inspiring success

AUSTRALIAN COMPUTER SOCIETY

# Cloud Computing Consumer Protocol

## ACS Cloud Discussion Paper

## July 2013

## CONTENTS

# Cloud Computing Consumer Protocol

## 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[1] - 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).

See full details at; http://www.dbcde.gov.au/digital_economy/cloud_computing

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.

[1] http://accan.org.au/index.php/broadband/broadband-policy-positions/514-position-statement-what-consumers-need-from-cloud-computing

In order to meet Government timelines, responses to this Paper are due by COB Monday 5 August 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 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 19 August to: policy@acs.org.au<mailto:policy@acs.org.au>**

**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[2] noted that four in five Australian SMEs are not interested in integrating the cloud into their business due

2 delimiter.com.au/vmware/myob-australian-smes-pdf

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."[3] 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."*

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

[3] www.dbcde.gov.au page 20

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.[4]

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

[4] ibid. Page 22

## 4. What is Cloud Computing?[5]

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.[6]

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

[5] See ACMA The cloud- services, computing and digital data, *Emerging issues in media and communications* Occasional paper 3, June 2013Page 4ff.
[6] www.nist.gov/itl/csd/cloud0102511.cfm

of awareness and enthusiasm among their consumers. But a protocol might also be adopted by private cloud providers as a voluntary best practice standard.

## 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]

| BENEFIT | DESCRIPTION |
|---|---|
| **Cost Savings** | 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 |
| **Productivity** | 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. |
| **Lower time to market, increased scalability** | 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. |
| **Overcome barriers to capital and expertise** | 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. |

[7] Extract from the National Cloud Computing Strategy, www.dbcde.gov.au. Page 20

| | |
|---|---|
| **Improved reliability and security** | 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. |
| **Mobility, flexibility and a platform for growth** | 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:<br>• 53 per cent more likely to have seen a revenue rise in the past year;<br>• twice as likely to grow their range of products and services compared to those who had not adopted cloud; and<br>• almost three times as likely to increase staff numbers in the coming year. |

*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.[8] 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

[8] ACMA *Digital Footprints and Digital Identities – Community Research* 2013 (unpublished).

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 Directorate[11], 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

---

[9] See Data Sovereignty and the Cloud; http://www.nextdc.com/media/news/581-nextdc-releases-data-sovereignty-guide-flags-australias-data-fabric-is-one-disaster-from-unravelling.html

[10] www.agimo.gov.au/policy-guides-procurement/cloud/

[11] www.dsd.gov.au/infosec/cloudsecurity.htm

[12] European Commission, Unleashing the Potential of Cloud Computing in Europe, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdfSeptember 2012 and OECD, *Science Technology and Industry Scoreboard 2011, www.oecd-ilibrary.org/sites/sti_scoreboard-2011-en/02/08/index.html?contentType=/ns/Chapter,/ns/StatisticalPublication&itemId=/content/chapter/sti_scoreboard-2011-19-en&containerItemId=/content/serial/20725345&accessItemIds=&mimeType=text/html*

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.[13] 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, 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.

[13] ACMA, *The cloud- services, computing and digital data, Emerging issues in media and communications* Occasional paper 3, June 2013, Page 17

**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 fallover. It should generally be assumed that consumers, SMEs and NFPs accessing cloud services recognise that internet

[14] ACMA, *The cloud- services, computing and digital data, Emerging issues in media and communications* Occasional paper 3, June 2013, page 17

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, 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?*