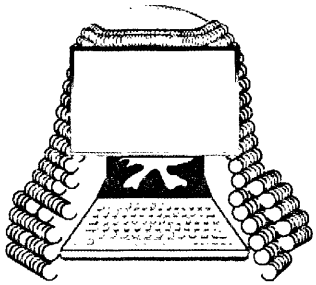
COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law



Editors: Martin Squires and Vinod Sharma

ISSN 08117225

Number: 79

January 2011

Legal issues in the cloud

By Mark Vincent and Nick Hart

***Mark Vincent** is lead technology and intellectual property partner, and **Nick Hart** is a senior lawyer, with Sydney based boutique media communications and technology firm Truman Hoyle.*

1. Introduction

> *The internet, our relationship with it, and our culture are about to undergo a change as profound and unsettling as the development of web 2.0 in the last decade, which made social media and search – Google and YouTube, Facebook and Twitter – mass, global phenomena. The rise of "cloud computing" will trigger a battle for control over a digital landscape that is only just coming into view.*[1]

Cloud computing services have been on offer for many years – most noticeably with free consumer services ranging from the launch of Hotmail to Gmail and social media sites like Facebook. But the scale and use of cloud computing – in particular as an enterprise or business solution – is being heralded as the next big thing in the IT industry.

At its simplest, "the cloud" relates to providing both services, and the perception of unlimited scalability of services, over the internet – including cloud infrastructure as a service; cloud platform as a service; and cloud software as a service. Compared to, for example, a situation where data processing or storage takes place on your own computer or an office network, with the "cloud" these take place via platforms offered "online" (or in a series of high tech data centres at multiple locations around the globe) by third parties (such as Microsoft, Amazon, Google and Salesforce).

The availability of cloud services is made possible by significant increases of scale and technological

In this issue

From the editors...

Lawyers practising in the IT sector are continually confronting legal issues generated by cloud computing offerings. In this issue, Mark Vincent and Nick Hart analyse some of the risks arising out of cloud computing. While cloud computing offers many benefits, customers will need to be aware of the legal risks when making decisions about such offerings.

As the use and popularity of social networking sites such as Twitter continues to grow, so do questions about how legal principles apply in respect of these new communication tools. David Martin, in his article "Tweet and Sour", raises the issue that, in theTwitterverse, brand owners have encountered both cyber-squatting and the use of Twitter usernames containing their registered trade marks. The author provides a brief summary of the legal and other options available to a trade mark owner who finds the integrity of their brand threatened by a third party on Twitter.

We are pleased to announce the winner of the 2010 Student Prize is Glenn Harwood, for the article "Copyright in the wake of Pirate Bay". Glenn, who is a Bachelor of Commerce (finance major) and a Bachelor of Law student at Bond University, analyses the implications of the litigation against *The Pirate Bay* in Sweden which resulted in four individuals being jailed following criminal convictions relating to copyright infringement.

There were a number of entries of a high standard in the 2010 Student Prize competition, and we thank all those who entered. A selection of entries will be published in future issues.

The Student Prize is being offered again in 2011. We encourage all those who are eligible to submit entries. Details of the competition are set out on page 7.

Finally, Pamela Gray continues her series of profiles of persons who have been significant to the life of the NSW Society of Computers and Law. In this issue, Pamela profiles the patron of the society, the Hon Michael Kirby.

Martin Squires and Vinod Sharma

Continued from Page 1

developments – such as advances in infrastructure with huge farms of computer servers (distributed in shipping container sized units) located all over the world, on which the biggest technology companies spend billions of dollars each year. Customers are able to store and access data and services online (in the cloud) thanks to the availability of increased internet bandwidth at reasonable prices and to the decreased costs of operating, powering and managing data centres – hence a resulting decrease in the cost of access to cloud offerings.

One of the key features of the cloud is what is called the "scalability" of service – which means the services and resources required can be scaled up or down depending on demand. This means that cloud users do not have to outlay capital expense on hardware or software based on their anticipated peak demands, rather they buy infrastructure on demand.

If you take as an example the Australian Taxation Office – its system load would peak for a few months of the year when online tax returns are due - and would be relatively quieter at other times. Equally, a company might run an online or television advertised competition – and it would not know the scale of the public response and therefore what processing, storage and bandwidth capacity it needs in advance. Rather than having to cater for anticipated peak uses via multiple physical servers in data centres - a company could turn to the cloud to provide these services on an "as needs", "on demand", basis.

