSBOA, Our Community, Chambers of Commerce and local Councils and Regional Development Agencies who have deep knowledge of their local businesses and industry sectors.

2. The NSCCC regularly review the need for a protocol in the light of changing circumstances.

3. Establish a process and methodology for monitoring SME and NFP uptake of cloud and for identifying perceived risks and barriers. This could be done for example in collaboration with groups such as Ai Group, MYOB, Digital Business Insights etc.

4. NSCCC review the need for any further initiatives in 12 months once the campaign has been rolled out and outcomes measured as per (3) above are available.

5. The Federal Government assist with funding and other relevant support needed to implement the above initiatives.

2. BACKGROUND

In 2012 the NSCCC recommended to the then Government that the industry develop a voluntary Cloud Protocol as a means of helping ensure potential consumers of cloud services are well informed about cloud products and services. The Protocol was seen as an effective means to help drive take up of cloud services, particularly amongst SMEs and NFPs. As part of the NSCCC recommendation, ACS indicated it would undertake and manage stakeholder consultation about the Protocol.

The then Government accepted this advice and included it in its Cloud Strategy released in May 2013. The Strategy aims to:

i) Maximise the value of cloud computing in government;
ii) Promote cloud computing to small business, not-for-profit and consumers, and

iii) Support a vibrant cloud services sector.

In relation to ii) above, the Strategy states:

“The Australian Computer Society will co-ordinate with the National Standing Committee on Cloud Computing (NSCCC), the Australian Information Industry Association and other government and industry stakeholders to develop a voluntary Cloud Consumer Protocol to encourage information disclosure by cloud providers and support consumers of cloud services in being well informed. DBCDE and OAIC will publish guidance for the cloud services industry about the new privacy reforms that are due to commence in March 2014.” (page 5)

It goes on to note:

“Given that economy-wide protections are already in place and that the cloud services industry is still an emerging delivery platform, the government considers that sector-specific regulation is not currently warranted. Self-regulation in the cloud services sector is an opportunity for key players in the cloud industry to promote their own efficiency and growth, while taking responsibility to ensure consumers are treated fairly, receive clear information and have adequate safeguards.” (Page 21)

Throughout the consultation process that followed, the ACS and Government representatives emphasised that if there was to be a Protocol applying to cloud suppliers, it would need to be:

- Voluntary and
- Industry led and supported.

This view was underpinned by the acknowledgement that sector-specific regulation is not seen as necessary because there is no identified market failure and that whole-of-economy protections were already in place. Government and ACS representatives who spoke at all consultation Workshops pointed out that existing legislative and governance frameworks such as the Australian Consumer Law, new Privacy Principles due in March 2014, the ACCC and ACMA processes, the Corporations Act, Telecommunications Acts and intercept powers provide strong protection for cloud users.
The ACS consultation process commenced with a comprehensive Discussion Paper canvassing the various options and approaches to cloud management and regulation, seeking input from respondents about a Protocol, the type and range of issues to be covered by such a Protocol, and any learnings that could be ascertained from the then nascent New Zealand Cloud Code, which has since been launched.

The ACS Discussion Paper was advertised on social media, through print media and via membership organisations such as AIIA, Ai Group, ACCAN, and AIMIA etc. ACS also conducted fully-funded and hosted workshops for all interested stakeholders in Melbourne, Sydney, Brisbane and Canberra. Senior representatives from the then Department of Broadband, Communications and the Digital Economy (DBCDE) attended each workshop and spoke about the background to the consultation process. They were supported by an ACS Cloud specialist and staff. ACS also met with peak body representatives and industry members to discuss the merits of a cloud protocol.

More than 400 stakeholders attended the workshops and ACS received 23 written responses to the Paper. Commentary was also provided through various online media outlets. Workshop attendees included representatives from industry, the ACS, numerous peak bodies, state and federal government departments and agencies, the banking industry, academia, media and the consulting sector.

A full list of these is provided in the Appendices to this report and all submissions received are available at: http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol

3. CONSULTATIONS
This section of the Report sets out the principal messages and verbatim comments received by ACS during the consultation process, including brief summaries of written responses to the Discussion Paper.

Melbourne

The Melbourne Workshop was the first in the series of stakeholder consultations and took place on 19 August 2013, shortly after the Discussion Paper had been released. In excess of
140 people attended the workshop, mainly ACS members, a small number of cloud suppliers and consultants, Ai Group and ACMA representatives. The then DBCDE provided a senior official to speak at the workshop. ACS provided a facilitator for the workshop.

Introductory themes from DBCDE and ACS emphasised that this process was aimed at ascertaining the need for a voluntary, industry-led and supported Protocol to instil confidence in cloud consumers, clarity in cloud implementation and security transparency. It was noted that current consumer protection in Australia is robust; the ACL, telecommunications legislation, privacy guidelines and intercept laws are among world best practice. Comments at the Workshop indicated either ignorance or confusion about how cloud works, what questions users need to ask, how users can educate themselves about cloud, and the apparent lack of ‘bargaining power’ small consumers have in cases where cloud is generally supplied by large multinationals. Verbatim comments included:

- Any protocol must be kept simple
- Use acceptance testing to an agreed standard is required for cloud
- Can resellers (third party cloud suppliers) be subject to the ACL?
- Any code must be mandatory – voluntary is a toothless tiger
- Mandatory regulation will stifle cloud innovation
- SMEs are time poor and ICT ignorant so understanding cloud is difficult for them
- Most cloud contracts adopt a take-it-or-leave-it approach to consumers
- Costs can be very high – better to use on-premise computing?
- Off-premise computing can put ACS members out of a job
- Cloud depends on a good NBN

**Sydney**

The Sydney Workshop took place on 30 August 2013 and was attended by DBCDE representatives as well as approximately 100 representatives from a mix of the ACS, cloud suppliers, telecommunications providers, media, lawyers and academia. The ACS provided a facilitator.

