The Legal Standing of Data in a Cloud Computing Environment

Alan Harris

A dissertation submitted in partial fulfilment of the requirements of Dublin

Institute of Technology for the degree of

M.Sc. in Computing (Data Analytics)

May 2012

DECLARATION

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Data Analytics), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: ___________________________________

Date: ***31 May 2012***

ABSTRACT

This research investigates the legal standing of data in a cloud computing environment. Legal uncertainties and conflict between the European Union and the United States over data privacy are hampering the take-up of cloud computing services. Existing research indicates that businesses see the advantages inherent in the adoption of cloud computing services, such as reduced cost of ownership, lower business start-up costs, improved economies of scale etc., however the legal implications of moving data and IT functions into the cloud environment has not been fully thought through. Further take-up of cloud services could mean large volumes of public and commercial data would migrate to servers potentially located outside national borders.

This raises pertinent legal questions; where is the data residing? Who has access to the data? Can I access my data? What jurisdiction's laws apply to the protection of the data, the laws of the jurisdiction where the data resides, or the laws of the jurisdiction where the cloud service was provided?

Businesses are increasingly beginning to see these legal uncertainties as a major issue in cloud computing. In this project a range of laws relating to IT and cloud computing will be examined, as will cloud technologies, and specifically geolocation technology that can assist in ameliorating the jurisdictional issues with cloud adoption. Along with this research, a number of technical and legal experts with experience in the cloud and data protection fields will be interviewed, the ultimate goal being to construct a user guide outlining how pertinent legal issues related to cloud can be understood and mitigated against. This work will also present an integrated country matrix outlining the differing legal perspectives a list of sample countries have in relation to laws affecting cloud adoption. This country matrix will form part of the aforementioned user guide, and will attempt to assist businesses in their endeavour of researching which countries provide adequate levels of protection for data when they are included in a cloud computing environment.

Geolocation technology enables the geographical location of data to be determined. This technology is highlighted in this dissertation as an example of a current technology which can provide solutions to address the legal uncertainties which have arisen with cloud computing. Many modern database systems now include geolocation functionality, and the dissertation will demonstrate how functionality within modern databases can also use geolocation technology to mitigate against the jurisdictional issues that arise when data of a personal nature is stored in a cloud computing environment. The technical and legal experts that were interviewed as part of the research process of this work will evaluate the resulting user guide. Their evaluation will be critical to determine if the guide is suitable for real world environments, and if not, hopefully indicate where the guide falls short of its intended objectives and where it can be improved.

Results suggest that the integrated solutions may provide certainty and clarity to the legal uncertainties pertaining to data privacy in the cloud computing environment.

Key words: personal data, cloud, cloud computing, security, legal

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to my supervisor, Damian Gordon. Without Damian's help this dissertation would never have been started, let alone completed. Damian provided invaluable direction, guidance and encouragement throughout the dissertation process. Thanks too to Brendan Tierney who gave vital technical assistance at a critical point in the dissertation.

I would also like to thank each of the technical and legal experts interviewed as part of the dissertation process, these individuals gave invaluable insight into cloud technology and law, which helped inform the literature review and experiment elements of this dissertation.

Finally I would like to thank my wife, Michelle. Having not only given birth in early February, Michelle then reared two children under the age of two single-handed throughout the entire final M.Sc. semester. And often decamped (with children!) to relatives in Cork/Meath/Down, in order to give me space and time to complete this work. Thanks for all your unending support Michelle.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1 Background - What is Cloud Computing?

Cloud Computing is the concept whereby computing is seen as a service, that is delivered to customers over the Internet, from large-scale data centers, or 'clouds'. Cloud computing has been a dominant emerging technology over the last decade. Within a cloud environment, computing is seen as a utility comparable to other utilities such as electricity or gas. Within a cloud computing environment, customers need only pay for the actual services they use, cloud resources can be billed on a pay-as-you-use basis, and this makes the technology attractive. For example, companies with large batch-oriented tasks can get results as quickly as their programs can scale, using 100 servers for one hour costs no more than using one server for 100 hours. Businesses that may only have seasonal demand for their products no longer need to outlay huge sums on an IT infrastructure they may only require for a few months of the year, instead they can avail of a cloud service which allows them draw down the necessary computing resources only when they are required.

Figure 1.0 from Wikipedia demonstrates the cloud computing environment, cloud computing refers to both the applications delivered as services over the Internet and the infrastructure and Platform software in the data centers that provide those services.

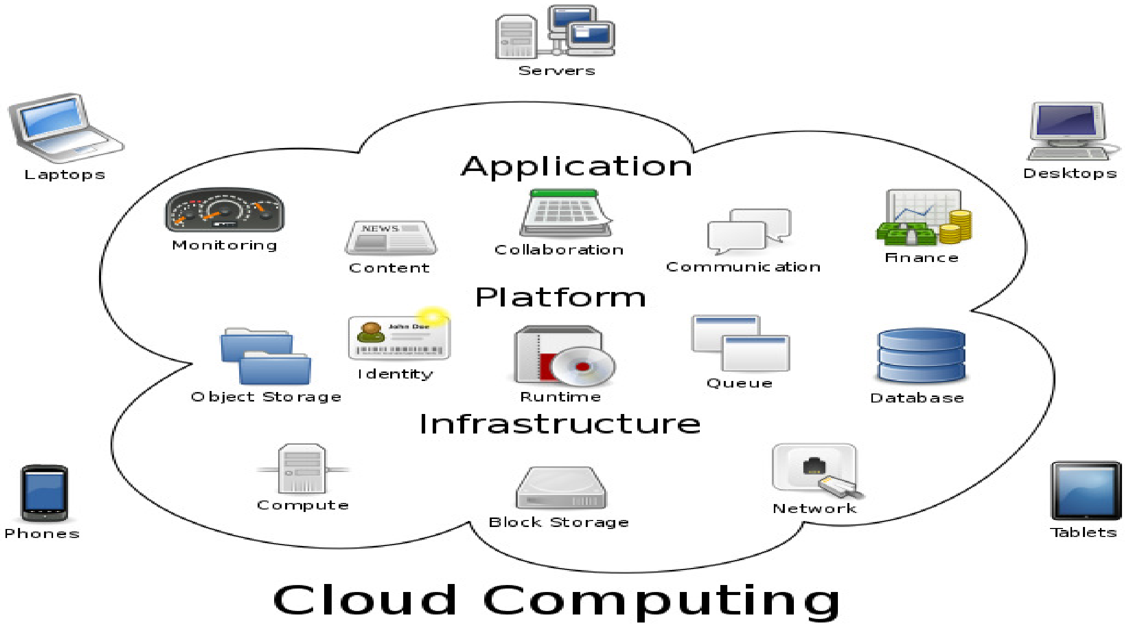


Figure 1.1: Cloud http://en.wikipedia.org/wiki/File:Cloud_computing.svg

Three main services are available from cloud vendors; Infrastructure as a Service (IaaS), a provision model whereby the vendor's IT infrastructure is made available to the customer on a needs basis, Software as a Service (SaaS), again a pay-per-use costing model whereby software applications are leased out to contracted organisations and Platform as a Service (PaaS), a category of cloud computing services that provide a computing platform and a solution stack as a service.

There are 4 main types of Cloud environments;

1. A *Public Cloud* is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the client over the Internet.

2. A *Private Cloud* infrastructure operates in a similar manner to the public cloud with the exception that the private cloud is intended solely for a single organisation.

3. *Hybrid Clouds* involve a combination of private and public cloud infrastructures. An organisation might normally use the services of a private cloud only, but for certain less secure operations, or in times of intense business activity might need to 'burst out' and avail of services in a public cloud.

4. *Community Clouds* arise when a 'community' or group of organisations with similar needs or interests (such as compliance considerations, security requirements) come together to share resources in a cloud environment. The cloud is not public, as it does not provide commercial services to public companies.

Cloud computing technology does provide businesses with many attractive computing options. It is not however without its pitfalls. Of concern to many organisations is the question of security within the cloud environment. Security questions include; in a cloud environment who has access to data, where is the data located, how secure is the data, what happens in the case of a disaster.

The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive which regulates the processing of personal data within the European Union. It is an important component of European Union privacy and human rights law.

The right to privacy is at the heart of this legislation, and with respect to the privacy of an individual's personal data, the directive incorporates the following 7 principles;

1. **Notice**—data subjects should be given notice when their data is being collected.
2. **Purpose**—data should only be used for the purpose stated and not for any other purposes.
3. **Consent**—data should not be disclosed without the data subject's consent.
4. **Security**—collected data should be kept secure from any potential abuses.
5. **Disclosure**—data subjects should be informed as to who is collecting their data.
6. **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data.
7. **Accountability**—data subjects should have a method available to them to hold data collectors accountable for following the above principles. (Shimanek 2001)

These 7 principles complicate the standing of data in a cloud computing environment, and as Hon points out, in particular article 4 of the directive requires member states to apply data protection rules to controllers who process personal data whether that controller is established in the EEA (European Economic Area (the European Union plus Iceland, Liechtenstein and Norway)) or for the purposes of processing data makes use of equipment situated in the EEA (Hon *et al.,*2011)

And as Hon says (Hon *et al.,*2011) "*Cloud users don't necessarily know in which data centers or even countries their data are stored or where their processing operations are run, or which sub-providers are used by the provider with whom they have the direct relationship. Indeed, even cloud service providers who use other providers' resources (e.g. a SaaS service layered on IaaS or PaaS) may not necessarily know which data centers or countries are involved.*"

Although cloud computing is seen as a panacea for many business/IT issues, the legal questions it raises (particularly around the whereabouts of personal data) certainly warrant further research and analysis to see if these issues can be quantified and assessed.

Geolocation technology has become more and more prevalent over the last few years, this is technology that enables an individual determine the geographical location of another party. Geolocation is being used widely by Internet companies to determine the exact whereabouts of web users, these companies can then tailor content for those users based on their geographical location.

Modern Database systems are also beginning to tag data with geolocation information, enabling users determine where their data has resided, and this is similar in a way to how modern electronic photographic files can contain GPS information if the camera device supports GPS technology. An informed user can determine the location where a photograph was taken by accessing the GPS information tagged to the image file. Determining not only the location of where data has been, but where data *is* currently residing and investigating ways of preventing data being moved to jurisdictions outside the scope of a cloud contract are important goals of this research.

1.2 Description

This research investigates the legal standing of data in a cloud computing environment. The legal status of data in a public cloud environment is currently unclear. For example, if an organisation today agrees to put data into a public cloud, and that data is stored in a data center outside the legal jurisdiction of the organisation, legal and data protections issues arise.

European Union data protection laws (Directive 95/46/EC specifically) regulate the processing of personal data within the European Union. Some important aspects of the law ensure citizens have a right to access their data, and that their data be kept safe and secure. If confidential data is put into a cloud environment, how do customers know where this data resides, how can they be confident the data is safe and secure? This dissertation will evaluate these uncertainties, in an attempt to construct an integrated user guide on the legal uncertainties of data in the cloud.

This project will identify several legal experts with experience in the legal issues affecting cloud computing, and several technical experts will be identified who have experience consulting and advising on cloud technologies. Each of these candidates will in turn be interviewed. A serious of questions will be constructed in order to understand the legal and technical issues with cloud computing. These questions will be put to the legal and technical experts. Questions will be designed to determine what level of knowledge companies have of cloud computing, are companies using cloud computing services or considering availing of some cloud services, and do companies know of the legal uncertainties cloud computing causes in relation to the protection and security of personal data.

The results of the interview sessions, along with the literature review will assist in the formulation of an integrated solution to the legal uncertainties pertaining to cloud computing. It is envisaged this integrated solution will be in the form of a User Guide, informing business of ways to go about mitigating against legal issues relating to personal data in the cloud.

