



Cloud Computing Contracts

White Paper

A Survey of Terms and Conditions

Prepared by:

Mark Vincent, Technology and Intellectual Property Law Partner
Nick Hart, Senior Lawyer
Kate Morton, Lawyer

TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	SURVEY OF CONTRACT TERMS	3
2.1	Basis of the Survey	3
2.2	Surveyed Issues.....	4
3.	RESULTS OF THE SURVEY	4
3.1	Law and Jurisdiction	4
3.2	Variations to Terms.....	6
3.3	Privacy Laws/Transborder Data Flows/Data Location	6
3.4	Security, Encryption, Backup	10
3.5	Service Level Agreements, Service Availability and Service Credits	12
3.6	Transition Out	14
3.7	Warranties and Warranty Exclusions and Limitations.....	16
3.8	Loss and Limitation Provisions	16
3.9	Consequential Loss	18
3.10	Multiple parties in the Cloud Stack.....	18
4.	CONCLUSIONS	19
	APPENDIX.....	20

Cloud Computing Contracts White Paper

A Survey of Terms and Conditions

1. INTRODUCTION

Cloud computing, at its simplest, relates to providing services over the internet in a way that gives the perception of limitless scalability where those services are not tied to a particular server or location. Cloud based services usually remove the necessity for organisations to invest in infrastructure up-front, and can enable the customer to scale its use of services up *and* down as demand fluctuates. Cloud services are particularly well suited to customers with variable or unpredictable demand, and economies of scale achieved by some cloud vendors provide compelling economic incentives for use of the cloud services or infrastructure.

In entrusting to a third party the provision of applications, infrastructure or services, elements of “control” may be to some extent taken out of customers’ hands. The terms and conditions being offered by the applicable service provider(s), especially terms relating to access to applications and data critical to the user’s business, the security of data, an ability to meet regulatory compliance needs, and the availability of legal remedies in relation to the service are all critical factors to be considered by both vendor and customer alike.

In this paper we have surveyed key terms taken from a range of publicly available terms and conditions for a variety of cloud services providers with a presence in the Australian market. Our survey does not include the contracts of every cloud provider and is not a critique of the contracts reviewed. As terms and conditions as well as the range and volume of cloud services available are changing quickly, this paper can only present a snapshot of some available contracts at the beginning of 2011.

Cloud services span a range of functionality and encompass different levels of service, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Infrastructure as a Service is, as the name suggests, the provision of computer infrastructure as a service. Customers buy infrastructure as an outsourced service as an alternative to purchasing servers, data-centre space or network equipment.

Platform as a Service provides the ability to develop and deploy software applications without the need to invest in the underlying hardware and software layers.

Software as a Service typically delivers software applications as a service over the internet. This eliminates the need for the application to be installed on the customer’s computer and can simplify maintenance and support.

2. SURVEY OF CONTRACT TERMS

2.1 Basis of the Survey

As part of this survey we have reviewed approximately 25 standard form contracts for the provision of cloud-based services.

We have focused on corporate offerings rather than those aimed predominantly at consumers. Consumer focused contracts are often based around free services and comparisons with those

contracts are less relevant for corporate users. Some of the corporate services are provided by Australian based companies, with others provided by international companies that offer their services on a global scale. The scope of the services covered by the reviewed contracts includes IaaS, PaaS and SaaS.

The majority of the contracts reviewed are publicly available on-line via the applicable vendor's web-site. We have sourced some contracts directly where they are not available over the internet.

We provide in the Appendix a list of the vendors whose terms and conditions formed a part of this survey. The chosen list is intended to produce some broad observations about the present state of contracts and does not purport to be a comprehensive list of cloud vendors with offerings in Australia, nor a direct comparison of their respective offerings and contract terms.

The contracts reviewed represent the standard terms of the vendors surveyed. For large corporate or government customers, these terms may be the subject of negotiation and customisation. For the small to medium enterprise ("SME") procuring any entry-level cloud service, the opportunity to negotiate may, in some cases, be more limited. Choice of vendor requires not just an assessment of contractual terms but requires a relationship of trust and confidence, which larger providers with global scope will frequently demonstrate.

2.2 Surveyed Issues

In this paper we have surveyed the following key provisions of commercial contracts for cloud services:

- (a) choice of law jurisdiction and dispute resolution;
- (b) variation to terms;
- (c) privacy laws and transborder data flows;
- (d) security and backup;
- (e) service level agreements;
- (f) transition out arrangements;
- (g) warranties and liability limitations; and
- (h) multiple parties in the cloud stack.

3. RESULTS OF THE SURVEY

3.1 Law and Jurisdiction

Choice of law and jurisdiction clauses are frequently included in written agreements.

Often the choice of law is specified as the place where the service provider has its main office or where it has a strong presence in a jurisdiction. The following clause is typical:

Any dispute relating in any way ... to products or services sold or distributed ... in which the aggregate total claim for relief sought on behalf of one or more parties exceeds \$7,500 shall be adjudicated in any state in federal court in King County Washington, and you consent to exclusive jurisdiction and venue in such courts

In other contracts, the choice of law can vary depending on the region where the customer is situated. For example, a USA provider with an established data centre in Singapore might specify that the contract for an Australian customer is governed by Singaporean law, while US customers are governed by US law. For example:

...what law will apply in any lawsuit arising out of or in connection with this agreement, and which courts can adjudicate any such lawsuit depend on where you are domiciled.... If you are domiciled in a Country in Asia or the Pacific Region ... the governing law is Singapore. The Courts having exclusive jurisdiction are Singapore.