Compared to more traditional uses of technology, benefits of cloud computing include: access to services from anywhere; reduction in costs of hardware; "paying for what you use" for services/storage; savings on IT support; and efficiency.

Users and providers of IT services will have to weigh these advantages of the cloud against the risks or perceived risks – such as: regulatory compliance; security; performance; availability of service; and liabilities and remedies under the governing contracts.

When it comes to legal considerations, there are a number of constant issues with which corporate users of technology services will already be familiar. Most of these are contained in the contract (or terms and conditions of use) for cloud-based services – including: issues around the standard of the services being provided; the ownership of IP; service level agreements; liability regimes; warranties and indemnity provisions; confidentiality obligations; termination clauses and the like. In addition to the terms of the contract, there are various other requirements that are imposed by law –

such as regarding confidentiality, the liability of the parties (under the Australian *Trade Practices Act*, for example), and privacy.

There are no laws unique to the cloud. However, the cloud brings with it some legal issues which, whilst not applying only to the cloud, are perhaps now uniquely important to those operating or using a cloud-based service. In this brief overview we focus on 3 main legal issues, namely:

- sovereignty on the internet: location and use of data;
- terms of use and reliability; and
- lock-in and exit issues.

Depending on the type of business and technology issues involved, in negotiating or offering any cloud computing services, these issues are likely to arise with varying degrees of importance.

2. Sovereignty on the Internet: Location and use of data

Cloud computing services involve the processing and storage of masses of data that is often commercially sensitive, confidential, and "personal information". A key question with any cloud computing service is: "where is the data stored or processed?" It is a key question because location is not fixed in the cloud. Unlike a fixed server in your office or at a data centre in Australia, data in the cloud could potentially be located anywhere in the World and even in multiple data centres in multiple copies worldwide. In fact, a cloud service provider may not even know where the data is residing.

The cloud may not be tied to any particular location but this is clearly not the case with the laws of each country. Each country passes laws relating to acts which take place in its territory, and its laws can also extend to its citizens, companies incorporated within its jurisdiction and their overseas subsidiaries. Any "global" technology solution will be impacted by the laws of a large number of nation states. As a result, sending and processing data around the globe could in the process fail to comply with data protection and privacy laws in various countries. The legal term for this phenomenon is "Transborder Data Flow". Each country has its own set of laws regarding data protection and privacy – and of course some are dramatically more stringent than others.[2] Compliance advice increasingly must run in parallel with all new technology product offerings and with all new cloud technology solutions.

The EU, for example, provides 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. Personal data may only be transferred to third countries if those countries provide an adequate 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.

If a European company is processing any data in the cloud, and indeed if any company is processing personal information in the EU (for example through transacting with EU citizens on the internet) it may not be complying with EU laws if data is moved to certain countries outside the EU. As a consequence, some of Amazon's cloud services include an option for the storage and processing of data in Europe where no data leaves Europe.

To take another example (and to demonstrate that this area of law is in a constant state of change), on 28 June 2010 the Australian Government released an Exposure Draft of the Australian Privacy Principles[3] ("APPs") that are professed to be set to replace the current National Privacy Principles. Under that exposure draft, Australian Privacy Principle 8 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 Australian discloser of personal information does not ensure that the overseas entity will 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. 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.

Compliance with the laws of each jurisdiction involved in any cloud solution will be an issue for regulatory advice. Work is ongoing into transparent assessment of competing regulatory regimes. A harmonised approach is desirable but difficult to achieve, particularly having regard to the differing cultural attitudes to privacy and its protection.

Work is being done at the international level through the OECD and at the regional level through APEC to harmonise approaches to privacy regulation. An example is the new APEC Cross-border Privacy Enforcement Arrangement which has created a framework for regional cooperation in the enforcement of privacy laws. This arrangement commenced on 16 July 2010. In the medium term it should be expected that sufficient harmonisation of approach will emerge to facilitate regulatory compliance for regional cloud computing solutions.

In choosing or offering cloud-based services, these types of questions should be asked and transparency encouraged:

- Does the flow of data adequately meet the regulatory requirements of each jurisdiction it flows through?
- What data will be in the cloud?
- Does the vendor offer solutions to issues such as de-identifying data for transboarder data flow?
- Where will the data be stored or processed? Can a commitment be obtained?
- Who/what is processing the data? Are there multiple cloud platforms/parties involved?
- Can the movement of data be controlled?
- Should/can the data be encrypted?
- Who is liable for the data or any security breaches and what are the legal, commercial and reputational risks?
- Can we access all of the data in the future? For how long will it be retained (and is it long enough for legal and tax purposes)?
- Do the relevant contract clauses offer any protection -- such as by referring to standards of equivalent legislation or "model clauses"? Do these standards meet our own internal policies?
- What are the restrictions on the use of data?