Suppliers who attended indicated they were not seeing any reluctance in the current market to adopt cloud or seek out information on cloud benefits. Several indicated they did not see
any market failure or any obvious need for a Protocol. Education of users was regarded by
some as the key to dealing with any apparent reluctance to take up cloud services.

Suggestions were made for standard contracts in the cloud space, and several attendees noted
that vendor lock-in was a genuine issue, although no evidence or case studies were provided
to support this claim. Attendees queried how any code or Protocol would be maintained and
kept up to date, given that industry did not favour such a Protocol and peak bodies would not
assume the task of its management.

Attendees suggested a list of key questions on a central website would help SMEs understand
how to approach cloud suppliers and what data to seek.

Verbatim comments included:

- Defining cloud is increasingly difficult as it takes in almost everything on the internet
- It is in the interests of cloud suppliers to take consumer concerns seriously
- Subcontractors in the supply chain are an issue
- Perhaps an initial approach is to look at Cloud Security Alliance and map the Australian
  concerns to the questions posed in that platform
- Consumers must undertake due diligence themselves
- De-risk SME decision-making by identifying the type of information SMEs must have to
  address cloud as part of their business
- Consumers must be able to compare like with like in assessing cloud suppliers and this
  is not possible in the current market
- There may be tax withholding issues connected with cloud use
- The NZ Cloud Code is a good start but it cannot be simply copied here

Brisbane

This Workshop was held on 4 September 2013. The ACS provided a facilitator. More than 80
people attended, mainly ACS members, cloud suppliers and academics. DBCDE provided a
departmental representative to introduce the consultation process and provide background.

As with the Melbourne Workshop, few attendees had read the Discussion Paper. It was
therefore necessary to lead attendees through the questions from the Paper and to elicit more
targeted input rather than discursive discussion.
Input focussed on the difficulty of dealing with cloud failures and outages, which severely impact SME businesses, but for which suppliers do not allow access to audits or reasons for the outage. Other concerns centred on resellers of cloud and how current legislation such as the ACL deal with third party suppliers. Some attendees agreed the current market situation is no different from any other and that ‘caveat emptor ‘must always apply; users are responsible, in this as in all other market interactions, for educating themselves. A recurrent theme was the need to understand where suppliers store data, with the attendant assumption that all offshore data was somehow less secure than if held in Australia. Those familiar with the NZ Cloud Code did not feel it provided good assurance because it is limited to IaaS and current cloud offerings are more complicated than this.

Verbatim comments included:

- Gold, silver and bronze cloud service levels will assist SMEs
- Third factor certification is required to secure cloud platforms
- Vendors must be required to disclose where they store user data
- A cloud Ombudsman will assist SMEs to deal with cloud suppliers’ contracts
- Consumer education is the solution
- Mandatory notification of security breaches by suppliers must be required

Canberra

The final Workshop was held on 5 September 2013. ACS provided a facilitator. The great majority of the 50+ attendees were from federal government agencies, attending as ACS members. In addition, representatives from AIIA and Telstra attended, as well as some SMEs and local academics.

Interestingly, attendees from Government agencies indicated that advice and guidance available from other agencies such as AGIMO and DSD sent confusing messages and “said different things”, so agencies are reluctant to approach cloud uptake because of the real risk of failure, and no appropriate guidance. Several expressed the view that a Protocol will not address the issues faced by individuals such as privacy concerns and failure by the supplier.

Industry representatives expressed strong views that there is no current lag in SME uptake of cloud. On the contrary they believe it to be a vibrant market. In addition, the evidence and research noted in the ACS Discussion paper and by ACMA and DBCDE was said to be “highly variable” and not consistent with broader research samples quoted by the suppliers.
Suggestions that cloud computing needs regulation or even just a Protocol sends messages to the market that cloud is unsafe, and different from any other ICT storage platform; in many situations cloud can provide better security and safety than traditional storage systems.

Verbatim comments included:

- Policy should not single out cloud as less safe than other services, nor should it indicate that data stored offshore is at risk
- Hybrid clouds need to be explained better
- Do not build a unique Australian Protocol
- Cloud here must be the same as the US and Europe
- Suppliers can go out of business in any market sector and a Protocol will not address this type of concern
- Users need more information about disaster recovery techniques
- Protocols or codes will only indicate that those who sign up are ‘good’ and others are ‘bad’ and this may not be true

4. WRITTEN RESPONSES

ACS received 23 written responses to the Discussion Paper to the closing date of 10 September. These have been uploaded to the ACS website and provided to Department officials.

As expected, responses ranged from suggestions for a mandatory Code with compliance provisions and regular audit functions, to allowing suppliers to continue educating consumers with proprietary guidelines, SLA’s, contracts and marketing activities. In addition, industry bodies believed there is now sufficient consumer protection and corporate governance measures in Australia (unlike New Zealand) and that the regulatory stock take mentioned in the National Cloud Computing Strategy must be completed before any policy decision is taken on the need or otherwise for a Protocol.