This project will attempt to evaluate if technical solutions can be developed to help solve the legal uncertainties that persist when data is moved to a cloud computing environment. Most modern relational database systems can add geolocation tags to data. This information provides exact GPS co-ordinates on the location of the data.

This research will investigate geolocation tagging technology, and determine whether this or a related technology can be used to at least over-come some of the data protection legal uncertainties.

Cloud computing experts, identified in the interview process will be interviewed a second time in an effort to evaluate the suitability of the integrated solution, and it is expected they will be able to able to critique whether the artefact produced from this dissertation is worthy of further research and development.

There will be two key deliverables from this research, the dissertation document, and a User Guide on the legal issues in cloud computing. The user guide will provide practical advice and recommendations to businesses on the legal issues relating to cloud computing. The guide offers practical advice under three headings:

1. **Education** – What is the pertinent legal information businesses should be familiarising themselves with prior to carrying out a migration of data to the cloud.

2. **Technology** – What technical means can be availed of to mitigate the legal issues with cloud computing.

3. **Business** – What business processes should be in place to ensure the legal pitfalls in the adoption of cloud services can be avoided.

The industry experts will be able to be able to evaluate the suitability of the user guide, and it is expected they will be able to able to critique whether this artefact is worthy of further research and development.

1.3 Aims and Objectives

The aim of this project is to evaluate the legal standing of data in a cloud environment, and to assess the data protection issues which arise with cloud computing.

In this dissertation a range of laws relating to IT and cloud computing will be examined, as will cloud technologies, and specifically geolocation technology that can assist in ameliorating the jurisdictional issues with cloud adoption. By interviewing a number of technical and legal experts with experience in cloud it is expected the project will identify a wide range of issues affecting cloud computing.

The dissertation will put forward an integrated solution to address the legal uncertainties that have arisen with cloud computing, the validity of the approach suggested will be evaluated by demonstrating it to the aforementioned industry experts, and their reaction and criticisms will be used to determine if the approach used merits further research.

The dissertation will identify what legal standards are being applied to cloud computing contracts, if such standards actually exist, and their content will be examined to see if it holds up to legal scrutiny.

The dissertation will also examine what legal issues arise when moving data between jurisdictions.

1.4 Project Scope and Limitations

The breadth of the literary research of this work is enormous, areas touched on include The Law, IT Law, Cloud Law and Cloud Computing. Other paragraphs delve into the different perspectives countries have on cloud computing, others touch on Geolocation and Database technologies. Any one of these sections could become the subject of an MSc. Dissertation in their own right. Moreover this paper is restricted in length and time. Therefore the dissertation manages to only lightly touch the pre-mentioned topics. The dissertation is attempting to understand the legal standing of data in a cloud computing environment. This will necessitate a look at the law in general, and then how the law is applied to IT and specifically Cloud Computing situations. The areas of law that cloud computing affects will be analysed. Based on the literature review and interview process, solutions to only the most common and important legal issue relating to cloud will be catered for. It will be impossible to provide an integrated solution to all legal issues affecting cloud.

Chapter 5 of this work will attempt to provide a 'Cloud Country Matrix', an analysis of the laws and regulations some countries have in place that affects cloud computing. This matrix will be incorporated into the integrated solution to the legal issues affecting cloud. It will be impossible though to examine different perspectives on cloud computing for more than 6 countries.

Chapter 8 of this work will attempt to demonstrate how a modern database system can use existing technology in an attempt to solve some of the legal issues affecting cloud technologies, namely the jurisdictional issues relating to personal data. One database vendor and the technology inherent to that vendor are demonstrated. It would go beyond the scope of this work to demonstrate how all modern database systems in the market place could provide technologies to cater for jurisdictional issues with cloud computing.

1.5 Summary

The legal implications of storing and moving personal data within a cloud computing environment are unclear. European legislation, such as Directive 95/46/EC regulates the processing of personal data within the European Union. The distributed nature of cloud computing though, potentially availing of computing resources in multiple jurisdictions to deliver the cloud service seems to contradict with some elements of the aforementioned European legislation. This dissertation via literature review and an interview process will endeavour to understand the pertinent legal issues concerning personal data in a cloud computing environment. Solutions to these legal issues, drawn from multiple disciplines will then be drafted, culminating in the production of a User Guide, an integrated solution to the legal issues affecting cloud computing. The solution will need to be evaluated, and it is expected that the legal and technical experts used in the interview process, will again be called upon to critique the artefact component of this work.

Finally this work is restricted by content length and time constraints. To that end it will be impossible to provide solutions to all the legal issues affecting cloud computing. Nor will it be possible to demonstrate different perspectives on cloud computing for more than six countries. Regarding the technical solutions put forward by this work: time and content length again mean this section of the dissertation will only be able to focus on one main technological solution, i.e. Geolocation technology, and with respect to how this functionality can be facilitated in databases, only Oracle's relational database will be examined.

2. CLOUD COMPUTING

2.1 Introduction

Developments in the ICT sector in recent years; higher internet connection speeds, reduced cost of mass storage and processing devices, advances in virtualisation technology, the proliferation of portable computer devices, the advent of Service Orientated Architecture, these have all helped lay the foundations for cloud computing. Moreover, the popularity of new business models such as Web 2.0, utility computing and Software as a Service have also assisted in readying the business environment for cloud's particular business delivery model.

It is important at this juncture to offer a concise definition of cloud computing, several definitions abound, but for the purpose of this dissertation the definition of cloud computing put forward by the National Institute of Standards and Technology is used;

"Cloud computing is a 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."

Cloud computing is purported to offer many things; computing as a utility, on-demand resource scalability, on-demand provisioning with little or no up-front IT infrastructure investment (Shimba 2010), elasticity of resources (Armbrust *et al.* 2009), ubiquitous access, high reliability (Buyya *et al.* 2008). Cloud computing certainly represents a paradigm shift in terms of how IT services of the future will be provisioned, charged for and managed. The adoption of cloud technology services by business will also lead to fundamental changes in how in-house IT departments work. It may also be a watershed moment for how businesses intend to treat confidential data when they move that data into a cloud environment.

This chapter attempts to chart the origins of cloud computing, the fundamental elements which needed to be in place in order for cloud computing to come to the fore and flourish will be discussed. There will also be analysis of cloud technologies which dominate the ICT industry, the leading players in the cloud sphere will be highlighted and the marketing strategies these companies have adopted to launch cloud will be explored. The chapter will end by looking at a cloud adoption case study, which will demonstrate how cloud computing has proved to be an invaluable technical solution in the business arena.

2.2 History of Cloud Computing

Cloud computing, or more accurately, the concept whereby computing could be sold like a utility, such as electricity or gas, was first suggested by computer science pioneer John McCarthy, an MIT professor, as far back as 1961. At that point in history the concept was well ahead of its time since the technology was simply not ready for cloud computing. Several pieces of infrastructure and technological breakthroughs needed to come into being before cloud computing could thrive.

The Internet underpins the cloud environment and gives the technology one of its unique selling points, available anywhere, anytime, on practically any portable device. The Internet only really came into being in as a commercial entity in the late 1980s. It was then that Internet service providers (ISPs) began to emerge offering connectivity to and storage capacity on the Internet. Another architecture which underpinned the advent of cloud computing was grid computing, coming to the fore in the mid 1990s, Grid computing was initially driven by large-scale, resource (computational and data)-intensive scientific applications that required more resources than a single computer (PC, workstation, supercomputer, or cluster) could have provided in a single administrative domain (Buyya *et al.* 2008). Virtualisation technology, whereby computer power can be represented as a logical entity (Bhattacharjee 2009), has been critical to the growth of cloud computing too. Virtualisation has existed in one form or another since the days of the IBM mainframe, but recent offerings of virtualisation from VMware and Oracle, where different operating systems can be housed on the same physical box has really been a boon for the cloud providers (Bhattacharjee 2009).

Other pieces of the cloud computing puzzle included the so-called *dot com bubble*, which brought about the use of data centers for many organisations. After the *dot com bubble* burst in the early noughties these data centers became under-utilised, and this led to the new advances in virtualisation technology, and thus the birth of modern day cloud computing (Bhattacharjee, 2009).

It is difficult to attribute the first cloud offering to any one particular individual or organisation. Shimba suggests though that the first attempts at cloud computing were in 1999 when Marc Andreessen founded the LoudCloud company which was to build the web's next power play: "*custom-designed, infinitely scalable sites that blast off a virtual assembly line.*" The company Shimba adds intended to be a managed service provider. It was the first company to offer services that are now called Software as a Service (SaaS) using an Infrastructure as a Service (IaaS) model (Shimba, 2010).

Other authors attribute the cloud offering of Amazom.com, Amazon Web Service in 2006, as being the first fully commercialised offering of a cloud services. Today many major software vendors such as Oracle, Microsoft, Google and more offer a host of cloud offerings, right across the cloud service spectrum.

2.3 Cloud Technologies and Services

The cloud environment is dominated by three main service delivery models; Infrastructure as a Service (IaaS), platform-as-a-service (PaaS) and software-as-a-Service (SaaS). It delivers these services through four deployment models; public cloud, private cloud, community cloud and hybrid cloud (CSA, 2009).

2.3.1 Delivery Models

IaaS is the foundation layer on which other service models are built. In this service model, dedicated resources are provisioned to the customer, allowing them to deploy applications in the cloud and run other arbitrary software. This software can include operating systems. Badger *et al.* explains that the consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (Badger *et al.* 2011). Figure 2.1 from tecires.ecs.soton.ac.uk shows the different cloud delivery models and depicts the level of control customers have as they move up or down the delivery model stack.

PasS is the middle layer in the delivery model stack. Customers will be able to deploy their own applications and have control over those, using programming languages and tools supported by the cloud provider. The customer will generally have less control of the cloud infrastructure than with the IaaS delivery model. Examples of PaaS services offered by cloud vendors are Google's App Engine, Salesforce.com's Force.com and Microsoft's Azure.

