Paper: Dimitrios G Eliades

TOPIC: Practice Management & Business Skills: Technology - Cloud Computing

1. What are ICT managed services?

   Information and communications technology (ICT) managed services are services which are designed to achieve a clients' desired outcomes in relation to productivity and efficiency gains through the provision of applications and services to end users, regardless of whether they operate from a fixed or floating location. For example:[1]

   - Hardware systems management (including full servers, desktops and printing management).
   - Data Networks, such as:
     - personal area networks (PANs);
     - local area networks (LANs);
     - campus area networks (CANs);
     - wide area networks (WANs), or
     - metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area such as a city support and management.
   - Business applications management;
   - ICT Help Desk management providing backup solutions and management;
   - ICT assets and software licensing management;

[1] Sonet Systems UK: http://www.sonet.com.au/index.php?option=com_content&view=article&id=73&Itemid=46

- Anti-spam, antimalware[2], antivirus[3] and WEB browsing management;
- Disaster recovery and business continuity solutions and management.
- Technology contracts management with your existing providers.

ICT managed services are also relevant to the public sector. The NSW Government's Infrastructure and Managed Services Plan provides a comprehensive roadmap for transforming the way the public sector uses ICT.[4]

As a general observation, the initiative is in response to a feature not limited to NSW. In NSW, Government agencies currently manage their computing infrastructure in a variety of ways, which results in a variety of *sui generis* systems. The difficulty with this is that it results in variable ICT service quality, increased costs and a diminished ability to capitalise on emerging trends such as cloud computing.[5]

The NSW Government identified the following urgent issues:

- Improving ICT infrastructure platforms so they can deliver better and simpler Government services;
- Improving the effectiveness of ICT expenditure; and
- Improving the agility of ICT infrastructure platforms so they can respond more rapidly to community needs.

The initiative entitled 'Infrastructure and Managed Services Plan' is said to take advantage of two major industry trends driven by technology advances and the adoption of web services by consumers:

- A move to a service orientation by both vendors and buyers; and

---

[2] Malware, short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses: http://en.wikipedia.org/wiki/Malware .

[3] Antivirus software is used to prevent, detect and remove malware (of all descriptions).

[4] http://www.services.nsw.gov.au/ict/priorities/infrastructure-and-managed-services

[5] Ibid.

- The deployment of cloud technologies into mainstream business.[6]

To achieve the significant financial savings goals set in place, government agencies will seek alternative IT delivery models that enable them to change how they pay for the serviceIT - to move away from *managing* IT operations, to *consuming* IT services.

While "clouds" that deliver IT services using web protocols through the Internet are emerging as viable alternative low-cost delivery models for commercial organisations, there is also an opportunity to create a secure 'government cloud' environment, to allow government organisations to take advantage of the same benefits.[7]

2. What is cloud computing?

A simple Google search reveals numerous definitions and opinions. One expression as a starting point is the following:

> Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet).[8]

The cloud is the space provided by the Internet via enabling software, whereby services, resources and information may be transported between 'computers', which of course, takes into account products which permit activation and use of the cloud from virtually any location.

The Australian Government has adopted the US Government's National Institute of Standards and Technology (NIST) definition for cloud computing:

> Cloud computing is an *ICT sourcing and delivery* model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [9]

---

[6] Ibid.

[7] http://assets1.csc.com/au/downloads/0809_15_G_Cloud_PoV_a.pdf The statement was made by CSC, which is a company providing technology based solutions and services and is headquartered in Falls Church, Va. CSC has stated that it has approximately 92,000 employees and reported revenue of $16.2 billion for the 12 months ended July 3, 2009: www.csc.com.au

[8] Wikipedia: http://en.wikipedia.org/wiki/Cloud_computing (24 February 2012).

[9] The complete NIST definition can be found at http://csrc.nist.gov/groups/SNS/cloud-computing/ .

There a various clouds or cloud delivery models.

- Private or internal cloud services: Cloud services are provided solely for an organisation and are managed by the organisation or a third party. These services may exist off site.

- Community cloud: Cloud services are shared by several organisations and support a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). These services may be managed by the organisations or a third party and may exist off site. A special case of Community Cloud is the Government or G-Cloud. This type of cloud is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role).

- Public cloud: Cloud services are available to the public and owned by an organisation selling cloud services, for example, Amazon.

- Hybrid cloud: An integrated cloud services arrangement that includes a cloud model and something else (another cloud model, agency back end systems, etc.), e.g. data stored in private cloud or agency database is manipulated by a program running in the public cloud.

3. What are examples of the types of relevant services?

Offshoring

Legal process carried on outside of an office refers to the process of obtaining services associated with legal practice through a service provider where the communication is predominantly online. Where those services are carried out outside of Australia, the process is referred to as 'Offshoring'.[10]
I can recall many years ago resisting offshore copy typing services as a cheaper alternative to secretarial services, on the basis of uncertain confidentiality arrangements. This primitive form of faxing documents to be copy typed, whilst not having the benefit of the cloud, reflected a desire to obtain perceived benefits, in the conduct of legal practice.