Government agencies and local councils indicated they were required to move towards cloud in any case but would appreciate more and better guidance on how to compare supplier offerings and how to avoid vendor lock-in.

Cloud vendors who responded to the Discussion Paper indicated they would not support a Protocol nor sign up to a Protocol. At most, a clear set of principles or guidelines would be
acceptable but only to the extent that such guidelines provide cloud information on issues such as data ownership, breach notification and offshore storage. Many noted that their cloud revenues are increasing annually as are cloud customer bases. Many users who state they do not trust cloud are using it without actually knowing that - e.g. as emails, websites, applications etc.

The mechanics of a Protocol were also questioned; using the NZ template, any supplier found not to be complying with their own disclosure only has to amend that disclosure, not the original cloud “problem.” In addition, the cost and resources required to establish, maintain and enforce a Protocol were queried. Industry bodies unanimously indicated they would not be responsible for such a management task.

Several suggestions were made to investigate the adoption of the Cloud Security Alliance system and STAR registry (see below). Larger users such as banks noted that interoperability, acceptable global standards and lack of a robust NBN continue to be the higher level business and enterprise issues impacting adoption of cloud. They also pointed to issues with third party suppliers who do not meet service continuity requirements of large users.

Potential users of cloud noted that as SMEs, they do not have the time or money to educate themselves about ICT generally, and cloud computing in particular. This lack of information to support an informed choice and facilitate de-risked decision-making on investments seems to be at the heart of SME concerns.

5. CLOUD IN OTHER JURISDICTIONS

New Zealand

The NZ Cloud Code is a voluntary disclosure-based Code of Practice that has been developed to improve the standard of services being provided by Cloud Service Providers. It also provides Cloud Service Consumers with the ability to view and compare disclosure statements from Cloud Service Providers and make informed choices when considering a Cloud Service Provider. There are two core commitments that all Signatories to the Cloud Code make and a set of Disclosures that are at its core:

A. Signatories won't say something is "Cloud Computing" unless it really is.

For the purpose of the Cloud Code, Cloud Computing is defined as:
“On-demand scalable resources such as networks, servers and applications which are provided as a service, are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider interaction.”

B. Signatories will disclose important details about their Cloud products and services.

The Cloud Code document outlines these disclosures in detail, to ensure all Cloud Code signatories meet the same obligations. Disclosures are in the following categories:

- Corporate Identity
- Ownership of Information
- Security
- Data
- Data Access and Use
- Backup and Maintenance
- Geographic Diversity
- SLA and Support
- Data Transportability
- Business Continuity
- Data Formats
- Ownership of Application
- Customer Engagement Data
- Breaches
- Law Enforcement

The NZ Code provides a complaint mechanism based on users registering their complaints about disclosure issues with the industry body’s review team.

To date there are fourteen local suppliers being “processed” and six cloud suppliers have now signed the Code. They are:

- HD.net.nz
- Webdrive
- OneNet
- Mega
- Xero
- Equinox
United States Cloud Security Alliance

The Cloud Security Alliance (CSA) is a US-based member-driven organisation aimed at promoting the use of best practices for providing security assurance within Cloud Computing, and providing education on the uses of Cloud Computing to help secure all other forms of computing. It currently has 140 corporate members including all major cloud providers. CSA has an active Asia Pacific arm and an Australian Chapter managed through a closed LinkedIn Group. CSA maintains a registry known as STAR (security, trust assurance register), which members can certify to and become publicly registered. STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.

See more detail at: https://cloudsecurityalliance.org/

Recently, CSA and British Standards Institution launched a technology-neutral certification they claim provides an additional layer of transparency around security controls used by cloud service providers. Under the STAR Certification program, service providers will be able to give prospective users a greater understanding of their levels of security controls.

The new certification is based on achieving ISO/IEC 27001 and the criteria outlined in the Cloud Controls Matrix, a set of criteria that measures the capability levels of a cloud service. There are 11 control points in this matrix including compliance, data governance, facility security, human resources, information security, legal, operations management, risk management, release management, resiliency and security architecture. An independent assessment by an accredited body will assign a ‘management capability score’ to each of the 11 control points and each control is scored on a specific maturity and will be measured against five management principles.

This development may be worth monitoring to ascertain its use in an Australian context.

Europe

The recent establishment of the European Cloud Partnership (ECP) brings industry and government together with the aim of boosting cloud adoption in Europe pursuant to the European Cloud Strategy. The Steering Group for the ECP released its goals for 2013-2014 including the following statement:
“A central aim of the ECP is to stimulate the migration of public IT use to the cloud (and as a result, further stimulate private procurement especially among SMEs). It is important to stimulate both infrastructure and service provision, in areas that can drive internal IT transformation and efficiency as well as benefits to citizens. We aim at an ambitious target by 2015, comparable to the US benchmark of 25% of federal IT spending as potential migration to cloud computing. To help this, the steering board will:

- undertake public awareness actions to forge a link in the public mind between public service performance and cloud take-up and raising awareness of the different types of cloud services; work to make cloud readiness and adoption a political priority;
- promote the development of common user requirements in the public sector, and catalogue and promote use cases of cloud computing adoption in the public sector; map out practical solutions to barriers to cloud computing adoption in the public sector whilst dispelling imaginary ones.