A few providers with a strong multinational presence specify the law as being the place where the transaction is performed:

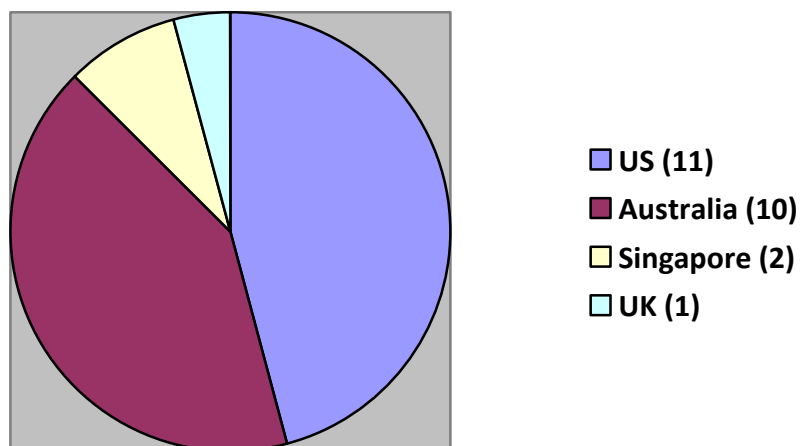
Both parties agree to the application of the laws of the state or territory in which the transaction is performed.

On the other hand, companies may provide that the applicable law is that of Australia:

The laws of New South Wales govern the Agreement and both parties irrevocably submit to the exclusive jurisdiction of the courts of New South Wales.

Of the contracts we reviewed, 11 provide choice of law and venue in the United States, 2 provide choice of law and venue in Singapore, 1 provides for choice of law and venue in the United Kingdom and 10 give an Australian State as a choice of law and venue.

Illustration: Choice of Law



3.2 Variations to Terms

In many of the contracts we surveyed, the provider has discretion to unilaterally amend the terms of the contract. This can be important to allow vendors to accommodate developments in technology and, in some cases, regulatory matters, such as updates to privacy laws, without the need for multiple amending agreements. For example, some of these contracts specify that variation can be effected by posting an updated version of the terms on the provider's web-site, and that the customer is deemed to accept the updated terms by continuing to use the service. For example:

[We] may change the terms of this Agreement or any Services Description at any time by posting a new version on the ... web site ... You agree to periodically review these web sites for changes to the Agreement .. You accept any modified terms by continuing to use the affected Services.

Contracting on terms that can be amended without notice involves an element of trust on the part of the customer that the provider will not change its terms in a way that is detrimental to the customer. This underlines the importance of selecting a vendor with an established reputation which it is unlikely to put at risk by a capricious use of the discretion. Alternatively, changes to contractual terms may be allowed without customer consent where, in the provider's opinion, they improve or do not have a material detrimental impact on the customer's rights. The following is an example:

Where, in [our] reasonable opinion, the amendment does not have a material adverse impact upon the client's rights under this agreement, [we] may amend any part of this agreement at any time without the client's consent by giving the client not less than 10 business days notice in writing.

Where, in [our] reasonable opinion, the amendment relates to improvements in the services, [we] may amend any part of this agreement at any time without the client's consent by giving the client not less than 10 business days notice in writing.

Other contracts we surveyed require the written agreement of the parties for variations of terms. An example is shown below:

No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and either signed or accepted electronically by the party against whom the modifications, amendment or waiver is to be asserted.

3.3 Privacy Laws/Transborder Data Flows/Data Location

Cloud computing typically utilises advances in technology which have allowed massive data centres to be built in ways which:

- (a) allow large economies of scale;
- (b) allow much lower numbers of people to manage and oversee this infrastructure;
- (c) are located close to economic sources of power supply; and
- (d) allow sharing of that infrastructure across multiple users with differing peak demands, including differing demands based on service delivered to multiple time zones.

Practically speaking, many of the advantages of cloud offerings will of necessity mean that cloud services are often not tied to Australia alone and many services operate across a region or indeed wholly from overseas.

Transborder Data Flows

Unlike a fixed server in an office or at a data centre in Australia, data in the cloud could potentially be anywhere in the world and even in multiple data centres and multiple copies. As a result, sending and processing data around the globe could involve issues of compliance with data protection and privacy laws in various countries. The legal term for this is transborder data flow.

Each country has its own set of laws regarding data protection and privacy.

In the EU, for example, there is a strict legal regime (under the *EU Data Protection Directive*) where, unless certain steps are taken, companies can be prohibited from transferring personal information to countries that do not give the same level of protection. Some exceptions to this rule are provided, for instance, when the controller itself can guarantee that the recipient will comply with the data protection rules. In terms of the EU's view of the Australian transborder protections, in 2001 an EU data protection working party formed the view that transfers to Australian businesses would only be seen as adequate if certain safeguards for personal data leaving the EU were put in place – such as approved contractual clauses, when exporting to Australia.

In Australia, the *Privacy Act 1988* (Cth) (“**Privacy Act**”) regulates the collection, use and handling of “personal information”. In the Privacy Act, personal information is defined as:

*information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*¹

This definition is broad enough to apply to a wide range of data kept by businesses.