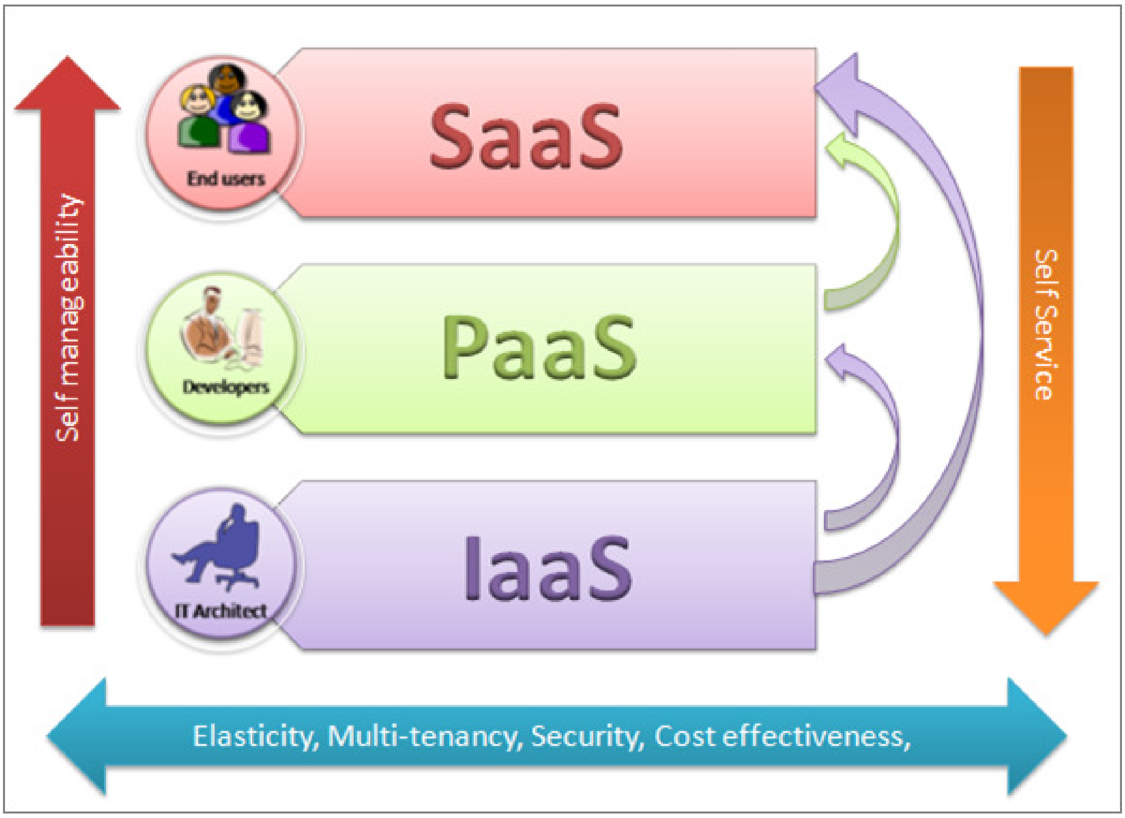


Figure 2.1: Cloud Service Delivery Models (tecires.ecs.soton.ac.uk)

SaaS is probably the most widely used, mature and known service type. It can be defined as a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet (Gray 2010). Badger *et al.* comment that with this service model, the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (Badger *et al.* 2011).

The CSA explain that this layer is built upon the underlying IaaS and PaaS stacks; and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the application(s), and management capabilities (CSA 2009). The most common known examples of SaaS include Salesforce.com, NetSuite, Google's Gmail and SPSCommerce.net.

2.3.2 Deployment Models

Four core deployment models for cloud deployment exist, regardless of the service or delivery model (IaaS, PaaS or SaaS) adopted. These deployments models are public cloud, private cloud, community cloud and hybrid cloud (CSA 2009).

Public cloud – In this model the cloud provider makes resources, such as email applications and file storage, available to the general public over the Internet. Usually the most in-expensive deployment model from a customer perspective, in many cases, services are made available with a pay-as-you-go model of payment.

Ahronovitz *et al.* notes a Public Cloud does not mean that a user's data is publicly visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions (Ahronovitz *et al.* 2010). Figure 2.2 depicts the Public Cloud deployment model, demonstrating how multiple cloud services can be provided by one cloud vendor to multiple customers.

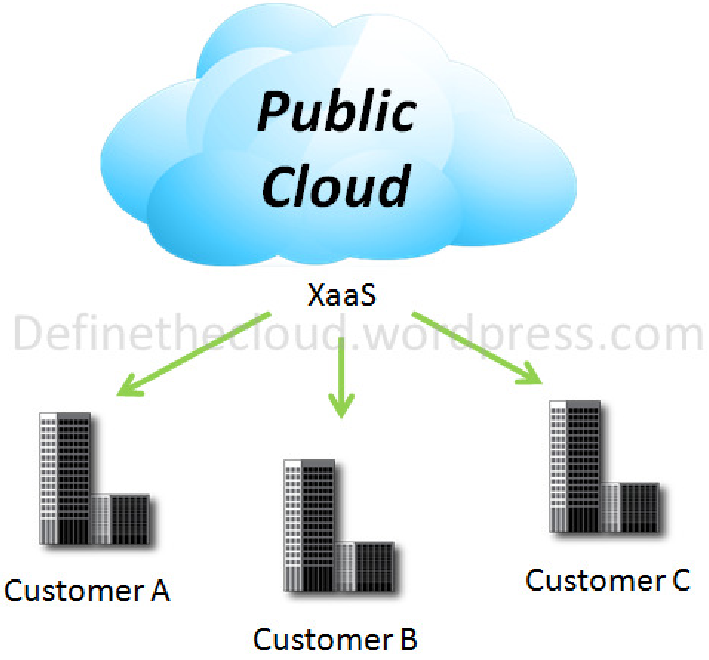


Figure 2.2: Public Cloud (www.definethecloud.net)

Private Cloud – with this deployment model, the cloud environment is usually a proprietary network or data center that uses cloud computing technologies, such as virtualisation. This type of deployment model offers many of the advantages of the public cloud model, but without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail (Ahronovitz *et al.* 2010). A private cloud is managed and maintained by the organisation it serves. Figure 2.3 represents the Private Cloud model, in which the 'cloud' or more accurately, cloud type technologies and services are maintained within a single organisation, to exclusively serve that organisation.

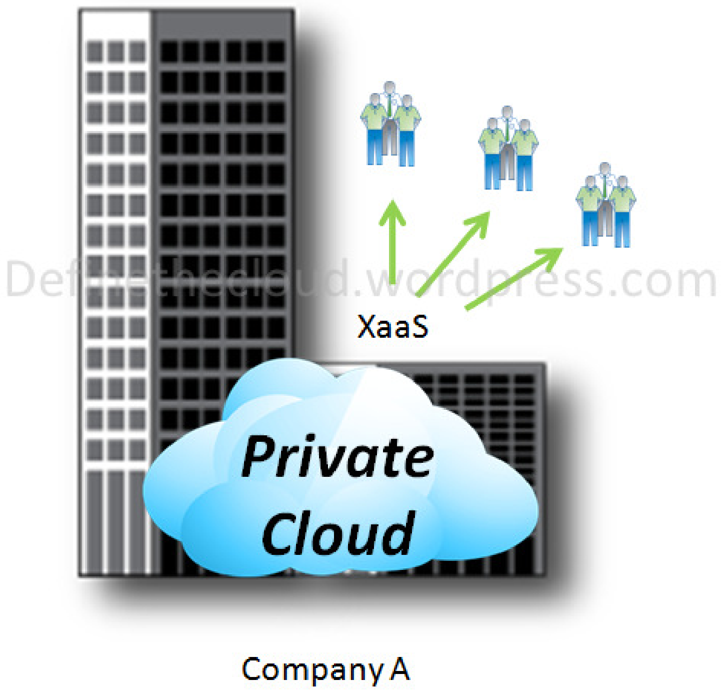


Figure 2.3: Private Cloud (www.definethecloud.net)

Community Cloud – As the name suggests, the community cloud deployment model arises when a 'community' or group of organisations with similar needs or interests (such as compliance considerations, security requirements) come together to share resources in a cloud environment. The cloud is not public, as it does not provide commercial services to public companies. The community cloud is controlled collectively by the group of organisations that have established it. Figure 2.4 demonstrates the Community Cloud, showing how multiple entities can share a cloud infrastructure that serves the common interests of the group.

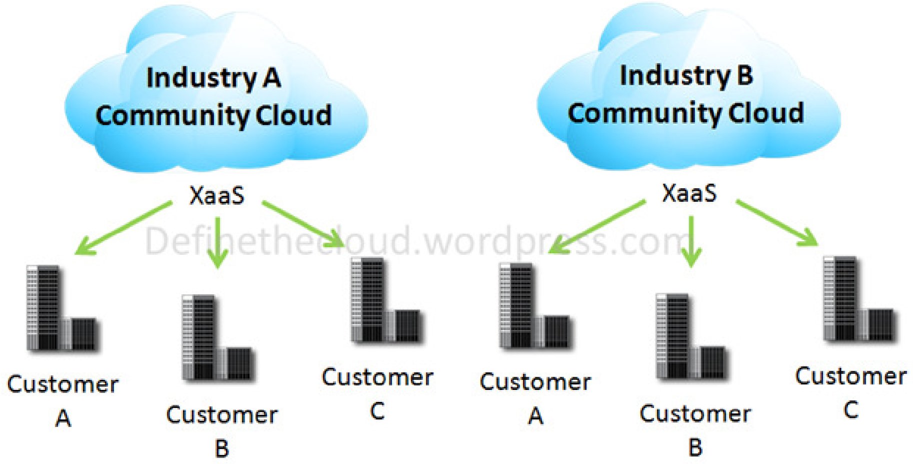


Figure 2.4: Community Cloud (www.definethecloud.net)

Hybrid Cloud – The final deployment model, the Hybrid Cloud, as the name suggests is a deployment model that incorporates multiple cloud deployment types that interoperate. In this model users typically outsource non-business critical information and processing to the public cloud, while keeping business-critical services and data in their control (Ahronovitz *et al.* 2010). Figure 2.5 depicts the Hybrid Cloud model, where multiple cloud deployment models, typically Public and Private Cloud models combine to serve the organisation's different requirements.

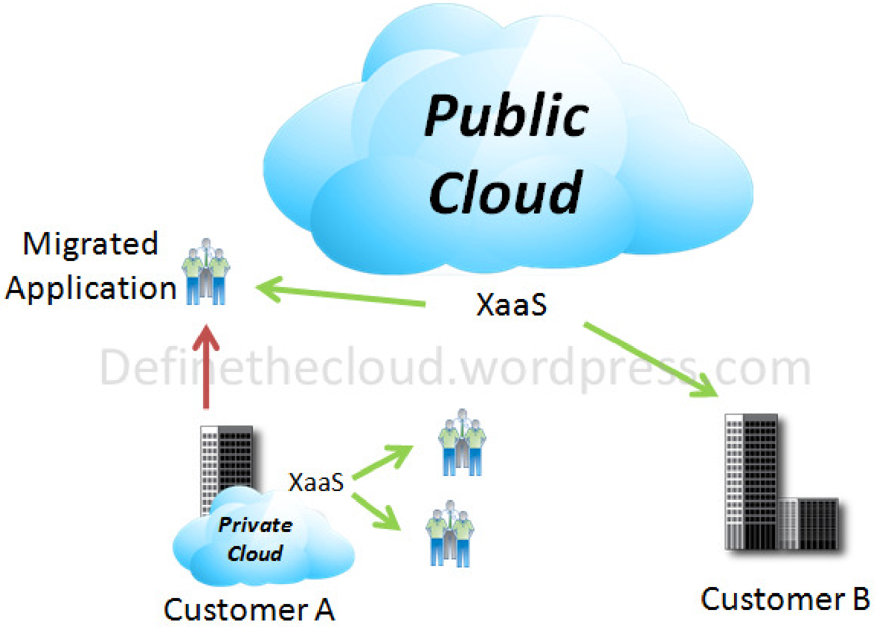


Figure 2.5: Hybrid Cloud (www.definethecloud.net)

2.4 Players in the Cloud Computing Environment

The sheer number and diversity of companies now ‘in the cloud’ is reminiscent of other big shifts in IT, when suddenly everyone latches onto the latest thing (techtarget.com 2009). The dominance of key players in the cloud environment is clearly demarcated based on the services those vendors are offering (IaaS, PaaS or SaaS).

IaaS, providing server and storage computing is the most widely used cloud service, and this market is dominated by Amazon and Rackspace. Cloud analytics site, jackofallclouds.com continues to carry out analysis on the domination of the cloud space by particular cloud vendors. Figure 2.6 represents recent figures on the top five hundred thousand web sites (publicly facing websites) as listed by Quantcast.com. jackofallclouds.com ran this list through web scanning tools in order to determine what IaaS service provider was providing hosting facilities for these sites. Figure 2.6, the most recent figures to date, demonstrate how Amazon’s EC2 service and Rackspace Cloud Servers dominates the sector.