These initial priorities will be developed into a road map for moving Europe into the cloud quickly and safely. The main beneficiaries of our actions will be European citizens, small and medium sized enterprises and national, regional and local authorities. Other stakeholders (network operators, data centre / cloud infrastructure providers, service providers, small and large software companies) will also benefit from the creation of a vibrant and self-sustaining ecosystem.”

However, EU members are now agitating for tighter cloud regulation since the revelations surrounding the Snowden affair and the new knowledge that the US Government has been accessing European sovereign national data. Whether the ECP will continue in this environment is unclear.

6. CONCLUSION

Based on the evidence presented to the ACS consultation process, there is no vendor industry support for a Protocol that adds cost, requires a “sign-up” mechanism, and requires complaints management processes and/or audits. Without majority industry support for
voluntary self-regulation, such an initiative would be ineffective and certainly not achieve the stated objective of supporting consumers of cloud services in being well informed. The ACS notes however that not all cloud suppliers participated or were represented in the consultation process, including for example a large global provider such as Amazon. Therefore we cannot claim to know the views of the entire vendor industry on the value and merits of a Protocol. All we can do here then is accurately reflect the views of those organisations that did contribute to the process.

Privacy advocates and certain consumer groups argued for mandatory regulation of cloud service providers based ostensibly on fears of supplier failure, access to personal data by foreign governments, vendor lock-in etc. The counter by the industry is that most if not all such concerns are adequately addressed through the extent of Australian privacy protection, corporation governance laws, Australian Consumer Law and other existing regulation applying to cloud suppliers.

The consultation process did reveal widespread support for an education and awareness campaign to support consumers in their efforts to understand more about cloud benefits and risks. ACS see this as the logical next step in building a wider and deeper understanding of potential benefits of cloud services in the SME and NFP sectors. This in turn should lead to greater confidence in, and take up of, such services.

An education and awareness campaign should include advice on current global ‘standards’ such as CSA STAR, as well as domestic regulations such as the ACL, new Privacy Principles, Corporations legislation, etc.

The campaign should also include dissemination of guidelines that identify the key issues that potential users should be raising with their suppliers or potential suppliers. ACS recommends that as minimum, the key issues should include:

**Transparency:** Companies that provide cloud computing platforms should be asked to explain their information handling practices and disclose the performance and reliability of their services, including having this information on their web sites.

**Use Limitation:** Companies that provide cloud computing platforms should claim no ownership rights in customer data and should use customer data only as their customers instruct them, or
to fulfil their contractual or legal obligations.

**Disclosure:** Companies that provide cloud computing platforms should disclose customer data only if required to do so by the customer or by law, and should provide affected customers with prior notice of any legally compelled disclosure to the extent permissible by law.

**Security Management System:** Companies that provide cloud computing platforms should maintain a robust security management system that is based on an internationally accepted security framework (such as ISO 27002) to protect customer data.

**Customer Security Features:** Companies that provide cloud computing platforms should provide their customers with a selection of security features to implement in their usage of the cloud computing services.

**Data Location:** Companies that provide cloud computing platforms should make available to their customers a list of countries in which their customer data related to them is hosted.

**Breach Notification:** Companies that provide cloud computing platforms should notify customers of known security breaches that affect the confidentiality or integrity of their customer data promptly.

**Audit:** Companies that provide cloud computing platforms should use third-party auditors to ensure compliance with their security management system and with these principles.

**Data Portability:** Companies that provide cloud computing platforms should make available to customers their respective customer data in an industry-standard, downloadable format.

**Accountability:** Companies that provide cloud computing platforms should work with their customers to designate appropriate roles for privacy and security accountability.

Finally, ACS recommends a process and methodology be established for monitoring SME and NFP uptake of cloud and for identifying perceived risks and barriers. The findings which emerge from this monitoring process should then be reviewed after 12 months by NSCCC or some other appropriate body to determine whether further initiatives need to be considered.
APPENDICES

SUBMISSIONS RECEIVED

Written submissions were received from;

AARNet
AIIA
Australian Communications Consumer Action Network
Australian Industry Group
Australian Privacy Foundation
Barry Simpson CCA CIO - Individual Submission
Brereton Consulting
Communications Alliance Ltd
Damien Pedersen
Four Quarters Computing
Google
Holly Raiche - Individual Submission
Bill Caelli - Individual Submission Part 1, Part 2
Information Integrity Solutions Pty Ltd
Logan City Council
Microsoft
National Australia Bank Limited
OCIO Government SA
OzHub
PCR Law & Associates
QSR International Pty Ltd
Telstra
Xamax Consultancy Pty Ltd
ORGANISATIONS WHO ATTENDED PUBLIC CONSULTATION WORKSHOPS

Over 400 individuals attended workshops in Melbourne, Sydney, Canberra and Brisbane. The organisations represented were as follows;