Additional protection under the Privacy Act is also given to sensitive information which includes, among other things, health information, information about racial or ethnic origin, political beliefs, membership of professional or trade associations and criminal records.²

Businesses with a turnover in excess of \$3 million, or which deal with certain sensitive information, are bound by the National Privacy Principles under the Privacy Act (“**NPPs**”). In addition, if a business provides services to a government entity it may be bound by the Information Privacy Principles (“**IPPs**”) which regulate how Australian Government agencies manage personal information. Similar legislation applies to State Government contractors.

In Australia, prerequisites for moving personal information overseas (transborder data flows) are prescribed by NPP 9 and include requirements to ensure that the overseas entity is subject to a “substantially similar” law, or privacy scheme, or binding contract, that “reasonable steps” are used to ensure information will not be used inconsistently with NPPs, or to obtain

¹ *Privacy Act 1988* (Cth), section 6.

² *Privacy Act 1988* (Cth), section 6.

consent to the transfer from the owner of the personal information.³ If a cloud service provider does not indicate where the relevant data is being stored, then arguably the customer is not in a position to know which privacy scheme (or schemes) apply.

On 28 June 2010, the Australian Government released an Exposure Draft of the Australian Privacy Principles⁴ (“APPs”) that are proposed to replace the current NPPs. Under that exposure draft, APP 8 and a proposed new Section 20 of the Act will regulate cross-border disclosures of personal information.

Before a company holding “personal information” in Australia can disclose that information to an overseas recipient, it must first take reasonable steps to ensure that the overseas recipient will not breach the APPs. Furthermore, if the overseas entity does not comply with the APPs, then any act by an overseas entity that breaches an APP will be taken to have been committed by the company transferring the data offshore. Clearly, this anticipates vicarious responsibility for breaches overseas.

This is only an exposure draft at present and a number of exceptions are contemplated (including where the individual to which the data relates makes an informed consent to the disclosure overseas and its consequences) but the trend towards tougher data protection, with an awareness that the uses of technology are increasingly not tied to any one legal jurisdiction, is clear.

Many cloud service providers place the onus on the customer to ensure that privacy laws are complied with, and that the customer obtains or provides any consent that may be required. For example:

You also allow us to provide your personal information to any of our suppliers (or their suppliers) who are responsible for providing ... services to you.

You understand that:

- (a) some personal information may be transmitted to and stored overseas*
- (b) other countries may not have privacy laws which are equivalent to, or as comprehensive as, Australia's privacy laws;*
- (c) a third party recipient of your personal information may in turn transmit that information to another country in the course of providing the services to you; and*
- (d) we cannot control how our suppliers (or their suppliers) will use, store and disclose your personal information.*

The proposed APP 8 (and the new Section 20) set out a requirement for “informed consent”, which appears to present a higher threshold for compliance by customers and their service providers. As a result, individuals may need to be told about the rights that they have and that are otherwise being waived. Additionally, “consent” may be difficult to obtain if it is not known where the data will be stored.

³ *Privacy Act 1988* (Cth), Schedule 3, National Privacy Principle 9.

⁴ See: <http://www.smos.gov.au/media/2010/docs/100622-privacy-part-1-Companion-Guide.pdf>

Some service providers promise to comply with applicable laws as a provider of IT services (which presumably would include security requirements) or to comply with US Safe Harbour provisions, which facilitate the transfer of European data to the US. For example:

Certain Services are designed to help you comply with various regulatory requirements that may be applicable to you. However, you are responsible for understanding the regulatory requirements applicable to your business and for selecting and using those Services in a manner that complies with the applicable requirements.

Each of us agrees to comply with our respective obligations under the Data Protection Act 1998 (the “Act”) as applicable to personal data that it controls or processes as part of, or in connection with, its use or provision of the Services.

Where the service is being provided from overseas, the provisions regarding data protection and privacy are frequently tailored around the laws of other jurisdictions, such as the US or Europe as in the following example:

[We] have established internal mechanisms to verify our ongoing adherence to our privacy policy, including the Safe Harbor Principles. [We] also encourage individuals covered by this privacy policy to raise any concerns about our processing of personal information by contacting [us] at the address below. [We] will seek to resolve any concerns. [We] have also agreed to participate in the dispute resolution program provided by the European Data Protection Authorities.

Different requirements may apply in respect of data in Australia. While some of the standard publicly available contracts surveyed did not include specific Australian data requirements, assurances around compliance with the privacy regimes of jurisdictions with strong privacy laws, such as the EU, indicate that issues surrounding privacy are taken seriously by the provider.

Document Retention

In addition to privacy laws, a range of acts and regulations impose requirements on companies relating to document retention.⁵ For example, the *Corporations Act 2001* (Cth) (“**Corporations Act**”) requires financial records to be retained for 7 years after the transactions covered by the records are completed.⁶ If records are kept overseas, a company must give ASIC notice of where the information is kept and sufficient written information must be kept within Australia to enable a true and fair financial statement to be prepared.⁷

Industry Specific Regulation

The Australian Prudential Regulation Authority (“**APRA**”), which is responsible for the regulation of financial institutions in Australia, requires that a regulated entity must consult APRA prior to entering into an off-shoring agreement involving a material business activity, so that APRA can satisfy itself that the risk of the off-shoring relationship has been

⁵ A list of all regulations relevant to off shore data storage is beyond the scope of this survey.

⁶ *Corporations Act 2001* (Cth), section 286.