3. Terms of use and reliability

A further key legal issue arises from the need for due diligence. This focuses around the area of identifying the players in the cloud relationship: i.e. who is actually involved in providing the services and are they the same entity (or entities) that are processing or storing data? In the case of aggregators, for example, a cloud user could be dealing with a single entity which itself is provided services by various third parties.

From a contractual and liability perspective, it can be vital that the user of cloud-based services knows whether it has a directly enforceable contract with the key players or whether it is relying on those with whom it does have a contract to enforce relevant provisions itself. For example, what happens if the services are unavailable or there is a breach of security and data is exposed? Has adequate due diligence been carried out along the chain of responsibility?

It goes without saying that terms of use should be reviewed in detail – and this should be done with all stakeholders, not just the legal and compliance teams. For example, a review of terms should seek to assess issues such as:

- The parties in the cloud stack – not just the contracting parties – and their roles, rights and obligations, especially regarding data;
- Whether each party has the rights required from other parties in the cloud stack;
- The capabilities and liability of other parties in the cloud stack;
- Backup/restoring data and disaster recovery;
- Service levels and what happens if the internet is unavailable;
- Continuous availability of services for business continuity;
- Treatment of data on termination/insolvency;
- What happens in the event of a security breach?;
- Other customary terms – e.g. change of control, service levels, service credits, audit rights, compliance with security standards, procedures in the event of a breach, force majeure.

Of course, in terms of risk management, users of cloud services are letting go of control when they use the cloud – and, for example, if there is an outage or a security breach, a user of cloud services could be in breach of its own contract with its own customers or of applicable laws, even if this is caused by the provider of services. This element of risk is brought into sharp focus when you consider that providers of IT services often tend to offer their services "as is", without assuming any risk – and with an exclusion for all liability where permitted by law. As an example, we extract part of a disclaimer clause from the terms of Google Apps Premier Edition:

"... GOOGLE AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND/OR NON-INFRINGEMENT. GOOGLE ASSUMES NO RESPONSIBILITY FOR THE USE OF THE SERVICE(S). GOOGLE AND ITS LICENSORS MAKE NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICE. GOOGLE MAKES NO REPRESENTATION THAT GOOGLE

(OR ANY THIRD PARTY) WILL ISSUE UPDATES OR ENHANCEMENTS TO THE SERVICE. GOOGLE DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE."[4]

We also extract some terms from Google Apps Premier Edition Terms dealing with data transfer and regulatory compliance:[5]

Trans border data flow	As part of providing the Service, Google may store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.
Privacy – customer consent	Customer is responsible for obtaining any necessary authorizations from End Users to enable Google to provide the Services.
Special protection for children	Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users.
Service Levels	During the Term of the applicable Google Apps Agreement, the Google Apps Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month.

An interesting example of the inadequacy of standard terms and conditions to meet the expectations and requirements of a business user (and the corresponding ability of large customers to drive customised legal terms) was reported recently in a successful bid by Google to provide cloud based services to the City of Los Angeles (such as disaster recovery and email to its 34,000 accounts)[6]. It has been reported that it is understood the contract includes unlimited damages for a data breach, guarantees as to where the data will remain and penalties if the services are not available for longer than 5 minutes a month.[7]

That these legal issues have been reported and discussed openly shows that the terms of business will be as important a factor in selecting cloud service providers as the services themselves. The importance of security, data and privacy issues also means that service providers and customers are likely to negotiate these terms upfront rather than dealing with them when a deal has already been agreed commercially.

4. Exist: Extraction of data / transition

The final legal issues we have chosen to mention in this article relate to notions of being locked-in to certain applications or systems – and if a user wants to transfer data or applications from the cloud, whether the data is portable between service providers. In these circumstances, a user will need to consider its requirements to access data some years into the future for a plethora of regulatory reasons.

Backup of data may well require the applications which created the data to be available in order to sensibly access it. This may be readily achievable if complete system backups and perpetual licences to applications allow a user to rebuild a system so as to restore data. In a cloud setting, rebuilding an application years later so as to make data intelligible may be impossible. Such an issue would be very important in assessing cloud offerings, which should allow a path toward compliant data retention.