Accenture
Affinity Vision Australia Pty Ltd
Airservices Australia
Apex Academic Technologies
ArgyStar.com
AstraCloud computing services
Australia Post
Australian Communications and Media Authority
Australian Computer Society
Australian Providers of Cloud
Australian Tax Office
Bennett & Philp
Brereton Consulting
British Aerospace Australia Pty Ltd
C3 Business Solutions
Callida Consulting
CDAS
CeniTex
Chairman, ACS Victoria
ChannelAdvisor
Chisholm Consulting Group Pty Ltd
Cisco Systems Australia Pty Ltd
CITEC
Commonwealth Bank Of Australia
Consult Point
CQU
Crimtrac
Deloitte
Deonvale Consulting Services
Department of Defence
Department of Finance & De-Regulation
Department of Human Services
Department of Immigration and Citizenship
Department of Industry, Innovation, Climate Change, Research and Tertiary Education
VIC Department of State Development, Business and Innovation
Developing Computer Solutions
Dialog Information Technology
Dimension Data
DWS Limited
Dynamic Investment Partners
eCorner
enotia
ENT Consulting
Enterprise Connect (Fed)
Enterprise Connect Qld
Ernst & Young
Family Planning Qld
FE Technologies
Fine Music 102.5
Four Quarters Computing
Frame
Fujitsu Australia
Geoscience Australia
GHD
Global Speech Networks Limited
Hewlett Packard
HP
IBM Australia
Infosec Services
Inventosystems pty Ltd
itSMF Australia Inc
kbConsulting
KBR
Leadership Management Australia
Leica Microsystems
Leopard Systems
Melbourne University
Mentat Solutions
Microsoft
NAB
National Science and Technology Centre
Oracle Corporation
Orion VM
Performance Education
Project Acumen Pty Ltd
Project Focus
Public Records Office Victoria
QFAB
QGCIO
Qodo
Queensland Rail
Queensland University of Technology
Regis Group
Seedready Inc.
Shell IT International
Skilled Testing Pty Ltd
SKM
Smart Idea
Softetspays Pty Ltd
Spotless
Stralion Pty Ltd
Sydney College of Business and IT
TAFE NSI Students
Tata Consultancy Services
Technology One
Telstra
The Frame Group
The Optimise Group Pty Ltd
The University of Ballarat
The University of Queensland
Transport Ticketing Authority
UnitingCare QLD
UXCC
VENTYX
VicRoads
Victoria University
Victorian Department of Education & Early Childhood Development
VIT Australia
William Buck
The ACS discussion paper was promoted via public notices, media and social media, to 22,000+ ACS members working in ICT, and directly to vendors and industry.


1. Introduction and Purpose

This Discussion Paper (the Paper) aims to elicit suggestions and information from cloud computing vendors and from users of cloud computing services – particularly small businesses, not-for-profits (NFPs) and consumers about the tools and protections they need to acquire and deploy cloud computing services in their businesses with confidence and trust. Government agency input, both Commonwealth and State and Territory, is also welcome.

The Government recently announced a National Cloud Computing Strategy, which includes an action to develop a voluntary cloud computing consumer protocol (the Protocol). The development of the Protocol is to be coordinated by the Australian Computer Society (ACS).


This Protocol will provide prospective and current users of cloud services with information about cloud computing together with undertakings from cloud suppliers who sign up to the Protocol about data ownership, security and a number of other matters. The proposed Protocol is intended to be in operation by January 2014.

2. Structure and Timelines

This Paper:

- provides a simple definition of cloud computing and its benefits;
- highlights what ACS sees as the top-level issues of concern to both cloud suppliers and cloud users;
- poses specific questions for respondents to answer; and,
- attaches the New Zealand CloudCode (July 2013) for review, comment and comparison.

In order to meet Government timelines, responses to this Paper are due by COB Thursday 5 September 2013. Based on feedback from these responses, a revised discussion paper and Draft Protocol will then be released for further consultation, including face-to-face discussion sessions in certain capital cities, commencing in August/September 2013. Revisions and amendments to the Protocol will then be made with a view to having a final Protocol and supporting administrative arrangements agreed to before the end of 2013.

Please send your responses and comments on this paper by 5 September to:

All submissions will be made available to the public on the ACS web site unless you indicate you would like all or part of your submission to remain confidential.

Enquiries should be directed to:

Ms Loretta Johnson, Principal, LJ Associates, on 0427/790574 or at lodestar@ozemail.com.au

OR

Adam Redman, ACS Head of Policy and External Affairs on +61 2 8296 4450 or at policy@acs.org.au

---

Question 1. Do you believe a voluntary protocol in which cloud suppliers provide undertakings and information about their services would improve confidence in the market and increase the adoption and take-up of cloud computing services?

3. Executive Summary

Despite the clear and compelling value of the cloud, SMEs and NFPs in particular appear reticent to integrate the cloud into their businesses and operations. The evidence suggests that this is due to a combination of a lack of understanding of what the cloud actually is, and secondly a lack of confidence in using cloud services due to concerns around issues such as privacy and security. The oft-cited MYOB 2012 vendor study into cloud adoption noted that four in five Australian SMEs are not interested in integrating the cloud into their business due to a lack of understanding about it as well as security and safety concerns. As the Government’s recent Cloud Strategy notes, “it is small organisations which stand to benefit the most from the cloud revolution. Cloud computing will fundamentally change the ability of small organisations to acquire new ICT capabilities that can increase productivity and foster innovation.” So any reluctance on the part of SMEs to embrace this new way of delivering online services will place them at a severe competitive disadvantage in the market, both globally and domestically.

This Paper explores possible reasons for the reluctance or hesitancy to adopt cloud computing with a view to identifying what needs to be addressed in a voluntary cloud protocol to support one of the goals of the Government’s National Cloud Computing Strategy, which is:

“Australian small businesses, not-for-profit organisations and consumers will have the protection and tools they need to acquire cloud services with confidence.”