⁷ *Corporations Act 2001* (Cth), section 289.

adequately addressed.⁸ On 15 November 2010, APRA issued a letter to its regulated entities⁹ clarifying that it considered that cloud based services such as mail, calendar and CRM solutions could form an integral part of the institution's core business and decision-making processes. Accordingly cloud based services may need to be subject to the same rigour as any other outsourcing arrangement and risk management frameworks as outlined in applicable APRA Prudential Standards and Prudential Practice Guides.

3.4 Security, Encryption, Backup

A key concern for a business considering cloud services is the security and integrity of its data. The concern is equally held by service providers who recognise that the future lies in the cloud¹⁰ and with it, their reputation. A breach of security or loss of data can cause financial loss to the business as well as damage its reputation and the confidence of its customers. Similarly a breach of security or loss of data would be equally damaging to the ongoing business of a provider. The importance of continuous attention to matters impacting security of data is recognised by service providers¹¹

In addition, legislation may impose security requirements for certain types of data. For example, NPP 4.1 under the Privacy Act requires that:

An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

To comply with this principle, the "Guidelines to the National Privacy Principles" issued by the Office of the Federal Privacy Commissioner¹² advises that organisations should perform a risk assessment to identify the security risks to personal information.

Cloud service providers can assist customers to perform the appropriate risk assessments by being open about the security regimes they have in place to protect data stored within their cloud service and by contractually committing to specified levels of security. The risk assessment should fairly compare the arrangements that are currently in place to secure data on existing IT systems with the protection proposed by the cloud vendor. Often cloud vendors will be in a position to offer very sophisticated approaches to security beyond the capability of many individual businesses.

Some of the contracts we surveyed do not include commitments or warranties regarding data protection and security, as is shown in the following example:

The Service is provided with no warranties regarding security, reliability, protection from attacks, data integrity, or data availability (including without limitation data integrity or availability related to cloud storage features of the Service)

⁸ APRA Draft Prudential Standard CPS 231, : "Outsourcing"; December 2010 accessed at <http://www.apra.gov.au/Policy/upload/Draft-CPS-231-Outsourcing-for-consultation-Dec-2010.pdf> on 3 March 2011.

⁹ Puay Sim, Letter dated 15 November 2010, "Outsourcing and Off-shoring – Specific considerations when using cloud computing services" accessed at <http://www.apra.gov.au/ADI/upload/Letter-on-outsourcing-and-offshoring-ADI-GI-LI-FINAL.pdf> on 6 March 2011.

¹⁰ See, for example, comments made by Steve Ballmer, CEO of Microsoft in March 2010.

¹¹ See, for example, <http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf>

¹² Office of the Federal Privacy Commissioner, "Guidelines to the National Privacy Principles", September 2001.

It is also not uncommon for some service providers to expressly include terms in their contracts requiring the customer to implement security measures to protect their data including using appropriate encryption and maintaining backups, for example:

You are solely responsible for procedures and controls regarding encryption and backup of all content and for the implementation of these procedures and controls.

We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly ... you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications ... We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

It may use the ..Service as a backup service but agrees to maintain at least one additional current copy of its software and data stored ... somewhere other than on the .. services.

Contracts which give more detail about security arrangements may provide more certainty to customers, although even in these cases the ultimate responsibility for security often lies with the customer, as in the following example:

... [We] agree to use best efforts and commercially reasonable best practices when deploying services related to data integrity, backup, security, and retention. These services include, but are not limited to: hard drive storage, raid hard drive arrays, network attached storage, storage area networks, operating system installs, operating system reloads, customer portal information, and other situations involving customer data. Customer assumes ultimate responsibility for data integrity, retention, security, backup, and ownership.

The only security we provide for a virtual computer is that which is expressly advertised as part of the service. You are solely responsible for: (a) determining whether that security is sufficient for your purposes.(b) implementing any other security measures you deem appropriate.

Very few contracts we surveyed specified what would happen in the event of a security breach or included a requirement for the customer to be informed of such a breach.

While the customer can control some aspects of security and data integrity, such as maintaining independent back-ups and using data encryption, many aspects of data security in a cloud based environment are out of the customer's control (or even knowledge). This includes the physical security of the data centre, virus protection, protecting against external attacks and maintaining security of data as it is transferred between data centres. Again, this underlines the importance of choosing a reputable service provider with strong data protection policies and procedures.

Providers may make representations about the security and services they provide, either on their web-sites, or during negotiations for the provision of the services, such as:

When you trust your company's information to [us], you can be confident that your critical information is safe and secure.

[The services are] designed to provide you with a secure and reliable platform for your data ... Unauthorized parties cannot access your data

However, representations are commonly excluded from the terms of the agreement that is ultimately entered into between the parties, for example:

This agreement sets out the only conduct, warranties and representations relied on by the parties and supersedes all earlier conduct, warranties and representations made by the parties with respect to its subject matter.

You warrant that you have not relied on any representation made by us which has not been stated expressly in these Master Terms.

Even if the representations are incorporated into the contract, the limit on a service provider's liability in the contract will, in many cases, restrict what can be recovered by a customer in the event the representations are breached or not satisfied. However, if the representations amount to misleading or deceptive conduct, a non-excludable claim may exist under the *Competition and Consumer Act 2010* ("CCA").