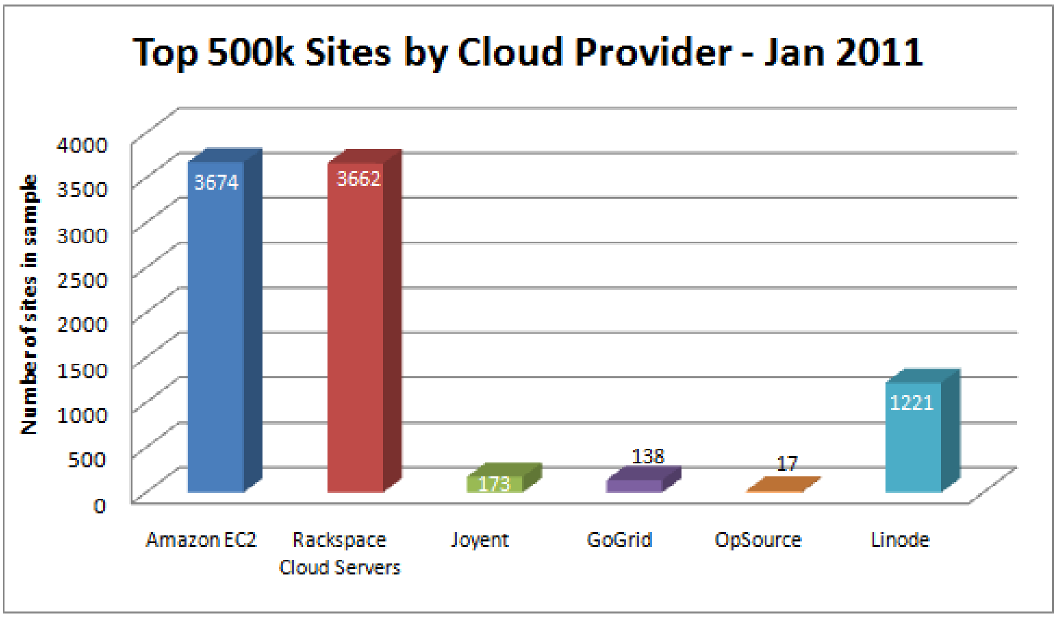
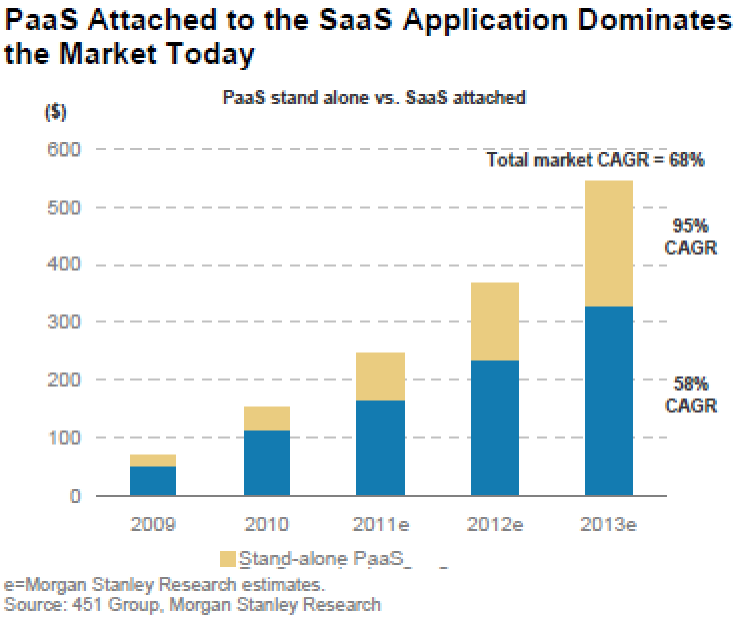


Figure 2.6: Who dominates the IaaS market place? (jackofallclouds.com 2011)

Amazon, or Amazon.com is an American multinational electronic commerce company founded in 1994, Amazon began life as an on-line bookstore, but in 2006 ventured into the cloud computing environment when it realised it could put idle computer power in its data centers to better use. Amazon’s EC2 (Elastic Compute Cloud) IaaS offering provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.

Rackspace US, Inc. is an American IT hosting company founded in 1998. Its experience at hosting web sites over the last 16 years has given it ideal knowledge and experience at providing IaaS cloud services.

The PaaS market, where customers can deploy their own applications and have control over those, using programming languages and tools supported by the cloud provider is dominated by 2 key players; Salesforce (Force.com) and Microsoft (Windows Azure). Morgan Stanley suggests that to date, the majority of the demand for PaaS has been building out additional functionality around existing SaaS applications (morganstanley.com 2011). Therefore the businesses that dominate this sector of the market are sure to have a large presence in the SaaS environment too. Figure 2.7 from morganstanley.com demonstrates how PaaS offerings attached to SaaS offerings dominate the market;


PaaS Attached to the SaaS Application Dominates the Market Today

PaaS stand alone vs. SaaS attached

e=Morgan Stanley Research estimates.
Source: 451 Group, Morgan Stanley Research

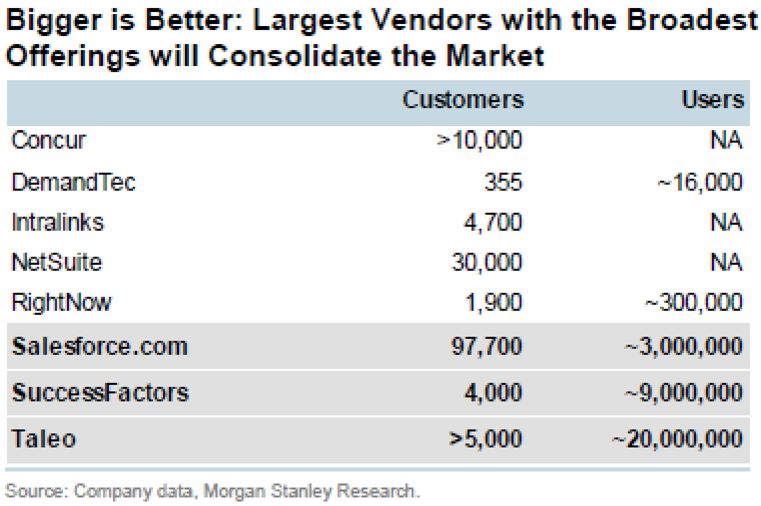
Figure 2.7: PaaS combined with SaaS applications (morganstanley.com 2011)

Salesforce.com a global enterprise software company, founded in 1999 specialises in SaaS, and are most widely known for their CRM solutions.

Microsoft.com probably needs no description, founded in 1975, is the world's biggest computer software company, Microsoft entered the cloud environment in 2009, with their Assure offering.

Interestingly morganstanley.com suggests that the dominance of players in the PaaS sector will be greatly influenced by the ability those PaaS vendors have in attracting application developer to their platforms. As PaaS transitions from primarily being a development environment for add-on functionality attached to existing SaaS applications to a standalone development and deployment platform for creating new standalone applications, the ability to attract developers will ultimately play a significant role in separating the winners from the losers (morganstanley.com 2011).

The SaaS market place has been touched on briefly in relation to PaaS, but Microsoft as yet does not seem to be a major player in this sector. Instead, and again according to morganstanley.com Salesforce.com and SuccessFactors command this area of cloud services. SuccessFactors, again another American company, founded in 2001, specialises in Human Resource management systems. Figure 2.8 from morganstanley.com shows the number of customers and users of the leading SaaS vendors.



Bigger is Better: Largest Vendors with the Broadest Offerings will Consolidate the Market

	Customers	Users
Concur	>10,000	NA
DemandTec	355	~16,000
Intralinks	4,700	NA
NetSuite	30,000	NA
RightNow	1,900	~300,000
Salesforce.com	**97,700**	**~3,000,000**
SuccessFactors	**4,000**	**~9,000,000**
Taleo	**>5,000**	**~20,000,000**

Source: Company data, Morgan Stanley Research.

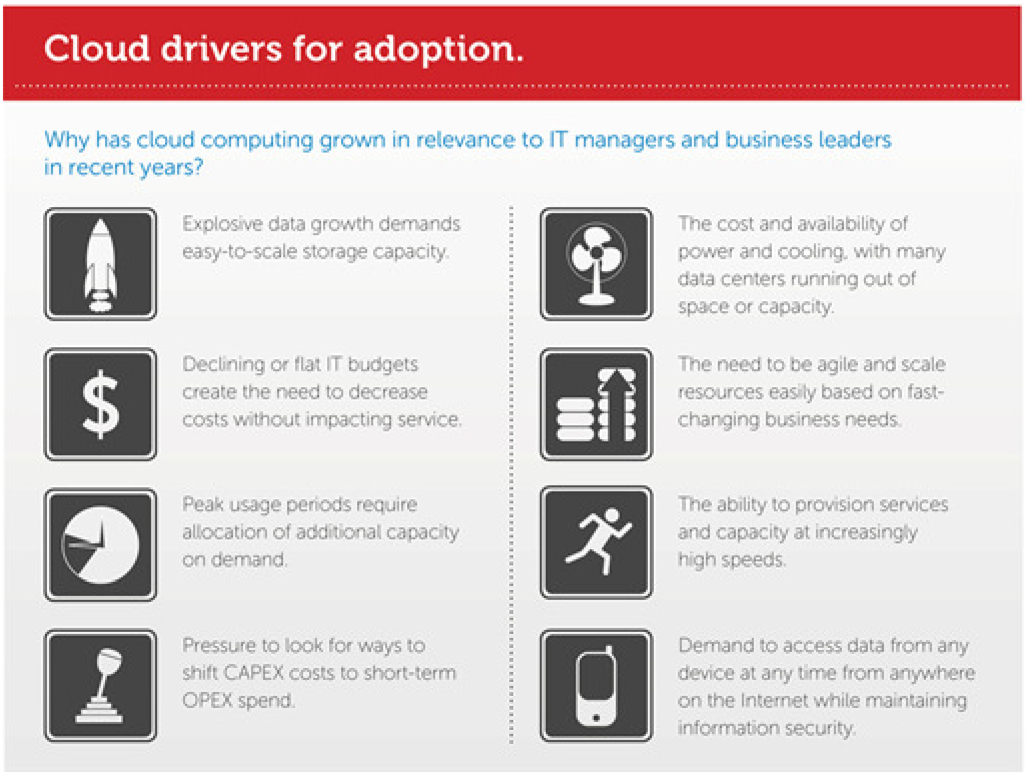
Figure 2.8: Leading SaaS players (morganstanley.com 2011)

The best-positioned companies of the next generation of SaaS will be defined by two dimensions: 1) vendors best able to consolidate application functionality onto their platforms while accelerating end user penetration, and 2) vendors playing in application markets most ripe for moving to SaaS (morganstanley.com 2011).

2.5 Business and Marketing in Cloud Computing

Cloud computing has been a welcome lifeline for IT marketeers in the last 5 years, struggling to encourage businesses to part with money from ever reducing capital expenditure budgets. The great marketing hype surrounding cloud computing though promises cost *savings*, suddenly IT manager's ears are pricked. The marketing documentation continues; reduce in-house IT expenditure, easy storage and maintenance, improve internal communications, accurate real-time information, improve customer relationship management, for new start-ups, no up-front infrastructure costs and on. Perhaps not surprisingly little marketing material refers to the security and legal risks inherent with cloud, vendor lock-in, data protection etc.

The following figure 2.9 from cloudtweaks.com demonstrates the drivers for cloud adoption driven by marketing departments, emphasising why cloud computing has grown in relevance in recent years;



Cloud drivers for adoption.

Why has cloud computing grown in relevance to IT managers and business leaders in recent years?

Explosive data growth demands easy-to-scale storage capacity.