[10] http://en.wikipedia.org/wiki/Offshoring

The nature of the services that are outsourced includes legal research, document review, secretarial and paralegal services, drafting pleadings, conducting due diligence and IT functions which support the delivery of legal activities. One article published in the American Bar Association identified time costing and billing services and secure electronic signatures as services provided in a safe environment.[11]

In one trade mark case, the respondent's business provided a means to expedite document delivery through an internet postal service.[12] Subscribers to the service were provided with software which enabled them to access a 'virtual' mail room, whereby the document was sent to a location physically proximate to the document's destination. The mail would be printed at that location, folded and posted as local mail.

Email access

Web-based email services like Gmail and Hotmail deliver a cloud computing service: users can access their email "in the cloud" from any computer with a browser and Internet connection, regardless of what kind of hardware is on that particular computer.[13]

Data Storage

Other cloud computing services include virtual server storage (Infrastructure-as-a-Service or IaaS), such as Amazon Web Services, and software and product development tools (Platform-as-a-Service or PaaS), such as Google Apps.[14]

Other services

[11] http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html

[12] *Bing! Software Pty Ltd v Bing Technologies Pty Limited (No 1)* [2008] FCA 1760 (Collier J, 25 November 2008)

[13] http://mobileoffice.about.com/od/workingontheroad/f/cloudcomputing.htm

[14] Ibid.

A range of applications have grown in popularity which include VoIP[15] (e.g., Skype, Google Voice), social media applications (e.g., Facebook, Twitter, LinkedIn), media services (e.g., Picassa, YouTube, Flickr), content distribution (e.g., BitTorrent), financial apps (e.g., Mint).[16] These are software solutions provided over the Internet, or Software-as-a-Service (SaaS).

Like many products there are accessories. Mint offers a debt payoff planner for .99c, a home budget application for .99c and YNAB (You need a Budget) for $4.99.

4. What are the advantages?

Costs

The outlay may be the enabling software and possibly hardware to communicate the information, however in many cases it is a recovery cost for the provider. Voice recognition files have been used for many years, being sent as attachments to emails and returning as completed compatible interactive documents.

> In one large piece of UK litigation a large number of emails were required to be de-duplicated and correlated with relevant colour attachments. The process took 5 days.[17]

Storage

Anyone who has moved from a bigger place to a smaller place is faced with the challenge of working out where to put their purchases. Anyone with a computer has, in varying degrees, a history of storing data. Just some reasons include storing data to use again, storing data to shed light on past events or storing data to read at a later more convenient time.

The problem will arise that after spending allot of time acquiring data, the problem is to try to find a way to store it.

Some of the options have been:

- To purchase larger hard drives;

[15] Voice over Internet Protocol – VOIP is the sending of telephone calls over the Internet for less cost than those sent via the traditional phone system: http://www.discover-voip.info/voip-basics/voip-terms.html

[16] Above n 13.

[17] http://www.hobslegaldocs.com/case-studies/litigation-support-solutions/

- To use external storage devices like compact discs or thumb drives, also known as USB drives or flash drives;
- To delete entire folders worth of old files in order to make space for new information.

Others however are using cloud storage**.**

Rather than storing information on your hard drive you save it to a remote database and the Internet provides the connection between your computer and the database.

The payment of a subscription allows a larger provider the ability to provide storage capabilities for smaller individuals.

> Storage as a service (STaaS) is an architecture model in which a provider provides digital storage on their own infrastructure…a large service provider rents space in their storage infrastructure on a subscription basis. The economy of scale in the service provider's infrastructure theoretically allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered.[18]

This solution is appealing to organisations which have difficulties with offsite backup challenges.

Mobility & ubiquity

Another advantage is that you are able to get to that data from any location that has Internet access. No physical storage device is necessary and you are no longer tied to your desktop in order to save and retrieve information.

The storage may even allow other people to have access to the data, so a project may go from an individual effort to a collaborative effort. Where a project involves a number of contributors, the ability to view a live state of the project may lead to avoiding overlapping of contributions.

Service Levels & Uptime

[18] http://en.wikipedia.org/wiki/Storage_as_a_service

The opposite of downtime, it usually refers to a computer operating system's stability to be able to be left unattended without crashing, or needing to be rebooted for administrative or maintenance purposes.[19]

A service-level agreement (SLA) usually forms part of a service contract where a service is formally defined and where the SLA is often a reference to the contracted delivery time (of the service or performance).

One provider put it nicely in these terms:

> Our Service Level Agreement (SLA) has serious teeth. You can read through all the nitty-gritty details below, but before you dig in let's just start with this tasty morsel: 24x7x365 network uptime…[20]

SLAs are more commonly cautious and will typically have a technical definition referring to the average time between failures or the average time to make repairs or the average time to recovery.[21]

Support, service abstraction

As the name suggests, ICT Support Technicians provide support for the deployment and maintenance of computer infrastructure and web technology and the diagnosis and resolution of technical problems.[22]

Abstraction is a principle that is applied in the provision of computer related services. The principle seeks to avoid the duplication of information in general, and also avoiding the duplication of human effort involved in the software development process. For example, for a programmer the abstraction principle can be generalized as "don't repeat yourself" (the DRY principle).[23]

The benefit can be identified plainly in a service contract context. The information which is available to the public in the service contract is limited to what is required to effectively use the service. In general terms, the benefit being that:

---

[19] http://en.wikipedia.org/wiki/Uptime
[20] Server Beach: http://www.serverbeach.com/dedicated-hosting-services/service-level-agreement
[21] http://en.wikipedia.org/wiki/Service-level_agreement
[22] Australian Government 'Job Outlook': http://joboutlook.gov.au/pages/occupation.aspx?code=3131
[23] http://en.wikipedia.org/wiki/Abstraction_principle_(computer_programming)

- the service contract should not contain any superfluous information;
- the service contract would be limited to the technical contract and the SLA, and no other document.