Where there is little offered in the way of contractual guarantees relating to data security, it is imperative that businesses undertake their own risk assessment. In fact, it may be the case that in practice the service provider provides superior security and data integrity than the customer could economically achieve in-house, even if it is not backed up by a contractual guarantee. In this area, the importance of choosing a vendor which shares a customer's reputational risk may be one of the most important aspects of vendor choice. The assessment of the impact on the vendor of a security breach should form a part of the commercial assessment involved in procuring cloud offerings.

3.5 Service Level Agreements, Service Availability and Service Credits

If business-critical applications and data are accessed and stored via cloud services, the failure of the service, even for relatively modest amounts of time, can have a significant impact. Service providers recognise this and seek to regulate and define the level of service that customers can expect through Service Level Agreements ("SLAs").

SLAs are not unique to cloud services and are commonly used in relation to other forms of technology related services, such as more traditional outsourcing and hosting arrangements.

Some of the contracts surveyed incorporate SLAs that specify a "guarantee" or "target" for service availability levels. Such guarantees or targets, if they are included, typically range from range from 99.0% to 100% uptime each month. This allows customers to determine their sensitivity to downtime and the impact of unavailability for reasons such as routine maintenance.

SLAs may provide the customer with a credit for the service fees paid or payable by the customer in the event the service outages exceed a predetermined amount. This demonstrates that the provider has a financial inducement to ensure that the service level guarantees or targets are met. Examples of the credits provided in the SLAs we surveyed include:

- 5% monthly service fee per 30 minutes of continuous service disruption;
- 5% per 60 minutes monthly cumulated down time;
- 100% if percentage up time in a month is less than 95%.

The amount of credit that can be claimed can in some cases be capped and outages due to many reasons may be excluded from the calculations of service levels. Examples of outages that are not counted in the calculation of service levels can include if:

- there is a planned outage;
- there is a failure of the internet connection;
- the provider's system is subject to attack by a virus, hacking or denial of service attack;
- the customer breaches the agreement;
- an emergency occurs; or
- the outage event is less than a minimum threshold eg.10 or 30 minutes.

The following is an example from an SLA that "guarantees" 100% uptime. However, credits are only available if the service is down for a continuous block of 30 minutes. This means that if there are several incidents causing downtime of 25 minute each throughout the day, the customer would not be entitled to any credits:

...[We] guarantee one hundred percent (100%) uptime on all Public Network services to Customers located in our data centres. Except for service downtimes resulting from Customer's fault ... for each continuous uninterrupted thirty minute interval of Public Network service downtime that Customer experiences during an applicable month ... agrees to grant to customer a SLA credit of 5% of the Customer's monthly service fees for that month ... downtime of less than 30 continuous uninterrupted minutes do not qualify for this service credit.

Many of the surveyed contracts contained terms which state that data and services will be unavailable during scheduled maintenance, either at particular times or after a notice period provided by the provider. In some instances, maintenance times are often scheduled for the middle of the night at the service provider's place of business or where a major market is located.

However, the reconfigurable nature of cloud infrastructure means that providers can in some circumstances be in a position to manage scheduled maintenance in a way that does not interrupt services to customers. For example, some service providers have announced the removal of the scheduled downtime exception from their SLAs and the removal of threshold limits of unscheduled downtime before customer service level credits can be claimed. This is done to overcome the apprehension potential customers may have that by moving to a public cloud model they will be vulnerable to experiencing unexpected downtime, thus leaving them unable to access business critical applications.¹³

In some cases, credits may only be given if the customer has made a claim in a particular form. An example of the type of information that may be required in order to claim a credit is as follows:

¹³ "No more schedule downtime for Google Apps", accessed at <http://www.pcauthority.com.au/News/245091,no-more-scheduled-downtime-for-google-apps.aspx>

To receive a Service Credit, you must submit a request by sending an e-mail message To be eligible, the credit request must ... (ii) include, in the body of the e-mail, the dates and times of each incident of [unavailability] that you claim to have experienced including instance ids of the instances that were running and affected during the time of each incident; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within thirty (30) business days of the last reported incident in the SLA claim.

In contrast, the following provider promises to monitor the availability of its services and proactively provide a credit if the service level targets are not met:

[provider] will monitor the availability of each Virtual Private Data Centre, and will automatically issue any credit that is due. In addition, you may report any instance of unavailability.

3.6 Transition Out

Access to data at the end of an agreement may be required by some customers. Some contracts surveyed by us state that the service provider is entitled to delete data on the cancellation of a service, or otherwise do not address the retrieval of data at all. In such cases, the onus is on the customer to ensure it has retrieved any necessary data before the contract is terminated.

An important aspect of data retrieval on termination may be the extent to which the data can be converted for use in alternative applications. Data may, for example, need to be accessed for the purpose of litigation up to 10 years after an event giving rise to the litigation.

If data is stored as part of a SaaS application, it may be important that the data can be retrieved in a vendor neutral format so that it can be imported to an application provided by a new third party service provider.

Below is an example of a clause that provides for data retrieval in a predetermined form:

Upon request by You made within 30 days after the effective date of termination ... We will make available to you for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format.

Some providers offer assistance to retrieve data, although the assistance given may be subject to agreement at the time and subject to payment of fees:

... during the 30 days following termination: (i) we will not erase any of Your Content as a result of the termination; (ii) you may retrieve Your Content from the Services only if you have paid any charges for any post-termination use of the Service Offerings and all other amounts due; and (iii) we will provide you with the same post-termination data retrieval assistance that we generally make available to all customers.