---

3 www.dbcde.gov.au page 20
The Paper also recognises that engagement with government, industry, the community and consumers is required to develop confidence in the marketing, brokerage, provision and consumption of commercial cloud services in Australia.

In coordinating the development of the Protocol, ACS supports the Government’s recognition that cloud computing presents some significant challenges which cloud suppliers and users, together with Governments, must address collaboratively. The issues include, but are not limited to, security, privacy, accessibility, competition, exclusion, jurisdiction and assurance.

The ACS also shares the Government’s view that in order for the full benefits of the cloud to be realised and thereby assist Australia fully grasp the opportunities of the digital economy, a voluntary/self-regulatory regime working together with the key whole-of-economy regulatory and legislative arrangements, represents the “first best” option to provide users with the basic safeguards they need. As the cloud becomes more sophisticated and ubiquitous, at the core of any proposed Protocol is a requirement to provide consumers with clear and straightforward guidance on what to expect as a minimum level of service from providers, marketers, brokers or resellers without adding unnecessary regulatory burdens to either the cloud supplier or the consumer. Similarly, and importantly, the Protocol should guard against excluding market entry, limiting competition or stifling innovation. It may also be that a protocol can help the market by increasing consumer confidence and addressing industry’s preference for regulatory certainty when making investment decisions.

Globally, cloud suppliers are also co-operating in security assurance and best practice activities. The Cloud Security Alliance (CSA) is a not-for-profit organisation with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The CSA is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. Most international cloud suppliers are members of CSA. Locally, the Telecommunications Consumer Protections Code (TCP) has been implemented in Australia pursuant to specific powers under the Telecommunications Act 1997. It is registered by the ACMA but will not apply to all cloud suppliers in Australia unless they fall within the purview of the Act’s definitions of carriage service suppliers.

The ACS view is that any cloud protocol for Australia must avoid further regulatory complexity, jurisdictional variation, anti-competitive outcomes and overly prescriptive disclosure requirements. In short, ACS agrees with the Government’s Cloud Strategy and its aims for a Protocol, namely:

- Adequate protection for consumers of cloud services
- Clear and relevant information about products and services before, during and after point of sale for consumers
• Open, honest and fair dealings between cloud service providers and consumers
• Adequate privacy protection
• Responsiveness to market and technology developments.  

It is critical to recall however, that some of these aims can be met through the application of current legislative protections.

4. What is Cloud Computing? 

Cloud computing is a general term for the delivery of hosted services over the internet, enabling users to remotely store, process and share digital information and data. As such it is more a new way of delivering technology services rather than a new technology itself. There are three main categories of cloud, although the distinctions between them are becoming more permeable as their sophistication grows. They are:

1. Infrastructure as a Service (IaaS) offers data centre capacity, processing and storage. An example is Amazon web services.
2. Platform as a Service (PaaS) provides an environment for the hosting of applications. An example is Salesforce’s online hosting services and content delivery services.
3. Software as a Service (SaaS) examples include Hotmail and Flickr.

There are other more detailed definitions available for the cloud. The ACS refers to the Australian Government definition of Cloud computing, itself taken from the US Government’s National Institute of Standards and Technology (NIST) definition. It comprises five elements or characteristics of the cloud:

• on demand self-service,
• broad network access,
• resource pooling,
• rapid elasticity and
• measured service. 

The proposed Protocol will focus on public and hybrid cloud services across infrastructure, platform and software (see above), as these are currently the services most available to consumers, SMEs and NFPs. Community and private clouds are more granular and customisable types of contractual service level agreements, which have generally higher levels of awareness and enthusiasm among their consumers. But a protocol might also be adopted by private cloud providers as a voluntary best practice standard.

---

4 ibid. Page 22
5 See ACMA The cloud- services, computing and digital data, Emerging issues in media and communications, Occasional paper 3, June 2013 Page 4ff.
6 www.nist.gov/itl/csd/cloud0102511.cfm
5. The Benefits of Cloud for SMEs

Cloud computing provides cost and efficiency benefits because its service delivery features are:

- Scalable and elastic – users can tailor the services to meet user demand and the size of the processing task undertaken;
- Platform agnostic – users can access services across multiple devices and operating systems. Almost any internet enabled device, including smart phones, will provide multi-location access to data when cloud computing is adopted;
- Free of fixed costs – ongoing licence fees and equipment purchase costs are eliminated because users pay-as-they-go for services. This permits greater economy of scale for smaller organisations.

The following benefits summary indicates how users can increase their productivity and decrease costs using cloud.7