Although this represents a 'what you see is what you get' approach, the level at which different consumers utilize the service will vary. Services can be designed to perform simple tasks. They may also be positioned to serve as gateways to entire automation solutions.[24]

5. What are the risks generally?

Choosing the Right Service Provider

The choice of the right provider will like most purchases, be dependent on the priorities of the purchaser. The following seem to be items service providers consider marketing advantages:[25]

- That the Data Centres & Support are located in Australia;
- That they carry Australian Tier-III certified data centres;[26]
- Payment is tailored to your actual needs on usage;
- Rapid Scalablity;[27]
- The time it takes to create and commence running the service;
- The speed of storage and integrity of the data storage facility;
- Data Protection through tools such as ZFS Replication which is said to represent durable storage for data protection.[28]

---

[24] http://www.exforsys.com/tutorials/soa/service-abstraction.html

[25] For example: http://www.cloudcentral.com.au/

[26] According to Macquarie Telecom, which states that its Intellicentre 2 is the first data centre in Australia to achieve Tier III Design Certification, this means the accredited centre:

- Utilises active power and cooling distribution path with multiple alternatives paths;
- Is concurrently maintainable which eliminates the need for shutdowns for equipment replacement or maintenance are eliminated;
- Has a guaranteed 99.982% availability:

http://www.macquarietelecom.com/corporate/data-centres/certification-accreditation

[27] A characteristic of a system, model or function that describes its capability to cope and perform under an increased or expanding workload. A system that scales well will be able to maintain or even increase its level of performance or efficiency when tested by larger operational demands: http://www.investopedia.com/terms/s/scalability.asp#ixzz2K0G0WPA0

[28] Zfs replication is that one creates a snapshot of the file system one wants to send initially to a secondary host. The command 'zfs send' is invoked on the first server, 'zfs recv' on the host getting

- The ability to provide a secure private network.
- The SLA provision for uptime – common to advertise 95.5% uptime.
- A guarantee as to the locality of the data.

Transition-In

This is a one-time effort that occurs each time a new element of the sourcing strategy is put in place. Transitions occur concurrently with other significant business and/or IT initiatives and are typically high-impact time-bound business activities.[29] The level at which the customer is able to minimise the disruption to the practice and integrate into the services seamlessly.

Transition-Out

There may be transitional issues associated with the termination of a service agreement. The NSW Supreme Court decision in *Cuscal Ltd v First Data Resources Australia Ltd* [2011] NSWSC 1625 (Rein J, 30 December 2011) exemplified the difficulties which may be associated with an exit strategy even where the service contract laid out a process to conclude a transition out strategy.[30]

Data Sovereignty & Security

One of the difficulties in keeping data stored in the Cloud is that the Cloud may be located anywhere in the world and/or in multiple data centres. The

---

the copy, and then the data is streamed over block by block, rather than relying on a process that must walk through directory trees: http://wikitech-static.wikimedia.org/articles/z/f/s/Zfs_replication.html

[29] http://www.finance.gov.au/publications/guide-to-ict-sourcing/phase-4-transition-and-manage.html#Transition

[30] In that case the defendant (the Service Provider) supplied a range of data transfer services to the plaintiff (the Client) which the Client then resupplied to its customers, who were credit unions and other small financial services providers. In the service contract which was to run for 5 years, there was provision for a process by which a transition strategy could be formulated. The termination assistance required the Service Provider to provide assistance to the Client that would transition the normal services from the Service Provider to the Client as the new provider (the termination assistance provision). Rein J considered that the Client had not taken certain steps set out in the contract toward the formulation of a transition plan and it followed Service Provider could not be expected to "ensure" smooth transition or continuity of supply where there had been such a failure: [22]. For Rein J considered it was necessary for the Client to specify what customers it wished to transition and by what date. His Honour concluded that the delay in seeking to enliven the termination assistance provision had been inordinate and that it was too late for the Client to rely on the termination assistance provision.

result is that there are multiple copies reproduced in various jurisdictions. There are likely therefore to be a variety of jurisdictional approaches to the laws those jurisdictions have as to privacy, access to the information and copyright.

For example, all U.S. citizens and permanent resident aliens, entities and organisations located in or out of the United States (including any subsidiary or foreign offices overseas) must comply with the USA PATRIOT Act 2001 and the Office of Foreign Assets Control regulations.[31] The US Treasury Department's Office of Foreign Assets Control (OFAC) maintains a list of nationals who have been specially designated.