Nonetheless, as in the above example, it is often the case that access to data and assistance may not be provided if termination is “for cause” or if payment of fees is not up to date. This could occur, for example, where a company is suffering financial difficulties and may have gone into administration. In this situation, the insolvency event may have triggered an

automatic termination of the agreement, and the inability of the customer to pay fees in a timely manner may result in the loss of the right to retrieve data.

Accordingly, it may be up to the customer to retrieve its data before the services are terminated, as in the following examples:

..we may delete your data immediately after the cancellation of your ... application. We will try to give you notice before we do this. We recommend that you make a copy of your data before your ... application is cancelled.

... after your service is terminated, we are not responsible for storing or retaining the contents of a virtual computer or data storage. It is solely your responsibility to copy and download any data you require before your service terminates.

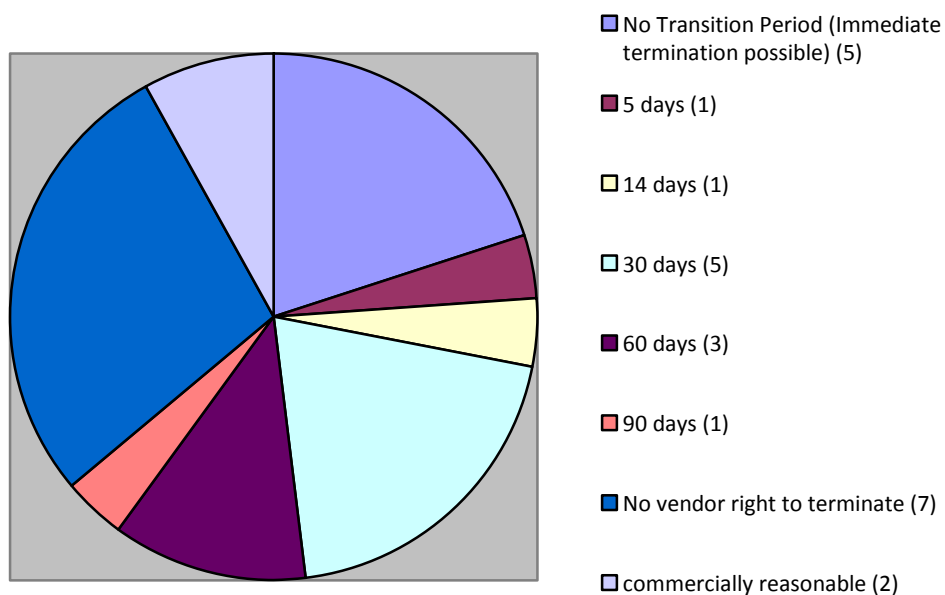
All Customer data remaining after the cancellation date will be destroyed for security and privacy reasons, unless otherwise required by law.

If the customer has consciously chosen to terminate the agreement, appropriate plans can be made to retrieve the data before termination. However, if the termination is inadvertent and immediate, the ability to retrieve data may be curtailed.

The table below specifies the time available for a customer to retrieve data when a contract is terminated by a vendor for convenience. This includes the notice period and any post termination right to retrieve data.

Note that virtually all contracts surveyed allowed the vendor to terminate the agreement immediately for cause in at least some circumstances. Of these only 1 specifically gave the customer the right to retrieve its data in those circumstances.

Illustration: Transition Periods (including notice period for termination for convenience, plus any post termination right to access data)



One final issue to note is that of the vendors whose terms and conditions were surveyed very few provided for destruction of customer data after the contract has ended. It may be important for some customers to have certainty as to the destruction of their data when a contract ends.

3.7 Warranties and Warranty Exclusions and Limitations

Most of the contracts we surveyed provided few express warranties in relation to the services provided, and sought to exclude implied warranties (such as merchantability and fitness for purpose) to at least some extent as demonstrated in the following example:

The Services are provided as is without representation or warranty of any kind, whether express, implied, statutory or otherwise with respect to the service. Except to the extent prohibited by law, we disclaim all warranties including implied warranties of merchantability, fitness for purpose and non-infringement.

In Australia, certain guarantees are implied into contracts by the CCA where the value of the services are less than \$40,000 or where the services are of type normally provided for ordinary household use. The CCA replaced the *Trade Practices Act 1974* (Cth) from 1 January 2011. The guarantees under the CCA include that the services are provided with due care and skill,¹⁴ and that the services are fit for a particular purpose if that purpose was expressly or by implication made known to the provider.¹⁵ Contracts that are expressed to be made under Australian law often acknowledge the application of the legislation, such as in the following example:

Some laws – particularly the Trade Practices Act 1974 ('the Act') – may give you rights and remedies that cannot be changed or excluded. These Master Terms and each Service Contract are subject to those laws.

In certain circumstances the CCA does allow liability in relation to these statutory guarantees to be limited. This is addressed in more detail below under the heading “Loss and Limitation Provisions.”

The approaches of vendors to this issue of warranties and implied warranties does not depart from norms established over time in relation to other IT services, where warranties are often viewed as introducing uncertainty in circumstances where the consequences of imperfections in service delivery are sought to be identified as the subject of specific support and maintenance arrangements.

3.8 Loss and Limitation Provisions

Most providers seek to limit liability for direct and exclude liability for indirect loss. For example, it is not uncommon for providers to seek to limit liability for direct damages in the following manner:

We and our affiliates or licensors will not be liable to you for any direct , indirect, incidental, special, consequential or exemplary damages (including damages for loss of profits, goodwill, use or data), even if a party has been advised of the possibility of such damages.