Declining or flat IT budgets create the need to decrease costs without impacting service.

Peak usage periods require allocation of additional capacity on demand.

Pressure to look for ways to shift CAPEX costs to short-term OPEX spend.

The cost and availability of power and cooling, with many data centers running out of space or capacity.

The need to be agile and scale resources easily based on fast-changing business needs.

The ability to provision services and capacity at increasingly high speeds.

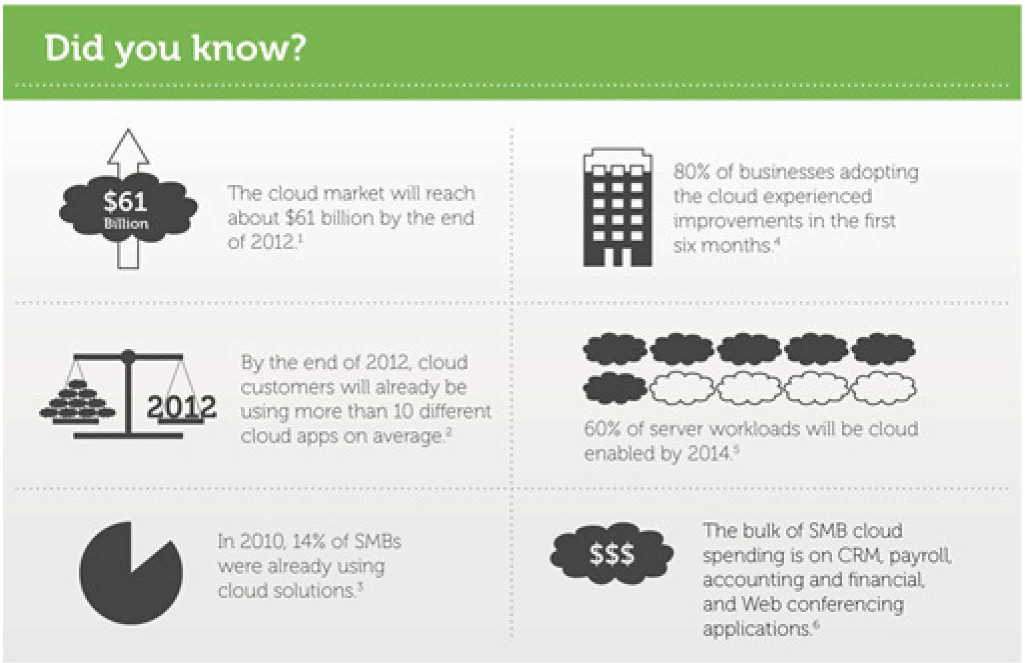
Demand to access data from any device at any time from anywhere on the Internet while maintaining information security.

Figure 2.9: Cloud Drivers (cloudtweaks.com 2012)

The cloud rhetoric seems to be summed up succinctly by Cloudmarketing.org "*The nuance of Cloud Computing and Software as a Service (SaaS) has changed the way* *businesses manage their infrastructures in innumerable ways. By outsourcing corporate software/hardware infrastructure and the manpower necessary to develop and maintain it, companies are able to incur fewer overhead costs. Thus, it is easier for companies to focus more on day-to-day business activities instead of internal upkeep*" (Cloudmarketing.org 2012). In the beginning though, not everyone was convinced; in 2008, Oracle founder and CEO, Larry Ellison delivered the following gem at Oracle OpenWorld;

"*The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?"...."We'll make cloud computing announcements. I'm not going to fight this thing. But I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads. That's my view.*"(Reiner D, 2011).

Gibberish or not, the graphic below in Figure 2.10, contends that the cloud computing market will be worth $61 billion by the end of 2012.



The cloud market will reach about $61 billion by the end of 2012[1]

80% of businesses adopting the cloud experienced improvements in the first six months[4]

By the end of 2012, cloud customers will already be using more than 10 different cloud apps on average[2]

60% of server workloads will be cloud enabled by 2014[5]

In 2010, 14% of SMBs were already using cloud solutions[3]

The bulk of SMB cloud spending is on CRM, payroll, accounting and financial, and Web conferencing applications[6]

Figure 2.10: Did you know? (cloudtweaks.com 2012)

For organisations today though, migrating to the cloud is as much a technology decision, as it is a business decision. There are trade-offs involved, which like the legal issues mentioned earlier include lesser control, bigger security vulnerability surface area and higher operating expense with the cloud migration. Viswanathan makes the point that moving to the cloud and picking the right strategy has to be made with a strong understanding of the enterprise's business model. However, we don't have a formal decision making framework to enable the enterprises to pick the direction in a more objective way (Viswanathan 2012).

Following up on Viswanathan's assertion regarding a formal decision making framework, Gartner further highlights the need for such a tool; prospective benefits need to be examined carefully and mapped against a number of challenges, including security, lack of transparency, licensing constraints and integration needs. These issues create a complex environment in which to evaluate individual cloud offerings (itwire.com 2012). Marketing hype or not, there is no doubt cloud computing has attracted huge attention in recent years. It has the potential to change the way businesses work, it will spawn thousands of start-ups, no longer put off by high infrastructure costs. But it will present challenges too. Figure 2.11 from zdnet.com summarises the dilemma businesses will face as they venture into the cloud mist;

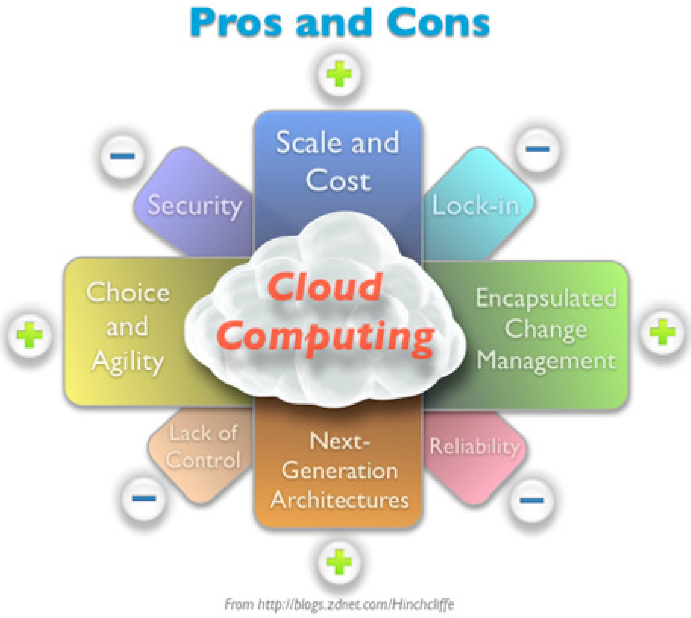


Figure 2.11: Pros and Cons (zdnet.com 2009)

2.6 Case Studies in Cloud Computing

In the previous section, many promises made in relation to the improvements cloud brings to businesses were mentioned. The following cloud computing case study demonstrates a real world example of how a large financial company used cloud services to address multiple business problems, the firm hope that over time this investment in cloud will promote innovation and increase productivity and decision-making.

2.6.1 The Company

Banco Bilbao Vizcaya Argentaria (BBVA) is a multinational Spanish banking group. The group has their headquarters in Bilbao, Spain, but has staff numbers tipping 110,000, located in 26 different countries around the world from Panama to Japan, Venezuela to France and Russia.

2.6.2 The Problem

Due to BBVA's high staff numbers, located in such disperse locations around the world, staff communication and collaboration was a problem. Decision-making was slow, different stakeholders needed to wait days on decisions made by others in order to take action. Productivity was an issue. Staff duplicated tasks. There had been a siloed and federated approach to the company's IT infrastructure and systems around the world. This resulted in information necessary to core business decisions being difficult to access and update. Innovation suffered. Much of the banks computing needs had moved to mobile devices, smart phones, tablet computers, laptops and home computers. Staff found it difficult accessing company IT systems from their mobile devices.

BBVA's director of innovation, Carmen Herranz, said "*The main goal is to promote innovation and making decisions and increase productivity. We are in a challenging market and need to make faster and more accurate decisions... and eliminate duplication*" (Weber 2012).

2.6.3 The Solution

In an agreement with Internet giant Google, BBVA has adopted Google's cloud-based collaboration and communication suite, Google Apps for Business, to increase productivity and drive innovation. Over 35,000 BBVA workers in Spain will initially use the productivity tools integrated in to the Google Apps suite including: Gmail with Google Chat, Google Calendar, Google Docs, Google Groups, Google Sites and Google Video. By the end of 2012 BBVA expects to migrate 110,000 employees in over 26 countries to Google Apps (press.bbva.com 2012). BBVA's data will not reside on dedicated servers, in a private cloud environment; instead BBVA's data will share resources in Google's public cloud data centers. But both Google and BBVA believe this model would meet the demands of banking regulators and data protection officials, and be as secure as any solution on the bank's premises (Weber 2012). The deal is the biggest that the search giant has signed with one company for its cloud-computing services. The official details of the BBVA-Google contract are so far unpublished, but the Google App Web site quotes the charge of 40 euros per user per year, charging BBVA about 4.5 million euros (smartplanet.com 2012).

Conclusions

BBVA believe Google's collaboration tools will help its workers communicate and collaborate more easily, regardless of location. Jose Olalla, chief information officer at BBVA, said because workers now had "*access [to] the information they need at any time from any internet-connected device, anywhere in the world, [they] will be able to be more flexible and mobile*"(Weber 2012).

Interestingly though, and perhaps acknowledging the legal and security concerns associated with cloud computing, the bank chose to retain all customer data, and other key banking systems in the bank's own data centers, completely separate from the cloud solution.

The deal is still seen as a breakthrough in corporate adoption of cloud technology. Traditionally, banks have been among the last companies to say they will consider cloud adoption, and are particularly nervous around who controls sensitive customer data (computerworlduk.com 2012). The deal, according to Sebastián Marotte, VP of Google Enterprise EMEA "*shows that cloud computing is now a reality - and leading organisations are already realising its potential to transform their business*" (press.bbva.com 2012).

The bank believe the biggest challenge they will face with the move to web based applications will be cultural; staff have worked for years on tried and tested client-server email applications. But the company has training programs in place, which they hope will help with the not so trivial transition.

2.7 Conclusion

As far back as 1967, the concept whereby computing could be sold as a utility, was given its first airing. This section has attempted to give an insight into the conditions that existed in the ensuing years which led to the advent of cloud computing. Several factors, the commercialisation of the Internet, the advances in virtualisation technology, the research in grid computing, all contributed to the arrival of cloud computing. The three cloud service models, IaaS, PaaS and SaaS have been described, demonstrating what each service model provides to customers. The deployment models were then analysed, Public, Private, Hybrid and Community. Each deployment model is tailored to a particular organisation's requirements, for example, Private cloud is more suitable to an organisation dealing in sensitive data, who wish to use aspects of cloud computing technology without running the risks of putting that data into the public arena.

Thanks to data from Morgan Stanley and jackofallclouds.com, it is clear to see who the main players in the cloud sphere are, and interesting to note that the leading vendors are segregated to a degree by the type of cloud service involved. For example Amazon feature prominently in the IaaS sector, but Saleforce.com dominate the SaaS sales. Perhaps this demarcation along service lines will merge in the coming years as large corporations such as Oracle and Microsoft attempt to introduce products in all service spaces. In the business and marketing section, the way in which cloud is sold was detailed. Marketeers promise many cost savings and improvements with cloud computing, but it is noted that there is not, as yet, a coherent framework for organisations to analyse the suitability and practicality of cloud for their businesses.