No individual or business in the U.S., ***or the foreign subsidiaries of U.S. companies,*** may conduct any kind of business with anyone on the OFAC list. Further, U.N. Security Council Resolution 1373[32] has the force of international law binding on all member states. Those obligations include an obligation to afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.

The relevance is that even if your data may be in-country, the relevant question is whether the owner of the facility is a company which has a US parent and therefore bound by the obligations of the Patriot Act.

Contractual Issues

A first priority must be to identify who are the participants in the provision of the particular cloud service. What difficulties of enforcement arise where there has been an acceptance of the service provider's ability to store data at multiple data storage centres, yet have no ability to control that those centres be located within the jurisdiction.

Further, as noted in *Cuscal Ltd v First Data Resources,* there may be relevant provisions contained in the service contract, which are overlooked and act effectively as a waiver of rights.

[31] Executive Order 13224

[32] http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/resolution_%201373%20(2001).pdf

SLAs, Uptime & Service Interruptions

A service-level agreement or SLA is a negotiated agreement between two parties, where one is the Client and the other is the Service Provider. This can be a legally binding formal or an informal "contract". Although an SLA might provide for uptime, one might seek to rely on s 18 of the *Australian Consumer Law* in cases of repeated service interruptions. The downside of cloud computing in relation to SLAs, is the difficultly in determining the root cause for service interruptions due to the complex nature of the environment.[33]

Liability & Risk Allocation

Risk is a situation involving exposure to danger.[34] Risk can be allocated and managed through the use of transactional documents such as an ICT service contract.

The Australian Government's ICT liability policy recognises that requiring unlimited liability and inappropriately high levels of insurance can be a significant impediment to companies wishing to bid for Australian Government contracts. This is particularly so for small and medium sized ICT firms, which are not in a position to negotiate with their insurers.[35]

However between Clients and Service Providers, there are some fundamental issues to consider:

- The ability to negotiate a variation from the supplier's pro forma position. The practical difficulty is that the more secure a provider is, the more custom it will attract and the more difficult to negotiate terms;
- The nature of the service to be provided: for example a data storage facility as opposed to an application which constitutes the service such as an email filter.
- The nature of the material which will be the subject of the service in terms of the confidentiality of the material or the ability to retrieve with confidence all copies of the data on termination.

[33] http://en.wikipedia.org/wiki/Service-level_agreement
[34] http://oxforddictionaries.com/definition/english/risk
[35] 'A Guide To Limiting Supplier Liability in ICT Contracts With Australian Government Agencies' May 2010: http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/Documents/LimitingLiabilityReport.pdf

- The persons who should be consulted in relation to any decision to use a particular Service Provider.
- Whether the Service Provider is in fact providing the deliverables or subcontracting some or all of the deliverables. In that case it should be incumbent for the Service Provider to identify all subcontractors engaged to provide the deliverables. This has an impact upon risk, security and recovery after termination. A Client would want to know that the subcontractor is bound by the same warranties and obligations the Service Provider is bound by.

Breach

There are with any contracts several considerations arising when negotiating or seeking to contract cloud services. Where most contracts involve parties within the jurisdiction, the Internet has introduced international traders providing deliverables in a seamless manner.

An ICT service contract may provide indemnities for the Client, however consideration should be given to:

- The practicality of enforcement – for example will there need to be service upon a foreign entity;[36]
- The capacity to assess the loss – will it be too difficult to quantify;
- What is the nature of the breach and its impact upon the Client;
- Contractual terms relating to mitigation of loss;[37]
- The potential difficulty in identifying the cause of the breach.

The essential difference with ICT service contracts is that where there was jurisdictional comfort, there is now an extra jurisdictional component which must be taken into account. This is because the assumption that local traders can go to a local court to resolve their local differences now can no longer be assumed.

[36] The relatively recent admission as a signatory state into the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters (the Hague Service Convention) alleviates some of the difficulties formerly experienced in relation to service abroad.

[37] The NSW procurement policy encapsulated in the ProcurePoint strategy provides in their short form ICT contract terms for the Supplier and the Customer to use reasonable efforts to mitigate loss and to the extent permitted by law cap damages at the greater of $150,000 or twice the contract value: http://www.procurepoint.nsw.gov.au/sites/default/files/documents/short_form_ict_contractgeneralterms_and_conditions_v6.0.pdf

It is usual that these contracts provide that the provision of the deliverables will not infringe any third party intellectual property rights (IP rights). Although this may give rise to a cross claim for contribution, there is potential exposure as infringement of IP Rights is a tort and introduces the concept of joint tortfeasorship or common design.[38] In addition, there may be cases where the infringement of a third party's copyright might be deemed to be 'authorised' by the Client.

Of particular risk are breaches of confidence. Although the Service Provider will usually contract not to disclose the confidential information to anyone other than the customer, the identification of the locations where the confidential information might have been disseminated, may be a logistical nightmare.