¹⁴ *Competition and Consumer Act 2010* (Cth), schedule 2, section 60.

¹⁵ *Competition and Consumer Act 2010* (Cth), schedule 2, section 61.

In Australia, as noted above in relation to warranties, the CCA can imply into certain contracts guarantees which cannot be excluded. Although any term that purports to exclude these guarantees is void, for most such guarantees, if the services are not of a kind ordinarily acquired for personal, domestic or household use, the CCA allows providers to limit their liability to supplying the service again or paying the costs or resupplying the service.¹⁶ Contracts governed by Australian laws are often specifically drafted to reflect this:

Where we are allowed to limit it, our liability for breaches of the [Competition and Consumer Act 2010] is limited, at our option to ...in the case of services:

- 1. supplying the services again; or*
- 2. paying for the cost of supplying the services again.*

A number of the surveyed contracts take a tiered approach to restricting liability, stating that if a clause is ineffective to exclude or limit a liability an alternative cap on liability would apply:

To the extent permitted by law, [our] liability to the Customer in relation to the Services and the Agreement is limited (at [our] option), to: in the case of Services, resupplying the Services or paying the cost of having the Services resupplied; or (b)

in the case of goods, repairing or replacing the goods or paying the cost of having the goods repaired or replaced.

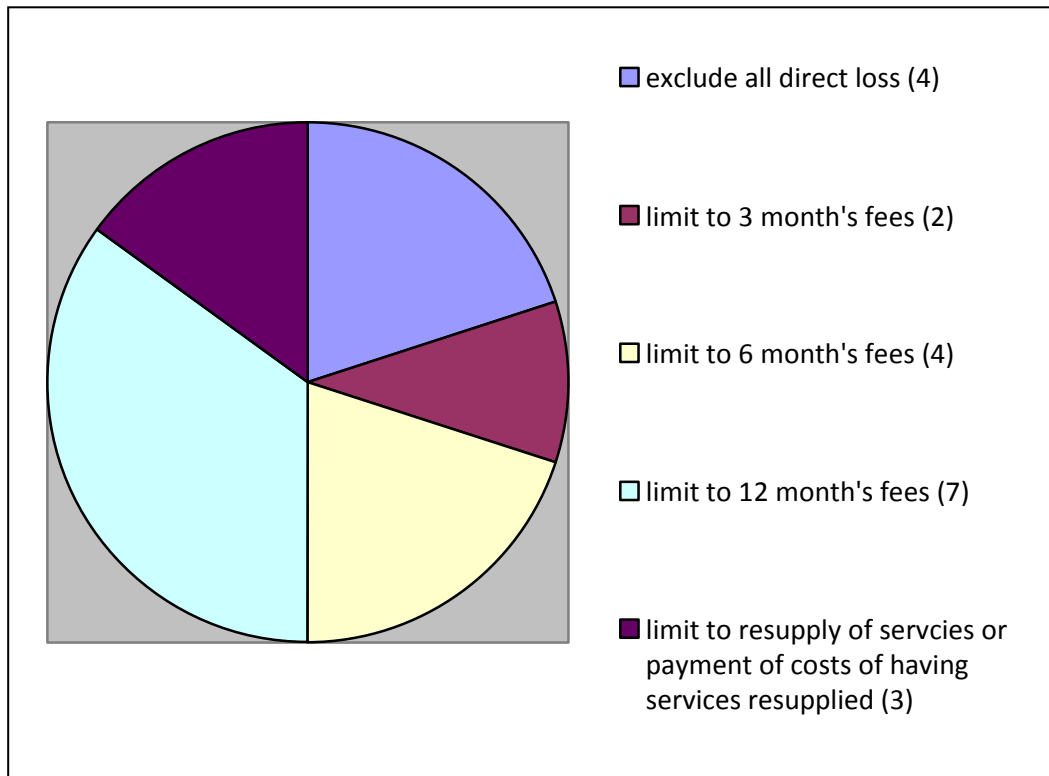
If, notwithstanding [the above clauses], [we are] liable to the Customer in relation to the Services or the Agreement, [our] liability is limited to a sum equal to the total amount paid or payable by the Customer under the Agreement in relation to the Services affected by the circumstances giving rise to the claim for the period of 12 months prior to the date of the liability arising.

All except one of the contracts we surveyed excluded all liability for consequential and indirect loss such as loss of profits.

All contracts surveyed seek to limit liability for direct loss to some extent. Of those 5 purport to exclude all direct loss. Others limit the loss either to the amount of fees paid during a specific period, a capped monetary amount, resupplying the services or the cost of resupplying the services or a combination of the above. One vendor limited compensation to the credits available under its SLA. The table below summaries the different approaches to direct loss limitations.

¹⁶ Competition and Consumer Act 2010 (Cth), schedule 2, section 64A(2).

Summary of approach to direct loss¹⁷



3.9 Consequential Loss

Typically, a service provider will seek to exclude all liability for so-called “consequential loss” (note that in Australia, consequential loss arising from breach of an implied guarantee under the CCA may not be excludable), such as a customer’s loss of profits, loss or damage to data or to its management time as a result of a breach. For example:

In no circumstances are we liable for any indirect, secondary or consequential loss or loss of income that you or anyone else may suffer.

An inability to access data or services crucial to a business may result in very large loss of profits, and it may be difficult for a provider to know the extent of the possible losses.