Finally the chapter concluded with a cloud case study, looking at how Spanish banking giant BBVA signed the largest ever cloud computing deal negotiated by search engine giant, Google. The deal show-cased was momentous, but highlighted the doubt customers still have in the security and legal concerns pertaining to cloud. BBVA choose NOT to put personal data into the Google cloud.

3. INFORMATION TECHNOLOGY LAW

3.1 Introduction

In 1947 the first transistor was invented, paving the way for the tremendous advancements in Information Technology in the following decades. The pace of these technological advances has been incredibly swift. The IT industry has evolved from mainframes through tablet computers running quickly developed ‘Apps’, downloaded for less than the price of a cup of coffee. In the interim there have been incredible improvements in personal computing, in networking technologies which ultimately led to the development of the Internet, next the advent of mobile computing, cloud computing, web 2.0 and on. As these technologies have evolved though, by virtue of their unique and volatile nature, computer technology has posed novel and complex legal problems for individuals, businesses and legislators.

This chapter will begin by reviewing how law has had to adapt in an effort to accommodate the legal challenges that computer advancements have brought about. The way in which the law has had to be changed and adapted in order to keep pace with the speed of technical innovations in the Information Technology sector will also be reviewed.

Legislation, the process by which laws are enacted by a legislature, and Case Law, rules of law made with judicial opinions, are the two core means with which legal cases are decided. The way in which the judiciary has used case law to interpret legislation applicable to the IT industry in the past, may well point to how legal cases surrounding cloud computing will be judged in the future. Legislation and Case Law, and how the judiciary has interpreted legislation in light of case law, particularly in relation to the IT industry will be analysed in this chapter.

Other key areas of law, which have had a profound effect on the IT industry, are also reviewed in this chapter, they are;

- Intellectual Property
- Data Protection
- Liability

How law is interpreted and applied can vary between jurisdictions. How these jurisdictional differences have affected IT law will be considered later in the chapter.

Finally in order to have a better understanding of IT law, a case study demonstrating how legislation has been interpreted and applied in a sample IT case will be reviewed.

3.2 Background and History of IT Law

There have been extraordinary advances in science and medicine in the latter half of the twentieth century, particularly advancements in computer technology since the late 1970s. Society is without doubt making the transition from an industrial manufacturing age to the information age. But much of the law on state's statute books dates back to the eighteenth and nineteenth centuries. Law it seems has been slow to adapt and evolve to the questions posed by technology. It is however possible to loosely chronicle the evolution of the IT industry in the last 60 years and to demonstrate how lawyers and the legal profession attempted to keep pace.

The early 1970s marked a point in history where events in the IT industry began to warrant the attentions of the legal profession. Until then, the number of computers in the world was small. Computers were expensive and cumbersome. They came as a complete system, encompassing hardware, software, maintenance, support etc., all provided by the same vendor, usually IBM. Generally only government agencies, large corporations and research centres could afford them. There was little incentive for hardware vendors to un-bundle their software, and independent software companies found it extremely difficult to break into the computer market. In 1969 though, IBM under pressure from the American government, pending anti-trust litigation announced that it would un-bundle much of its software (Scott 2008). This action by IBM essentially launched the era of the software industry, licensing and contract issues for software now came into the realm of the legal profession.

Investments in software development now heralded intellectual property concerns, as companies began to copyright their work. Government now too began to gather more and more data on citizens, initiating the adoptions and enactments of data privacy acts by countries such as Germany, and America.

The mid 1970s also saw the rise of computer-related crime, as financial institutions made more and more use of computer infrastructure to carry out their business. And as

Scott points out, little (if any) criminal laws specifically created for these crimes existed. Scott adds further that the first American federal computer crime law was proposed in 1979, but not enacted until 1984. (Scott 2008).

Personal computers entered the market in the late 1970s, spawning the start-up of thousands of software companies, all needing lawyers who could provide legal services and give advice on start-ups, licensing, IP protection etc. The personal computer also laid the path for the 'multimedia' age in the 1980s. Lawyers were once again in demand advising venture capitalists who wanted to 'take a punt' on the emerging technologies.

The multimedia furore gave way to the emerging Internet in the early 1990s. With the Internet came the registration of domain names and the subsequent lawsuits by large corporations in the later years attempting to regain those naming rights. The Internet became an open forum for all, but its open architecture and controls led to excessive, criminal behaviour too. Child pornography, obscenity, lewd and often defamatory content found its way onto the Internet. Legislators have since struggled to strike a balance between controlling criminal behaviour on the Internet and not impeding free speech rights. Major legal battles regarding intellectual property on the Internet also began to surface at this period in history. Copyright laws were drafted and re-drafted in an attempt to counter copyright crimes. The emergence of the Internet also heralded the creation of huge Internet companies such as Amazon and eBay. Just like traditional tangible companies, 'on-line' organisations needed to be bound by legal rules and regulations.

With increased on-line commerce came an increase in the quantity of personal data stored on-line, identity theft duly followed, and these problems in turn led to a need for updated computer law to deal with these crimes. The *dot.com* bust of 2001 had huge ramifications for the legal profession who now found itself dealing more with bankruptcies, mergers and acquisitions than aiding new start-ups get up off the ground. Over the next 5 to 10 years an explosion of activity surged on the Internet, Internet business models morphed and changed, information stored on the Internet grew exponentially. In the last few years Web 2.0 has become the latest web phenomenon to prick the ears of the legal profession. Social network sites are creating huge amounts of work for the legal profession, who have had to draft legislation to counter the data protection and intellectual property issues raised by these sites.

Cloud computing has only served to further burden the legal profession. With cloud computing come legal questions of jurisdiction, data protection, intellectual property, liability and more. Little doubt, further technological breakthroughs in the coming years will further challenge the legal profession.

3.3 Case Law and Legislation

Legislators create and pass laws. They do so usually in response to political pressure/public outcry, which is often due to changes in moral values in society or in response to particular heinous crimes, sometimes in an effort to combat criminal activity that has arisen from the development of a new drug or technology. The courts though, work out what these laws actually mean in practice. Laws are interpreted and tested by a succession of trials/cases, over a period of time. These trials, and the way in which the courts interpret and apply the legislation during the trials make up case law. Case law has a particularly important role in the area of contract law, where few statutes exist (Goldman *et al.* 1987).

Case law, in practice can determine how the judiciary rule on similar cases that find themselves before the courts. A judge for example, on coming across a case before the courts relating to cloud computing, might determine that cloud computing is very similar to grid computing, and apply precedents set in grid computing cases to the cloud computing situation. This scenario has important implications for IT cases before the courts, will a judge liken such a technology to something similar which has arisen in the past, and apply rulings based on precedents set in previous cases? Similarly, a legal team having proven a particular technology is similar to one where decisions and precedents were set by the courts in the past, might bring these similarities to the courts attention, in the hope of gaining a similar ruling.

A recent example in a European trial between computer hardware giant Lenovo and a French citizen, demonstrates how precedents can be set, and could be used in similar cases in the future. In 2007, a French citizen bought a laptop from Lenovo with Microsoft Windows Vista pre-installed, which the individual did not want, a refund was sought on the price of the operating system licence. Four years later a French court decided in favour of the claimant, judging that Lenovo's practices contravened provisions of the 2005 European Union directive on unfair commercial practices (theinquirer.net 2012).

It is very likely that the decision reached in this case will be used in the future to decide software bundling cases. "*The current victory symbolizes the crumbling of hardware-software bundling in France. This means that the legal arguments in Mr. Pétrus's case can be used again in any EU country*" (no.more.racketware.info 2012).

We have seen how the legal profession lags some way behind when attempting to keep pace with the rapid and ever changing developments in the IT industry. Therefore when precedents are set in technology cases, it is incredibly useful and time saving for these precedents to be used by the judiciary and the legal profession in future cases. This pattern will surely persevere into the future and can act as a steer to future technological companies who find themselves facing litigation.

3.4 Intellectual Property

Intellectual Property (IP) according to Lloyd is a legal phenomenon developed during the middle ages, initially drawing some controversy, as it was seen largely as a device for promoting the interests of those in authority (Lloyd 2011). A modern definition from the World Intellectual Property Organisation (WIPO) describes IP as:

"The term refers broadly to the creations of the human mind. Intellectual property rights protect the interests of creators by giving them property rights over their creations."

And as Bainbridge writes, "*In view of the large investment required to finance research, design and development in respect of computer hardware and software, these intellectual property rights are of critical importance to the computer world.*" (Bainbridge 2004).

IP can be seen to cover three main areas of legal rights;

Patent – A form of IP, granted for new, non-obvious inventions, giving the owner a monopoly in his invention, enabling him to exploit the invention for a number of years to the exclusion of all others (Bainbridge 2004).

Copyright – An exclusive IP right which protects works from being copied without permission, and extends to other activities such as making an adaptation of the work, performing or showing the work (Bainbridge 2004).

Trade mark – an IP right that protects ownership of distinguishing marks used to advertise goods and services (Adams 2010).

IP, originally the concern of the print and music industries has become critically important to the IT industry. It can be argued that IP rights are at the cornerstone of the Software Industry, enabling technology giants such as Microsoft and Apple become some of the largest and most successful companies in history. Without Patent, Copyright and Trademark rights it is incredibly difficult to see how these corporations could have achieved the successes they currently enjoy.

IP rights are vital to economic growth, as the ICC opine "*the purpose of the intellectual property rights system is to provide incentives to innovators to produce new inventions and creations. This in turn provides society with a steady stream of innovations that fuel economic, cultural and social progress, help to alleviate poverty and disease, and enrich our cultural heritage"* (ICC 2005).

The advent of digital technology and the Internet though has made copyright infringement more prevalent. New compression technologies and advancements in the speed of network connectivity have made it incredibly easy to copy and distribute copyrighted electronic media.

IP rights also raise fundamental questions for cloud computing users. The protection of copyright in types of data stored on and shared through clouds environments is currently being debated. Licensing of software in the cloud is proving a very interesting area, throwing up legal questions in regard to software distribution and usage. Jaegar *et al.* (2008) give examples of licensing questions that have arisen in the cloud:

"*If a user has a license for a particular software product or dataset and uses it in his or her work, can he or she still use the licensed product in the cloud?",* and further:

"*Cloud computing means that anyone with an Internet connection can access the cloud, including people in other countries. Licensing and use agreements may be* *different across national markets and certain products may only be available in certain markets, but the cloud eliminates such differences*."

These examples certainly show how the concern regarding copyright in the cloud is a very real and current problem for cloud clients and vendors alike.

Governments have drafted legislation in an attempt to counter IP issues, the latest offering coming from the US government, in the form of SOPA (Stop Online Piracy Act) and PIPA (Protect IP Act).

Both bills are aimed at non-US websites that infringe copyrighted material. The bills provide methods for fighting copyright infringement, one method would allow rights holders to seek court orders requiring payment providers, advertisers, and search engines to stop doing business with an infringing site. In other words, rights holders would be able to request that funding be cut off from an infringing site, and that search links to that site be removed (Newman 2012).

PIPA and SOPA have both their opponents and supporters. Opponents arguing that the laws will stifle the very innovation IP rights are designed to protect, and that the bills will lead to the shut down or censorship of legitimate websites. Supporters of the legislation believe it will protect the intellectual-property market and corresponding industry, and that it is necessary to support enforcement of copyright laws.

At time of writing, plans to draft the bills had been postponed until there was time for wider agreement on a solution to the issues the bills had brought about. Whatever the outcome of the legislation, whether PIPA and SOPA are passed eventually in their current state, IP rights within the IT industry remains a contentious issue, and certainly warrants further investigation and research.