In respect of information relating to an invention before the priority date of the invention, that is not yet filed, publication of the information will not affect the validity of the patent where the publication is made without the consent of the nominated person or patentee.[39] However that preservation of novelty or inventiveness, is alive if the publication is without the consent of the nominated person or patentee. The issue will be whether a patent is invalid because a failure to take reasonable steps to ascertain the security of the deliverables may be taken as an implied consent by the nominated person or patentee. Publication after lodgement of the patent application raises no issue, but lodgement before the date could be fatal.

Termination

In relation to private contracts, the Client's obligations generally involve payment for the deliverables. Accordingly, termination is normally associated with a failure to pay.

There may be termination arising from an unauthorised use of IP Rights where there is an attempt by the IP Rights holder to implicate the Service Provider. We can see in more obvious cases of infringement of IP Rights, that

---

[38] *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd* [2012] FCAFC 59 (27 April 2012) – The TV Now case. The Full Court favoured the interpretation that Optus and the subscriber could be said to be the maker for Copyright Act purposes as they acted in concert for the purpose of making a recording of the particular broadcast which the subscriber required to be made and of which he or she initiated the automated process by which copies were produced. In other words, they were jointly and severally responsible for the act of copying.

[39] *Patents Act* 1990 (Cth) s 24(1).

social media hosts Facebook and Twitter, have power to and do shut down sites clearly offending IP Rights. Such power is incorporated into their membership conditions and IP Policy.

From the Client's perspective, rights of termination may arise where:

- There is a failure to provide all of the deliverables.
- Where there is a breach incapable of remedy.
- Where there is a failure capable of remedy but is not remedied within the time provided by notice;
- The Service Provider is a company, an administrator or liquidator are appointed.

In many cases issues which are likely to arise include:

- The difficulty in recovering data;
- The extent of any downtime while services migrate.
- Dispute resolution policy and the question of the provision of the deliverable whilst that process occurs.
- Whether any of the Client's confidential information has been retained by the Service Provider.

Changing Providers

The decision to change providers will be influenced to some extent by the:

- complexity of the deliverables;

- the terms of the service contract.

In *Cuscal Ltd v First Data Resources* an exit strategy within the service contract was provided. The parties agreed in their 5 year contract, that they would prepare a termination assistance plan within 1 year of the commencement date. In that case, the Client was to take over the role of service provider for its customers rather than onselling the deliverables it contracted with the Service Provider to provide.

There was an anticipated collaborative approach to an exit strategy whereby the parties agreed to formulate this termination assistance plan. The failure to take steps to affect the termination plan was not taken for some time by the Client and the Client could not insist on its strict compliance.

Termination assistance may be required to assist the Client migrate with as little downtime as possible. This could be a relatively simple process such as changing web hosts. Alternately, data services for example, which cover

management information systems (MIS) may be more complicated. MIS are likely to include a wide range of applications including finance, human resources, payroll. These deliverables may be provided either as a single product/service or as a component in an integrated solution.

In *CA, Inc. v ISI Pty Limited* (*CA Inc*),[40] Bennett J of the Federal Court of Australia was dealing with relational database management systems. This was software which allowed users to store and retrieve data stored inside a "table".

Relational database management systems enable a user to relate data from one table to data in another table using a common "relation", for example, "find a row in the PAYROLL table and using an employee number (or name) and then find all entries in the SICK LEAVE table with the same employee number (or name)": *CA Inc* at [9].

Another difficulty to be considered in changing providers is the duration of the change. Where the migration requires downtime which can only be tolerated for very short periods of time, the time available for large scale data migration is generally very limited. In one example given in the evidence in *CA Inc, t*he conversion process took eight years.

Insourcing

Insourcing or 'in-house providers' is as an alternative to outsourcing. Outsourcing is well known and has been accepted by organizations across the world. Outsourcing is usually a cost saving tactic and allows a business to concentrate on its main functions while leaving its non-core functions to outsourcing providers in low-cost countries like India. [41]

Insourcing may be seen as a reaction to the hidden costs involved with outsourcing and dissatisfaction with the service provider. Companies may hire labour and services from an external organisation in order to cut costs and decrease their tax burden. Insourcing is also used when workers fill positions within an organisation for a short time only.[42]

Insourcing may also be considered where there may be some reluctance or inexperience with outsourcing. Where businesses seek to cut costs and limit their exposure to the use of the specialist, outsourcing is a preferred option.

[40] [2012] FCA 35.

[41] http://www.outsource2india.com/why_india/articles/outsourcing-versus-insourcing.asp

[42] Ibid.

The costs associated with insourcing specialised skills and processes are greater than outsourcing the same skills base.

Independent consultants Deloitte Consulting however argue that, 'instead of simplifying operations, outsourcing often introduces complexity, increased cost, and friction into the value chain, requiring more senior management attention and deeper management skills than anticipated'.[43] In addition it was noted that a fifth of all previously outsourced services in the United States were brought back in-house. The research found primary reasons for insourcing were: a failure to maintain service quality by the outsourced contractor (73%); and a failure to achieve cost savings (51%).[44]

There were several reasons for local authorities in the UK to reconsider insourcing. These included:

- the need for higher standards and better services;
- User dissatisfaction;
- Cost considerations;
- Desire for better performance;
- Need for synergy between sections in the local authority;
- Poor performance of contractors.[45]

Information Privacy[46]

For the purposes of the *Privacy Act* 1988 (Cth), an act or practice of an organisation (defined to include an individual) is an *interference with the privacy* of an individual if, inter alia, the act or practice breaches an approved privacy code that binds the organisation in relation to personal information that relates to the individual.[47]

Similarly there is a breach where the organisation is not bound by an approved privacy code in relation to the personal information and the act or practice breaches a National Privacy Principle in relation to personal information that relates to the individual.