The contract will not act as insurance against all loss and many providers will be keen to avoid the reputational damage caused by a failed service. When assessing this issue, it is important to consider the differing impacts of outages for major global providers as opposed to small start up companies providing cloud offerings.

3.10 Multiple parties in the Cloud Stack

In many cases, cloud services will be provided by multiple parties. A cloud SaaS application provider may have developed the application based on a cloud platform service such as Microsoft Azure. The application may be hosted by another company that supplies IaaS services. An IT services company may provide a total solution which is based on multiple re-

¹⁷ All but 1 provider excludes indirect losses and several providers provide a monetary cap as an alternative to measuring fees over time.

sold cloud products. The increased reliance in many cloud services on multiple parties will have implications for cloud contracts. For example:

You also allow us to provide your personal information to any of our suppliers (or their suppliers) who are responsible for providing ... services to you.

You understand that:

...

- (c) *a third party recipient of your personal information may in turn transmit that information to another country in the course of providing the services to you; and*
- (d) *we cannot control how our suppliers (or their suppliers) will use, store and disclose your personal information.*

As a result, issues such as who the customer is dealing with, who has access to the data and what are the relationships with subcontractors arise in relation to the existence of multiple parties in the cloud stack.

4. CONCLUSIONS

Our survey has identified a number of differing approaches in standard form contracts for cloud services. While many of these are not new and readers familiar with IT contracts will recognise some of the differing approaches, they do demonstrate and seek to address the transformation of the computing experience enabled by the cloud. As the cloud evolves we can expect to see a corresponding evolution in the terms and conditions applying to the delivery and use of cloud services.

As we have shown, the fact that the services to be provided are in the cloud and not tied to a particular location has resulted, in particular, on a focus on issues relating to the transfer, protection and security of data. This focus highlights the importance of confidence in the cloud and demonstrates the benefits that engaging a trusted provider who is at the forefront of development of best practice in the area and whose reputation both relies on and supports the principles of data protection and security, can bring.

Truman Hoyle Lawyers

5 April 2011

APPENDIX

Provider	Link to Agreement
3Tera	http://www.3tera.com/Terms/index.php
Akamai	http://www.akamai.com/dl/akamai/akam_terms_conditions_05.pdf - retrieved on 14 March 2011
Amazon	http://aws.amazon.com/terms/ Amazon Web Services Customer Agreement http://aws.amazon.com/agreement/
Brennan IT	http://www.brennanit.com.au/Portals/0/Information/IAAS%20Product%20Terms.pdf accessed 21 February 2011
Cloud Central	http://www.cloudcentral.com.au/terms accessed 21 February 2011
GoGrid	http://www.gogrid.com/legal/terms-service.php accessed 7 March 2011. (terms) http://www.gogrid.com/legal/sla.php (sla)
Google	http://www.google.com/apps/intl/en/terms/premier_terms.html - Retrieved 15 March 2011
IBM	Smart Business on the IBM Cloud – Public Cloud Agreement https://www-180.ibm.com/cloud/enterprise/beta/static/Z125-8338-01-30Sept09CloudServicesAgreementInternational.pdf - accessed on 19 January 2011
IntraPower	http://www.intrapower.com.au/uploads/files/09productgroupconditionsondemandservices.pdf accessed 8 March 2011. (cloud computing specific) http://www.intrapower.com.au/uploads/files/02basicconditions.pdf (basic terms)
Joyent	http://www.joyentcloud.com/about/policies/terms-of-service/
Macquarie Telecom	http://www.macquarietelecom.com/downloads/Aust_service_agreements/Macquarie%20Telecom%20Trading%20Terms%20-%20v10%2010%20August%202010.pdf
MelbourneIT (Beta)	https://vcloudexpress.melbourneit.com.au/terms-and-conditions/ accessed 21 February 2011
Microsoft SQL Azure	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=fa4f7fed-b17f-4cf5-b80f-531b9b681b5c – Retrieved 14 March 2011
Ninefold	http://ninefold.com/legal/customer-agreement accessed 16 February 2011
Nirvanix	http://www.nirvanix.com/how-to-buy/terms.aspx accessed 15 February 2011
OpSource	http://www.opsource.net/OpSource-Cloud-Terms accessed 8 March 2011. (cloud computing specific)
PayPal	https://cms.paypal.com/au/cgi-bin/?cmd=_render-content&content_ID=ua/MerchServices_full accessed 15 February 2011

Provider	Link to Agreement
Rackspace	http://www.rackspace.co.uk/rackspace-home/legal/general-terms/ accessed on - 26 January 2011
Salesforce	http://www.rackspace.co.uk/rackspace-home/legal/general-terms/ accessed at 27 January 2011
Softlayer	http://http.cdnlayers.com/softlayerweb/SoftLayer_MSA.pdf accessed 22 February 2011
Telstra	http://www.telstra.com.au/customer-terms/download/document/t-suite.pdf accessed 21 February 2011
The Planet	http://content.theplanet.com/Documents/legal/Planet-TOS.pdf accessed 15 February 2011
UltraServe (Rejila)	http://www.rejila.com/about/terms-and-conditions accessed 21 February 2011
VM Vault	http://www.vmvault.com.au/images/vmvault%20service%20agreement%20v1.3.pdf accessed 21 February 2011
Voxel	http://www.voxel.net/msa accessed 7 March 2011. (terms) http://www.voxel.net/sla