3.5 Data Protection

Data Protection (DP) laws owe their origins to the 1960s, when states, in order to operate the developing welfare state, began to collect and store increasingly larger amounts of data on their citizens. This decade also culminated in the roll out of early computer technology, so the machinery was in place to facilitate data retrieval and storage (dataprotection.eu). The early DP acts, borne from a perceived threat that the state would misuse personal data stored on citizens, had as their primary objective the transparency of the large, primarily state-owned databases. Looking to establish data protection rights, these new laws considered the challenges of the new technology, and attempted to make its application controllable and transparent.

Individual states enacted their own DP laws, going back as far as 1970, when the German state of Hesse adopted the world's first data protection statue (Lloyd 2011). In Ireland the Data Protection Act of 1988 and the subsequent Data Protection (Amendment) Act of 2003 are the main Irish laws dealing with Data Protection. Other European Union member states enacted their own particular legislation. In 1995, though, arguably the most important DP law (certainly from an European Union perspective) was enacted, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (dataprotection.ie). This Directive contains provisions that are crucial to ensuring that users can trust the services and technologies they use for communicating electronically (europa.eu).

As demonstrated, the laws on Data Protection have evolved since the 1960s, but the core principles remain the same today, namely, and by way of a definition "*Data Protection legislation applies where personal data relating to an identifiable individual is subjected to certain forms of processing …… the legislation should require that personal data be obtained fairly, that it should be accurate and up to date, should be relevant and not excessive nor retained for longer than is necessary*" (Lloyd 2011).

Kuner (2012) defines DP law as follows: "*Data protection law gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards*". In essence DP is about each individual's fundamental right to privacy. The individual should have access to, and the ability to correct data about oneself. And principally those who keep data about you have to comply with data protection principles.

DP law developed differently in the US and Europe. In Europe, DP laws tended to be omnibus, covering all aspects of processing of personal data, in the US however a more sectoral approach has been favoured, where a range of privacy protection statutes have been enacted to regulate specific forms of information handling (Lloyd 2011).

Although DP legislation and guidelines have been in place for decades, the explosion of data storage in recent years has had a huge part to play in explaining why DP is still such a huge and prominent topic in the IT industry today. The advent for example of Web 2.0, Facebook, Google, the Cloud and more, means personal data is increasingly being disseminated across the internet. Recent examples where individuals and groups such as 'Europe-v-Facebook' have filed complaints against social media websites indicate the level of scepticism there is that DP policies are being adhered to correctly. Culminating in an audit by the Irish Data Commissioner, Facebook have recently agreed to boost their privacy policies (finance.yahoo.com).

As recently as March 1st 2012 Internet Search Engine giant Google published information relating to changes it was making to its security settings, making it easier for the company to share information about users with other services they own, such as YouTube. In a stinging response to the privacy policies changes, European Union commissioner Viviane Reding questioned the legality of the changes, indicating they could contravene European Data Protection law (telegraph.co.uk).

Data and more importantly personal data is very much deemed a commodity which social media sites are willing to exploit for financial gain. And the recent examples of large corporations seemingly flouting DP law demonstrate the battle currently waging between Internet Social Media giants and local law enforcement agencies.

The growth of cloud computing technologies has raised further interesting issues in relation to DP. Cloud computing is a globalised concept. Computer hardware tasked with storing personal data on customers in a cloud environment can be distributed across many jurisdictions. It is often difficult to determine the location of the data and if adequate measures are being taken to ensure that data is being protected. These points conflict directly with DP principles. In a scenario where data is distributed over multiple jurisdictions, it is also difficult to know which jurisdiction's DP laws should be applied to the data. These questions have resulted in a demand for DP law to be amended, in order to find an appropriate arrangement for cloud computing.

3.6 Liability

Legal liability is defined as "*a term applied to being legally responsible for a situation, and is often associated with a contract, especially if the terms of that contract are not fulfilled*" (wisegeek.com).

Two main legal strands of liability prevail within the IT industry, Contractual Liability, which imposes duties on contracting parties, e.g. Party A contracts Party B to provide it a platform service in a cloud computing environment (PAAS). And Non-Contractual Liability, a situation where no legal contract exists between parties, e.g. a pedestrian is injured by a vehicle whose brakes fail due to a software defect in the vehicle's braking mechanism. Remedies to disputes in such cases are usually predicated by evidence of negligence on the part of the defendant (Lloyd 2011).

Cloud computing by its very nature is opaque. When data is stored in a public cloud it is often difficult to tell where that data is stored, it is impossible to know who has access to the data, from a security perspective it is difficult to ascertain what security mechanisms are in place to keep the data safe. What business continuity plans (if any) are in place is also an unknown. All these unknowns raise pertinent legal questions:

- What liability do companies face when there has been a security breach in the cloud that has resulted in the theft or loss of personal data?

- If data has left the client's jurisdiction, and now resides in a state where an adequate level of protection is not applied, contravening European Union Directive 94/46/EC, who is liable for this breech in European Union law?

- If there is a hardware failure, and a client is without their cloud service for an extended period of time, who is liable for the cost of this outage?

From a more general computing perspective, there have been numerous occasions where defects in computer hardware and software have had quite serious implications. The 'Millennium bug' for example was estimated to have cost the global economy £400 billion (Lloyd 2011). Patients treated at the National Cancer Institute in Panama in November 2000 died after receiving an excessive dose of radiation, the cause of which was applicable to the computerised treatment planning system (Zollers *et* *al.2005*). History (and the courts) are littered with other (less fatal) examples of parties to a contract to supply computer systems ending up in the courts when the computer system fails to deliver what was expected.

In the early days of software development it was typical for suppliers to abdicate their responsibilities in situations where their software systems failed to deliver on promises made. This practice is not uncommon though for burgeoning industries, attempting to establish a foothold in a new and upcoming market place. License agreements for participating parties once attempted to eschew all liability away from the supplier, a typical agreement would have read as follows;

> THE SOFTWARE IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND. FURTHER, (Producer) DOES NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATIVES REGARDING THE USE OF, OR THE RESULTS OF USE, OF THE SOFTWARE IN TERMS OF CORRECTNESS, ACCURACY, RELIABILTY, CORRECTNESS OR OTHERWISE. THE ENTIRE RISKS IS ASSUMED BY YOU.

But there is evidence today that the IT industry has moved on, and as Loyd (2010) says, "*vendors are somewhat more 'generous', guaranteeing that the software will perform 'substantially in accordance with the accompanying Product Manual(s) for a period of 90 days"*.

Cloud computing though, being one of the new up and coming technologies in the IT industry has seen vendors revert back to the over-eager reluctance to bear any responsibility for problems that occur within the cloud environment. The current Licensing agreement for Amazon's Web services sounds all too familiar;

> THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND... REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR

CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

Arguments abound that imposing a strict liability regime on Software and Hardware vendors would hamper the growth of the computer industry, stifle innovation etc. Proponents of a more liability regime argue though that the Computer Industry is no longer in its infancy, even cloud computing in its current guise has been around for nearly 10 years. They argue that the industry now has the maturity and financial support to deal with costs that may accrue from defective systems.

3.7 Jurisdictional Issues

Adams attempts to explain the jurisdiction of the state by stating "*the law of any country is binding only within its territory"* (Adams 2010). This definition alone though raises important questions in relation to the IT industry. The Internet is without borders. Reidenberg suggests, "*The current internet technology creates ambiguity for sovereign territory because network boundaries intersect and transcend national borders"* (Reidenberg 2005). Since the Internet's inception it has not always been clear what jurisdiction's laws should apply when criminal activity have taken place on the web. Indeed activity deemed criminal in one jurisdiction might be deemed completely legal in another. Herein lie the problems for legislators. As Kuner suggests "*as the global economy has become more interconnected and the Internet ubiquitous, jurisdictional conflicts involving States, private actors, and regulatory agencies are becoming increasingly common"* (Kuner 2012).

Unfortunately cloud computing has only exacerbated the jurisdictional issues. The distributed nature of cloud computing creates jurisdictional uncertainty. Kyer remarks, "*with information being stored and available "anywhere", who has jurisdiction over it? Whose laws apply?*" (Kyer *et al.* 2011). Within a cloud storage environment, data can be broken up and stored in multiple data centers across multiple jurisdictions. This fact has obvious implications for certain jurisdictions, Canada for example, who impose an obligation on certain sectors to keep certain data outside the United States. Other countries may also want to avoid data storage in the US, where data is now subject to the Patriot Act, which "*gives controversial new powers to the Justice Department in terms of domestic and international surveillance of American citizens and others within its jurisdiction*" (techtarget.com 2002). Some of Amazon's cloud offerings enable the client to determine what jurisdictions their data must be stored in, but this is not necessarily common practice across all vendors. Cloud computing services can also involve many vendors supplying different layers of the cloud service. Therefore although a direct supplier of your initial cloud offering may promise data containment to a certain jurisdiction, this cannot be necessarily guaranteed once that vendor makes use of another, underlying cloud technology at another layer of the service.

Copyright in the cloud is also affected by the distributed nature of cloud computing. From a software perspective, copyright law is determined by the jurisdiction within which that software is created. If software is created in the cloud though by a development team dispersed throughout the globe, what jurisdiction copyright regime will apply?

Arguably the most pertinent question for any legal issue involving jurisdiction is when will jurisdiction be taken, and what are the implications of this. Article 4 of European Union Directive 94/46/EC on data protection, attempted to determine when jurisdiction could be taken with respect to the protection of data of European Union citizens. Article 4 of the Directive requires Member States to apply data protection rules to controllers who process personal data in the 'context of the activities' of their EEA 'establishment', or who are not 'established' in the EEA but, for purposes of processing personal data, 'makes use of' equipment (or 'means', in some languages) situated in the EEA (Hon *et al.* Sept. 2011).

Hon et al, go on to give a sample case, in 2010 where an Italian court convicted a number of Goole executives for breach of Italy's data protection law in relation to a video uploaded to Google Video: "*even though the video data were not processed in servers in Italy, and decisions about content were not made in Italy. Google had an advertising/marketing establishment in Italy, Google Italy, and the judge considered that Italian law applied because the processing was in the 'context' of Google Italy's activities*." This example of a court claiming jurisdiction based on the 'context' issues is demonstrated in other international cases. Courts have tended to claim jurisdiction when they have ascertained a connection between the offending act and the organisation involved.

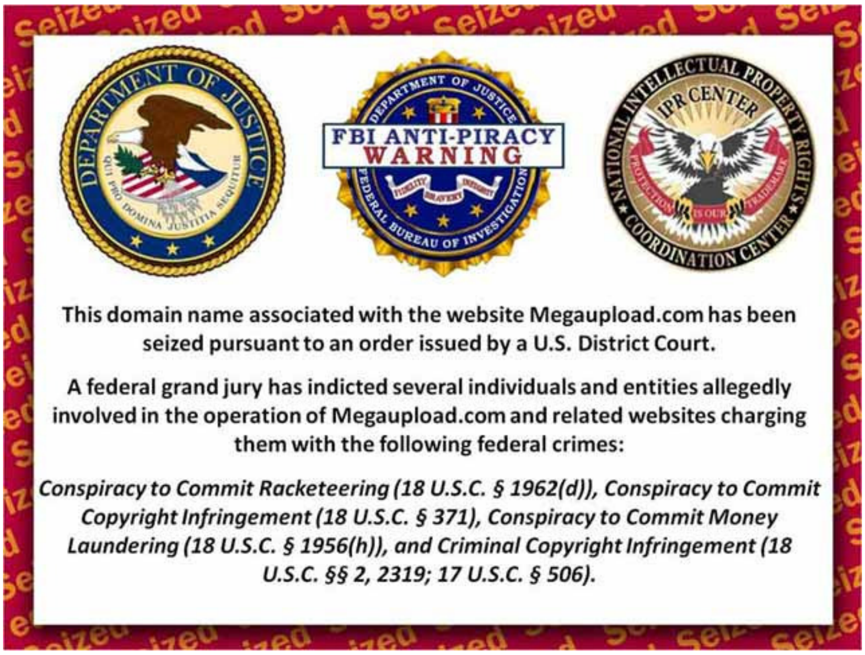
It has been argued that the results of judgements such as Google vs. Italy given above serve to discourage organisations from investing in European jurisdictions. It is difficult to determine if this will be indeed the case, but it certainly seems more clarity and consensus needs to be established with respect to jurisdiction on the Internet.