---

[43] http://www.apse.org.uk/page-flips/2011/insourcing/files/in-sourcing.pdf
[44] Ibid.
[45] Ibid.
[46] Submission to the Victorian Information and Communications Technology Advisory Committee (VICTAC) *Victorian Government ICT Strategy – Digital by Design – Public Consultation Draft* 17 October 2012
[47] Section 13A(1)(a).

The National Privacy Principle[48] includes a prohibition against a use or disclosure of personal information unless the secondary use, say storage in the cloud, is related to the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.[49] Of course, there is an exception where the individual has consented to the use or disclosure[50]

The issues which arise are:

- whether the storage in the cloud is a secondary use; and
- if it is, whether the individual would reasonably expect the organisation to use or disclose the information in that manner.

In the absence of the individual's consent, the question will be what steps have been taken by the organization (practitioner) to alert the individual that personal information was going to be stored in a cloud facility. Further what inquiry has been made and can it be relied upon, as to the integrity of the security systems in place to protect the privacy of the individual's information.

Document Retention

An effectual document retention structure reduces the risk of:

- Fines imposed by statute and penalties arising from failure to retain documentation;

- Inability to properly evidence conduct or instructions arising from e-discovery requests for old emails or other documents;

- Lost cases resulting from absent email and other business records;

- Business losses from an insufficient archiving and recovery process.

Another aspect of document retention is the possibility of documents remaining in storage facilities, after the provider's service are terminated. This may arise from storage of data at several, possibly international, locations. What steps may be taken in the contract or in preliminary investigations, as to

[48] Schedule 3 of the *Privacy Act* 1988 (Cth).
[49] Schedule 3 of the *Privacy Act* 1988 (Cth) s 2.1(a).
[50] Schedule 3 of the *Privacy Act* 1988 (Cth) s 2.1(b).

whether there will be no retention of any copies of the documentation after service contract has come to an end and another provider is used.

Reporting

Save for situations where the Service Provider is prevented from reporting an ICT security incident, such as steps taken against a US corporation who is the Service Provider under the *Patriot Act*, inquiry should be made as to when and the circumstances in which, the Client is notified of an ICT security incident.

6. What are the specific risks for legal practitioners:

Duty of care & diligence

Duty of care and due diligence will raise at least the following issues from the inherent feature of cloud computing that documents and information are transported to a destination which may be unidentifiable.

Such information or documents may relate either to the administrative side of a practice or to substantive legal matters relating to the conduct of professional work conducted on behalf of clients. In addition they may be exported:

- To a destination or destinations which may or are likely to be outside of the jurisdiction;
- To persons who may be in a contractual relationship with the practitioner, but are for one reason or another 'beyond reach' to enforce those rights;
- To persons who may not be in a contractual relationship with the practitioner, as part of the Service Provider's subcontracting network.

In relation to the second point, they may beyond reach simply by reason of the fact that they may be overseas, but also because there may be a complexity in identifying if the Service Provider was responsible or the extent of the loss.

In the UK, the Solicitors Regulation Authority (SRA), introduced on 13 October 2011, new regulatory requirements and an updated code of conduct. Chapter 4 of the SRA Code provides:

'IB (4.3 you only outsource services when you are satisfied that the provider has taken all appropriate steps to ensure that your clients' confidential information will be protected.' [51]

It is further advised, as expected that the client should be informed in the retention agreement, that outsourcing may take place. The Ethics Committee of the Law Society of England and Wales states:

> 'In addition to taking all necessary steps to ensure information will be kept confidential by third parties, you should ensure that the client is aware, for example through the practice's terms and conditions, that such outsourcing may take place. You should also consider whether specific consent is needed from clients prior to outsourcing taking place.'[52]

One would think that it would be reasonable to be satisfied on the following matters:

- What are the deliverables?
- Does the Service Provider hold insurance and what does in cover?
- Will the Service Provider indemnify the Client against liability, loss, damage, costs of any settlement and legal costs?
- What security measures have are taken to ensure the data stored or provided is accessible to the legal practitioner;
- What security measures have are taken to ensure the data stored is kept confidential;
- What steps are taken by the Service Provider to ensure its officers, employees, agents and subcontractors are aware of, and comply with, the security and safety requirements.
- Warranties which include:
    - 'fit for purpose' type warranties;
    - Correctness of information provided to the Client;
    - That the deliverables may be integrated into and be compatible with the Client's existing systems;
    - That the Service Provider owns or is entitled to the IP Rights associated with providing the deliverables;
    - The use of the deliverables does not infringe any third party IP Rights.

[51] http://www.lawsociety.org.uk/productsandservices/practicenotes/outsourcing/5044.article

[52] Ibid.