<table>
<thead>
<tr>
<th>BENEFIT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Savings</td>
<td>SMEs can make immediate cost savings of between 25 and 50 per cent by simply shifting basic services such as email and data storage into the cloud</td>
</tr>
<tr>
<td>Productivity</td>
<td>Cloud services use subscription-pricing models that outsource support and maintenance to providers that have greater resources and expertise. This allows small business to free up resources and focus on core business.</td>
</tr>
<tr>
<td>Lower time to market, increased scalability</td>
<td>Smart adoption of cloud services reduces time to market for new products and services and allows almost limitless scalability for almost no marginal cost. In the face of global competition and the opportunities of the Asian Century, reducing time to market will be a key competitive edge for Australian small businesses.</td>
</tr>
<tr>
<td>Overcome barriers to capital and expertise</td>
<td>Cloud computing can help overcome the traditional barriers SMEs face through limited capital and expertise. In comparison to traditional ICT, cloud services can allow small businesses to acquire new capabilities at only a fraction of the cost.</td>
</tr>
<tr>
<td>Improved reliability and security</td>
<td>Cloud services offer a range of benefits including increased security, access to the latest upgrades, integrated management and backup that may not be available to small organisations that are not ICT focused.</td>
</tr>
<tr>
<td>Mobility, flexibility and a platform for growth</td>
<td>Mobility supports faster decisions and agile business models with a greater potential for growth. Mobility has been identified by 42 per cent of SMEs as a key driver of cloud service adoption. MYOB research in 2012 found businesses that had adopted the cloud were:</td>
</tr>
<tr>
<td></td>
<td>• 53 per cent more likely to have seen a revenue rise in the past year;</td>
</tr>
<tr>
<td></td>
<td>• twice as likely to grow their range of products and services compared to those who had not adopted cloud; and</td>
</tr>
<tr>
<td></td>
<td>• almost three times as likely to increase staff numbers in the coming year.</td>
</tr>
</tbody>
</table>

Question 2a). If you are a potential user of cloud services, do you now have a better understanding of cloud computing and its benefits for your business or operations? What further information do you need to feel confident in deciding to adopt cloud services into your business?

b). If you are a provider of cloud services, is the description above of cloud services and the outline of its benefits accurate and comprehensive for prospective users who may know little of the details of cloud computing?

6. Barriers to Cloud Uptake for SMEs

Recent research by the Australian Communications Management Authority (ACMA) has disclosed that 52 per cent of respondents lack confidence in privacy settings for online service providers. More than two-thirds are concerned about security and unauthorised use of personal information by providers, (see ACMA, Communications Report 2—Australia’s progress in the digital economy: Participation, trust and confidence, 2012). Recent publicity about access by the US government to private consumers’ online information has exacerbated this concern. So it seems clear that to address cloud adoption barriers and ensure appropriate market conduct, the Protocol’s challenge goes beyond educating audiences on productivity enhancing technologies. Cloud users need to have an understanding of the consumer protection and privacy provisions in Australian legislation such as the Australian Consumer Law (ACL), as well as Privacy legislation and the common law of contract. Warranties already exist in the ACL against services that are not fit for purpose, and false or misleading representations of products or services are actionable under the ACL as well as contract law (in some circumstances).

In addition, there are some specific statutory requirements in Australia that mean data must be stored on Australian territory. These include a provision in the Personally Controlled Health Records Act 2012 that health records must be stored locally by a locally registered entity.9

The Protocol will complement existing legislation. It will also recognise current Guidelines issued by the Government which, while aimed at Government agency adoption of cloud, still contain useful guidance for consumers. These include the AGIMO Better Practice Guides,10 and the security outline for cloud users by the Defence Signals Directorate11, which addresses the availability of data and business functionality, protecting data from unauthorised access and handling security incidents. In addition to these resources, the OECD and the European Commission both provide a wealth of information and data about practices for cloud adoption in those economies. Many of these documents are useful for Australia consumers because of the comprehensive analysis they contain.12

---

In the absence of a one-stop-shop resource for consumers, SMEs and NFPs, the Protocol will reference these resources as well as the relevant Australian national legislation and regulations applicable to cloud services.

Domestic protections for consumers are readily available and explicable. But cloud computing service providers are more often than not based internationally and national economy-wide legislation (such as privacy legislation) may not capture providers who are based only in other jurisdictions. That said, recent amendments to the Australian Privacy regime have included a requirement that entities disclosing personal information about an individual to an overseas recipient must take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles. These amendments are due to come into force in March 2014.

Providers resident in foreign jurisdictions will be subject to their own local legislation and this has raised concerns about end users’ abilities to manage access to their private data in accordance with protections available in their home country. ACMA research has shown that 35 per cent of respondents would withhold personal information if the provider’s site were not based on Australian soil. As part of the Government’s ongoing efforts to assist consumers and align regulatory protection environments, addressing this issue is key. Consumers need to understand that redress is still available under Australian legislation against cloud providers operating in Australia even if those providers do not have data centres on Australian soil.

Question 3. If you are a potential or current user of cloud services, do you have other concerns about cloud computing that have not been outlined in this section? What are they?

7. Protocol Disclosures by Cloud Suppliers

The following categories of disclosure and information are suggested for inclusion in a Protocol. Also attached is the recently developed New Zealand CloudCode, which provides, at section 5, a Code of Practice Disclosures expected of cloud suppliers operating in NZ who sign up to the Code. The New Zealand CloudCode is expected to go “live” in mid to late August. For more details go to: www.nzcloudcode.org.nz

Corporate Identity

Cloud providers should disclose - by making available to the consumer and alerting them to the availability of - certain information before, during and after the sales process including company name,

13 ACMA, The cloud - services, computing and digital data, Emerging issues in media and communications Occasional paper 3, June 2013, Page 17
business registration, registered physical and postal address (but not necessarily the address of the
data/operations centre), the company website, telephone number, and which national legal
jurisdiction(s) apply to the company.

Ownership of Data and Information
The ownership of data and information supplied by the client to the service provider needs to be clearly
disclosed, to ensure the rights to use the information are clearly understood. This will help identify who
owns client data, and data generated by the service provision. Providers
should disclose to customers who owns data uploaded to them, processed by them, and any data which
may be generated outside of the commercial agreement by the service provision such as correlative
metadata (e.g. location mapping and statistical information) or data that is provided to a third party in
an arrangement not visible to the consumer such as an upstream provider or a law enforcement agency.