All records, whether electronic or not, should be retained for at least the minimum period stated in any applicable statute or regulation. In Australia there are more than 80 acts of legislation, regulations and rules specifying document retention requirements applicable to companies under Australian law.[8] Data needs to be accessible for 5, 7 or 10 years (as applicable) after creation.[9] Such access may be required, for example, to comply with e-discovery rules where proceedings in Australia can be commenced up to 6 years after the events giving rise to the claim.[10] Another clear example of the need to access documents is for compliance with the Australian *Corporations Act*, which requires records to be retained for 7 years.[11]

Exit scenarios such as these should be considered at the outset of any relationship – and give rise to questions such as:

- If service providers change, can the records be usefully accessed?
- Are there any lock-ins?
- Can data be extracted from the cloud?

- When will data be transferred and what form will it take?
- What are the obligations on each party regarding an exit plan?

Vint Cerf, the computer scientist who is often called the father of the internet, has identified the issue of moving data between clouds as one of vital importance. He has said that developing "intercloud" standards and protocols (so that data does not get caught in one cloud) is the equivalent now of the issues faced in 1973 when networks could not communicate with each other.

As one commentator put it, one of the issues with cloud computing is that it can work a bit like Hotel California – you can check your data in OK, but will you ever get it out?[12]

5. Conclusion

Cloud computing offers some compelling efficiencies and an unprecedented ability to achieve scale without heavy upfront investment. The technologies which have developed to offer these new opportunities will change the way IT services are delivered.

Vendors, users, government, members of the legal profession and industry participants generally will have to work together to allow the full potential of these new technologies to be accessed and used. Some of the issues surround development of standards and best practice in the areas of security, interoperability, escrow, data transfer and privacy. An industry focus on defining first problems and then solutions to these practical impediments to roll out of cloud solutions will assist vendors and their customers alike.

In light of the additional layers of risk, and particularly in light of data and privacy issues, business users of cloud services will need to very carefully consider the terms of service and associated commercial and compliance issues. For the most powerful (largest) customers – negotiating terms of contracts will be important. For those with less bargaining power a careful consideration and comparison of the trading terms of multiple vendors will be essential.

---

[1] This statement was made by a think tank of the British Council, on 22 January 2010, Charles Leadbeater *"Let's open up cloud computing"*, The Guardian newspaper, 22 January 2010

[2] In the UK for example, HSBC (in one of a series of security breaches relating to its customer data) was last year fined GBP3 million for failing to have adequate safeguards in place for its customers' confidential details. http://www.esecurityplanet.com/news/article.php/3870071/HSBC-Confirms-Massive-Database-Security-Breach.htm

[3] See: http://www.smos.gov.au/media/2010/docs/100622-privacy-part-1-Companion-Guide.pdf

[4] http://www.google.com/apps/intl/en-au/terms/premier_terms.html as at 7 September 2010

[5] http://www.google.com/apps/intl/en/terms/premier_terms.html as at 7 September 2010

[6] http://latimesblogs.latimes.com/technology/2009/10/city-council-votes-to-adopt-google-email-system-for-30000-city-employees.html

[7] http://www.youtube.com/watch?v=Sa9fg8tLlIs and http://www.computerworld.com/s/article/9146118/LA_s_move_to_Google_Apps_is_underway

[8] *"Electronic Evidence, Document Retention and Privacy. Is a document worth the paper it is written on?"*, by Philip Argy, copy found at http://www.mallesons.com/publications/2006/Mar/8367966w.htm

[9] *In BT (Australasia) Pty Ltd v State of New South Wales (No 9)* [1998] 363 FCA the Australian Federal Court held that a party obliged to discover documents is obliged to discover data or information stored or recorded by electronic means. Telstra (who was subject to an order for discovery) was required to restore back-up tapes to recover deleted emails and their attachments. This was despite the fact that such a task was very onerous due to the vast amount of data kept on the back-up tapes.

[10] See for example the NSW *Limitation Act* (1969)

[11] In addition to document retention requirements under taxation legislation, Section 286(2) of the Australian *Corporations Act*, requires that accounting records "must be retained for seven years after the transactions covered by the records are completed".

[12] http://www.guardian.co.uk/technology/blog/2010/feb/05/google-cloud-computing-intercloud-cerf