Ensuring rights of access to client data

In this regard, it will be of concern how access is treated in the service contract and as a matter of practice. In other words, how might access to the data be blocked:

- By a deliberate action of the Service Provider e.g. a reaction to a failure to make the payments in accordance with the service contract.
- By an interruption to uptime;

In addition, what steps have been taken to ensure that the data is not irretrievably lost, such as by reproduction on other related secure storage facilities.

Document retention

In *Residential Funding Corp. v. DeGeorge Fin. Corp*. 306 F.3d 99 US the plaintiff failed to produce certain emails until after the trial had begun. After judgment for plaintiff, the defendants appealed on one issue: the trial court's denial of their request for an adverse inference instruction. The appeals court held that ordinary negligence was sufficient grounds for an adverse inference instruction arising from the failure to produce the emails.

In the case the appeal court considered several matters which indicated the plaintiff acted in bad faith. The plaintiff encountered difficulties in retrieving the email from backup tapes from October December 1998. For several months the plaintiff made a series of inaccurate or misleading representations about the status of the production and when the email would be produced.

On several occasions the plaintiff indicated it had retained, or was going to retain, an outside vendor to assist with the recovery of email. When defendant offered to attempt the recovery through its own experts, the plaintiff refused to provide the tapes. When the plaintiff, eventually after a number of broken deadlines, did produce emails, none were from the critical time period. The plaintiff explained the void by stating that responsive emails either did not exist or were not accessible.[53]

The appeals court held that the plaintiff's "purposeful sluggishness" was evidence from which the trial court could find that the emails would have been damaging.

[53] http://www.ediscoverylaw.com/2004/12/articles/case-summaries/court-has-broad-discretion-to-fashion-sanctions-for-breach-of-discovery-obligations/

Discovery

It is clear from *Residential Funding* that the inability to produce documents may lead to an adverse inference on the substantive issues. If a client is unable to corroborate a vital aspect of their pleaded case, by reason of the inability to locate or access documents given to the legal practitioner, the failure to make reasonable enquiries regarding security, access and backup, where the client is unaware of the risks taken, would in my view expose the practitioner in tort.

Liens

The retaining lien only attaches to items the property of the client (which for this purpose can include a person who has retained the lawyer on behalf of others).[54] It extends to money belonging to the client held by the lawyer.[55]

However, where the item in question is owned by a third party, no retaining lien can attach to it arising out of the solicitor-client relationship, and the solicitor must *deliver up the item to its true owner* unless the solicitor has some valid security as against the true owner.[56] There is no need for a lien over property that is the *solicitor's property*, as the client has no entitlement to that property in the first place.[57] (emphasis added)

Issues to consider are:

- Delivering documents to the true owner if other than the client may be interpreted as the copyright owner;
- However, a document sent into the cloud and stored, should still be a 'document' over which a lien exists, because a document includes anything from which sounds, images or writings can be reproduced with or without the aid of anything else;[58]

---

[54] Lexis Nexis 'Halsbury's Laws of Australia' at [250-4510], referring to *Re Dee Estates Ltd* [1911] 2 Ch 85 (recognising the right of a solicitor acting for a trustee to maintain a retaining lien over documents prepared on the instructions of the trustee can be asserted against the beneficiaries).

[55] *Legal Profession Act* 2007 s 258. Relevantly: (1) A law practice may do any of the following in relation to trust money held in a general trust account or controlled money account of the practice for a person— (a) exercise a lien, including a general retaining lien, for the amount of legal costs reasonably due and owing by the person to the practice;

[56] Above n 49 referring to *Re Cao* (1996) ANZ Conv R 321 at 324 per Beazley J.

[57] *Sheffield v Eden* (1878) 10 Ch D 291 at 293 per Bagallay LJ.

[58] *Acts Interpretation Act* 1901 (Cth) s 2B.

- If a document is prepared overseas by a third party, the ownership of the copyright in that document resides in the author, subject to any agreement to the contrary;[59]
- Accordingly, there should be an assignment of copyright from the author to the legal practitioner or the client as agreed in that situation.
- If the legal practitioner prepared the document then the same rule applies, however sending it into the cloud arguably includes an implied licence that the Service Provider may reproduce the document in carrying out the storage service on several storage facilities.

Duty of confidentiality

Of course, this will depend on what you plan to use the cloud for. If it is intended to store confidential client information then it becomes critical to ascertain further matters regarding the service:

- How is access gained to the information?
- What security is in place to protect the information:
    - From destruction;
    - Unauthorized disclosure?

These matters give rise to regulatory and professional issues. The American Bar Association has identified ethical considerations in using the cloud.'[60]

Some of the ethical concerns regarding outsourcing are:

- Whether there is a lack of data security and confidentiality of client information, which may give rise to a waiver of privilege;

- Those who provide the legal outsourcing service must be required to observe the ethical standards required of the consumer who retains them;

- The lawyer has a duty to supervise documents prepared in their offices. The duty cannot be less if the lawyer unilaterally chooses to use

[59] *Copyright Act* 1968 (Cth) s 35(2).