Security
Ensuring that a cloud service provider has in place a good set of standards and practice surrounding
security is important. There are various security standards and platforms currently available and more
are being developed globally. Providers could indicate which of these they are accredited to or comply
with.

Data Location
Cloud Service Providers may host data on a number of servers, located locally or offshore. Knowing
where hosted data is located can help customers assess any risks or benefits for their business. Legal
jurisdictional power over data and information may change depending on the location and the national
security requirements in place. For example, domestic legislation may prohibit some providers from
revealing where sensitive data is located.

Data Access and Use
Knowing how customer data can be accessed both during and after a service has been provided is an
important step to ensuring that, when a service has been ceased, the appropriate provisions are in
place.

Backup and Maintenance
Understanding the backup procedures of the service provider and their maintenance policies allows the
user to make decisions on what further steps they may need to ensure their data is backed up
sufficiently.

Service Level Agreement (SLA) and Support
Cloud Service Providers may offer premium support packages that are additional to their standard
service offering. This section could set out the standard support mechanisms and service level agreements that apply to services.

**Vendor Lock-In**

Consumers are concerned about vendor lock-in and the inability to move between service providers either during or after service provision. Exit strategies for users need to be clearly explained by vendors in this section, and relevant contractual obligations undertaken by consumers when they acquire cloud services should spell out the circumstances under which users may ‘move’ between suppliers.

**Data Portability**

Proprietary standards may limit users’ ability to easily transfer their own data or to access their content via other services. Currently, there is no open standard or technical specification that ensures data portability between data controllers. Data portability is a prerequisite for users of cloud computing services, if they are to have an ongoing choice between providers for a range of services, but the challenge of providing data portability is different with each cloud service type. There are efforts underway, such as open source software tools, to facilitate data portability. At a supra-national level, the EU is considering a proposal for regulation of personal information, including a right to data portability. At present, the lack of interoperable technical standards between cloud computing services means that users may risk losing their content and media if they change services. For both business and consumers, this is an increasingly high barrier as social and professional lives move online.¹⁴

**Business Continuity**

The service provider should disclose what their own business continuity preparations are, which may include an upstream provider’s SLA, redundancy and failover. It should generally be assumed that consumers, SMEs and NFPs accessing cloud services recognise that internet connectivity and power supply can interrupt cloud services and these are generally not the responsibility of the cloud service provider. This could be noted in the protocol.

**Data Formats**

Provider disclosure statements may be offered under this heading with regards to portability and interoperability features that the service provider may offer.

**Data Breaches**

Understanding what will happen when there is a data breach is important. The Privacy Amendments (Privacy Alerts) Bill 2013 was passed by the House of Representatives on 27 June and is before the Senate for its Third Reading when Parliament resumes. This draft legislation imposes on providers a mandatory obligation to notify consumers and relevant authorities of any major data breach. If passed,

¹⁴ ACMA, *The cloud-services, computing and digital data, Emerging issues in media and communications* Occasional paper 3, June 2013, page 17
this Bill should be in place as legislation by March 2014.

Law Enforcement
Cloud users should be made aware how, when and for what purpose the supplier will access their data and if, when the agreement ceases, data access by the provider or a third party (including law enforcement agencies) will occur or not. When requested by appropriate law enforcement agencies to supply customer related information without a warrant or legal mechanism to compel disclosure, providers should advise users of their practice.

Question 4. Are there other disclosures from cloud vendors that have not been outlined in this section? What are they?

Question 5. Can you outline any experiences you have had with cloud computing which illustrate issues such as data security, data location, privacy or vendor lock-in?

Question 6. If you are a provider of cloud services and products, what is the current state of market confidence in cloud computing, and are there any outstanding transparency issues that concern users? If so, what is the best method of addressing these concerns?

Question 7. If a voluntary protocol is introduced, do you have any comments on potential compliance costs, jurisdictional complexities and the interaction between the Protocol and other cloud standards currently being developed globally?

8. Complaints Guidelines & Process
The Protocol is to be a voluntary, industry-supported activity. To help ensure the Protocol is effective however there needs to be a means by which users of cloud services can raise concerns and lodge complaints against service providers who are signatories to the Protocol but who have allegedly made untrue or inaccurate statements in their Disclosure Document.

Importantly, this complaints process would not be intended to cover the following situations:

- Complaints about a service or product;
- Complaints about support, lack of service or issues surrounding restoration of service;
- Complaints about alleged breaches of laws or regulations;
- Issues about payment, pricing or collections of payment for service;
- Complaints about alleged misleading product statements or advertising, other than where the alleged statement does not accord with a cloud supplier’s Protocol Disclosure Document.
Complaints or concerns about the above issues are mainly contractual matters between users and their supplier and would need to be dealt with through other jurisdictions. For example, concerns about advertising, pricing or misleading conduct would in the first instance be raised through the ACCC at www.accc.gov.au/consumers

Key issues we seek comments on are:

- How to make a complaint
- The complaints resolution process
- Possible outcomes of a complaint.

The attached New Zealand CloudCode outlines a complaints process addressing these issues.

*Question 8. Using the New Zealand Code as an example, are there changes or improvements that could be made which would improve the efficacy of that process in an Australian context? Are there other issues not addressed in the New Zealand Code that need to be considered?*