[60] American Bar Association publication: http://www.americanbar.org/newsletter/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html
In Opinion 701, the New Jersey State Advisory Committee on Professional Ethics emphasized the lawyer's responsibilities to take affirmative steps to guard against inadvertent disclosures and exercise "reasonable care" against unauthorized access when using cloud services: http://www.americanbar.org/newsletter/publications/law_practice_today_home/law_practice_today_archive/december11/an-update-on-governing-cloud-computing.html

these services onshore or off-shore, particularly to a place where there has been no inquiry as to security, confidentiality restraints or background of the Service Provider.

There are some difficulties associated with this. How does one discharge these obligations when time and distance make constant supervision impossible? Confidentiality agreements with the provider and evidence of qualifications may be required if it is a lawyer off-shore who is conducting the service. There may be a practical difficulty in having larger Service Providers agree to sign confidentiality arrangements regarding the material they store in delivering their service.

These issues of course raise the problem of enforceability and if the confidential information is disclosed without authority the possibility or likelihood of claiming compensatory loss.

Data security & privacy

I refer to the material under the heading *'Information & Privacy'* above.

It seems clear that enquiry must be made by practitioners who have been provided with confidential information by the client, as to what measures are being taken to protect the data from exposure.

The High Court has consistently rejected the concept of the proprietary nature of information.[61] However in respect of an action for breach of confidential information, it is critical that the defendant owes the plaintiff an obligation to keep the information confidential. It is all well to say the service agreement provides for it, but how would one know of unauthorized disclosure, the party responsible and what are the practicalities of enforcement. One element that may or may not apply, is that where copyright is in the client or the practitioner, and the country where an unlawful reproduction has occurred is a convention member to the Berne Convention, enforcement will be in terms of copyright laws similar to our own.

[61] *Victoria Park Racing & Recreation Ground Co Ltd v Taylor* (1937) 58 CLR 479; *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414; *Breen v Williams* (1996) 138 ALR 259.

Preserving legal professional privilege

There are some warning bells coming up in this area when one considers a practitioner's decision to use the cloud for storage or document creation or any other services where a document may have its confidentiality compromised.

The danger arises where a practitioner may have to give evidence in a proceeding. One case reminds us of the potential dangers of practitioners giving evidence in relation to substantive issues in a proceeding.[62]

The background of this case is in patent law however the case has a wider application for practitioners. The patent holder (Servier), sought by motion to amend its patent pursuant to s 105 of the *Patents Act 1990* (Cth). The only evidence in support was provided by the solicitor conducting the matter. In his evidence he stated that he had acquired the knowledge to make the affidavit from his involvement in the proceedings and some records obtained from the patent records of his client.

It was argued that this reliance on the solicitor's recommendations for the application opened the door to further documents ordinarily within the claim for privileged communications.

Bennett J stated the common law principle that a person who was entitled to claim legal professional privilege could waive that privilege. Waiver could be express or implied and was a matter for objective consideration regardless of the intention of the party who has lost the privilege (*Mann v Carnell* (1999) 201 CLR 1 at [29]).

Section 122 of the *Evidence Act* sets out the circumstances in which client legal privilege may be lost. Bennett J observed that the *Evidence Act* applied to the adducing of evidence in proceedings to which the *Evidence Act* was applicable. It did not however apply to pre-trial processes such as discovery or to the production of documents prior to the adducing of evidence (*Mann*; *Esso Australia Resources Limited v Commissioner of Taxation of the Commonwealth of Australia* (1999) 201 CLR 49).

Of telling relevance was an examination of whether there was an inconsistency between the conduct of the client and maintenance of the

[62] *Apotex Pty Ltd (ACN 096 916 148) v Les Laboratoires Servier* [2008] FCA 1466 (Bennett J, 30 September 2008).

confidentiality of the relevant communications (*Mann v Carnell* at [28]). In *Apotex*, it was determined that relying solely on the solicitor's advice to amend the patent and claiming privilege to protect that advice was an inconsistency.

Under the *Evidence Act* (Cth) a client or party is taken to have so acted if:

(a) the client or party knowingly and voluntarily disclosed the substance of the evidence to another person; or

(b) the substance of the evidence has been disclosed with the express or implied consent of the client or party.

In terms of the cloud, the issue will be whether steps have been taken to bind the Service Provider with obligations of confidence (and further to preclude subcontracting unless confidentiality in the same terms are imposed), in relation to material capable of being the subject of confidence.[63]

In other words, the question will be whether there is an implied consent to disclose where there is a total failure to require confidential obligations in the service contract. Will that be enough? Time will tell, but like other areas, acting reasonably in the circumstances will not be satisfied by relying purely on obligations in a written agreement when other factors dictate further enquiry is needed.

7. Conclusion

There are many services available in the cloud, which offer apparent benefits. What is required is 'back-up':

- Back-up plan to recover documents;
- Back-up plan if documents lost;
- Back-up reasons to support your decision to choose *a* service/s;
- Back-up reasons to support your decision to choose *that* service/s;
- Back-up plan to enforce rights.

Dimitrios Eliades
Barrister, Brisbane
22 February 2013

---

[63] See *Maggbury Pty Ltd v Hafele Aust Pty Ltd* [2001] HCA 70; 210 CLR 181 (13 December 2001).