3.8 Case Study

Megaupload Limited is an on-line Honk Kong based company, established in 2005, that ran a number of cloud computing services related to file storage and viewing. The company employed 150 users and at the height of its popularity had registered members in access of 180,000,000. It comprised a number of web services, providing hosting capabilities for music, data, video, pornographic content and more. One huge issue for a hosting company like Megaupload is the risk of copyright infringement. Users can potentially (and did) store copyrighted material in the Megaupload cloud. This copyrighted material became available to other Megaupload members, and was openly shared and downloaded.

On January 5th, 2012, after two years of investigations, the American government shut down the company's web sites, seized its domain names, confiscated $50 million dollars worth of the company's assets and with the assistance of New Zealand police had four of the company's key employees arrested. A Virginia federal court charged Megaupload on a number of counts, most notably *"conspiring to commit copyright infringement"*. Megaupload had portrayed itself as an organisation which operated within the law, and one who actively discouraged clients from distributing copyrighted material. They even developed an 'abuse tool' which allowed a rights holder remove links to their material. The courts ruled though, that Megaupload's attempts to prevent copyright infringement was just a facade, and that the company turned a blind eye to such activities. The indictment claims Megaupload has caused the entertainment industries more than $500 million in lost revenue.

Visitors to the megaupload.com web address are now confronted with the following image:



This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court.

A federal grand jury has indicted several individuals and entities allegedly involved in the operation of Megaupload.com and related websites charging them with the following federal crimes:

Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

Figure 3.1: American District court seizure of megaupload.com

One other interesting aspect to this case is that user content is now inaccessible. In Megaupload's Terms of Service the company stated that users have no proprietary interest in any of the files on Megaupload's servers and that they must assume the full risk of complete loss or unavailability of their data and that Megaupload can terminate site operations without prior notice.

This case demonstrates succinctly many important facts regarding cloud computing. The risk of copyright infringement in a cloud environment is a very real and present danger, and as this case has shown will be pursued relentlessly by the relevant authorities. The case also highlights the danger of storing personal data in a cloud environment, Megaupload clients currently have no access to personal data they may have stored in the cloud environment, and furthermore, those clients don't know who has access to their data, and if it will ever be returned to them.

3.9 Conclusion

This chapter has attempted to give a brief overview of the main legal matters that are relevant to the IT industry. Since the 1970's and the birth of the software industry, the legal profession has found itself constantly trying to keep pace with the new advancements thrown up by the IT industry every few years. Lawyers and legislators have not always managed to react quickly to legal issues presented by new technological innovations. But they have nevertheless benefited greatly by the huge swathes of legal work which IT developments have brought about. Case law and precedents have helped the profession form and apply legal opinion to trials concerning newer technologies. This has given the profession time to 'catch up' with the technological advancements.

Intellectual Property, Data Protection and Liability, key areas of law affecting the IT industry have been discussed. These 3 facets of the law have had major implications for cloud computer vendors and clients alike. IP has been demonstrated to be of particular relevance to cloud computing, where major hosting sites are feeling the wrath of the judiciary where proper copyright infringement measures are not seen to be in place. DP principles are also to the fore of cloud computing legal issues, with Social media sites too feeling the scorn of government watchdogs in relation to their perceived flouting of DP guidelines, particularly in respect to personal data. And of course liability will be an evolving issue with IT companies, hopefully assuming more liability upon themselves as their products and services become more robust and mature.

Finally we looked at jurisdictional issues in IT, again relating particularly to cloud computing, where it is vividly evident that jurisdictional issues will continue to cause legal issues for cloud vendors. With information being stored and available 'anywhere', who has jurisdiction over it?

In the next chapter, 'The Cloud and the Law', jurisdictional issues and indeed other pertinent legal issues pertaining to cloud computing will be examined in further detail.

4. THE CLOUD AND THE LAW

4.1 Introduction

Key areas of the law which affect the IT industry have been explored in Chapter three. In that chapter the impact certain laws have had, and may potentially have, on the cloud computing environment was discussed. And some of the salient aspects of the cloud computing environment which raise serious legal concerns have been touched on. This chapter will take a more detailed look at the legal issues which are typically associated with cloud computing. Utilising cloud services should in many ways only raise legal concerns broadly similar to those considered when availing of any third party service. The potential for data to be distributed across multiple servers and stored in different jurisdictions is the main noticeable difference that arises from cloud computing services.

Three legal areas to be considered in more detail in this chapter are;

- Data Protection compliance
- Intellectual Property Rights
- Law of Contract/Liability

Data protection compliance, particularly in relation to personal data, has been the subject of several high profile news accounts in recent months, and certainly merits further analysis in this section. The European Data Protection directive is the guiding legislation with regard to personal data, and its reach and implications will be outlined. It will be important to understand the legal definition of personal data, and determine who is responsible for its protection and security in the cloud. Jurisdictional issues are at the core of any legal conversation regarding cloud computing, and those issues will be addressed under the DP compliance heading. Jurisdiction leads onto laws of local states, and the EU – US Safe-Harbour principles, an agreement between American and the European Union with regard to the protection of European Union citizens' data residing in America. These principles will be discussed in this section.

Copyright infringement is a continuous thorn in the side of the IT industry. Unfortunately the architecture of the cloud computing environment doesn't make copyright infringement any less likely. In fact some argue the distributed and open structure of the cloud environment only serves to exacerbate the problem. Copyright infringement/Intellectual Property Rights and their volatile relationship with the cloud will be reviewed in this chapter. Finally, as with any other outsourced provision, a good service level agreement is essential, and laws of contract will be examined.

4.2 Data Protection Compliance

Several legal enactments, in many countries have evolved in the last 30 to 40 years attempting to deal with the issue of data protection. From the world's first data protection statue in 1970 in the German state of Hesse, to the 2012 re-draft of the European Union data protection directive, DP compliance has been an important element of IT law. DP is ultimately a privacy issue, and the privacy of individuals has often been cited as a concern with cloud computing. Most EEA states take their DP guidance from the 1995 European Union data protection directive, and it will be heavily focused on in this chapter. America has no single data protection law comparable to the European Union's data protection directive.

The advent of cloud computing has made DP compliance much more of a concern for companies. Previously when personal data was stored in-house, on local company infrastructure DP compliance was still a concern. There are always risks of security breaches whether from internal or external resources, disaster recovery or business continuity procedures may not be adequately worked out etc. But there has been a perceived notion that personal data stored within a private institution is much less vulnerable to attack, or at least is perceived to be at less risk. It is also argued though, that security in a cloud environment can be more robust than that of a private environment. It has to be. Unfortunately this discussion is beyond the scope of this work.

Cloud computing obviously takes personal data out of the private setting, and for sake of a better word, 'exposes' that data to a whole host of unknowns. Where is the data? Who has access to it? Is it secure? Is it backed up? Who has access to the backups? If there is a hardware failure, will the data be retrievable? Although these questions may arise when data is stored in a local/private facility, the questions can at least be answered there with some certainty. Within a cloud environment, this is not so. Cloud computing has completely brought DP compliance to a new level of relevance and importance.

4.2.1 European Union Data Protection Directive

The European Union data protection directive (DPD), in its full guise is known as "*DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*". The DPD was intended to encourage the free movement of personal data within the EEA. And as Hon *et al.* suggest, this was meant to be accomplished by "*by harmonising national provisions on data protection while protecting to a high level the rights and freedoms of individuals (known as 'data subjects) who are the subjects of such data, in particular their rights to privacy with respect to the processing of their personal data wholly or partly by automatic means*" (Hon et al 2011a). The DPD is also relevant even to non- European Union jurisdictions because of its potentially broad reach. For example, cloud providers based in America, utilising IT infrastructure in the EEA can still be subject to the DPD.

The nature of European Union directives means that national parliaments have some leeway in how these directives are interpreted and adopted into local law. Therefore there is scope for some elements of the directive to be exempted or extended. This means that there is the possibility for national differences in DP law to exist in different EEA countries. Cloud computing services are in the main concerned with storing data in remote locations, in many cases far removed from the served institution. Quite often the data stored is of a personal nature, and therefore means the cloud service being offered (if it is an EEA offering) is subject to the full ramifications of the European Union DPD.

4.2.2 Personal Data - What Information is regulated?

The European Union DPD has serious consequences for cloud providers in an EEA setting, so it is obviously quite important to establish what is meant by 'personal data'. Moreover the DPD *only* applies to personal data. The DPD defines 'personal data' as:

"any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

To stay within the guidelines of the DPD cloud vendors must ensure all adequate measures are in place to ensure the protection of personal data. There is scope in the directive though, for measures the cloud provider can take to render the data 'non-personal', and therefore avoid being subject to the data protection requirements. These measures could include anonymisation/pseudonymisation, encryption and data fragmentation. However the DPD is not completely clear as to what levels of complexity these measures need to have achieved in order for the data to be rendered, 'non-personal' and as Hon *et al.* suggest "*in the cloud computing context the status of encrypted data as non-personal data should be clarified, at least where it has been encrypted and secured to industry standards and best practices*", Hon *et al.* go on to make the point that the DPD is too rigid and that the definition 'personal data' "*should be based on the realistic likelihood of identification.*" (Hon et al 2011a).

4.2.3 Personal Data, who is Responsible?

Under European Union data protection law, responsibility for personal data is imposed on the 'controller', who may employ 'processors' to process the data on its behalf. From a cloud perspective, the 'controller' in the main, remains the institution who availed of the cloud service, and the cloud provider is regarded as the 'processor'. This means that full responsibility for data protection usually lies wholly on the institution employing the cloud service. This fact further highlights the importance of service level agreements between cloud customers and vendors.

However, due to the multi-faceted nature of cloud computing, it is not always accurate to classify the cloud provider as the processor, if for example the cloud provider has an individual user as its customer; it is likely to be the controller of the personal data collected related to that user. Moreover, in many cloud services, there may be layers of cloud providers involved, and this may affect a cloud service's classification in respect to whether that cloud provider be classified as 'controller' or 'processor'. Hon *et al.* have argued that in some respects cloud providers are only neutral intermediaries, certainly with respect to IaaS delivery models, where the provider can have no involvement or knowledge as to the type of data being stored (Hon et al 2011b).

For these reasons Hon *et al.* have suggested that the binary distinction between controllers and processors is unsuitable for a cloud computing environment and should be abolished. They add "*The definitions of 'controller' and 'processor' need updating* *to allow a more nuanced and flexible approach*". The more flexible approach they argue would be based on a principle of end to end accountability, "*this may impose primary liability on one party, but assign different degrees of responsibility and liability to other actors in proportion to the individual parts they each play in the processing chain*" (Hon *et al.* 2011b).

4.2.4 Jurisdiction

"*Jurisdiction over activities on the Internet has become one of the main battlegrounds for the struggle to establish the rule of law in the Information Society.*" (Reidenberg 2012).

The DPD seems to have foreseen the concept of remote processing of data, where the processor is established in another country, and does contain provisions on applicable law and its jurisdictional reach. Hon *et al.* suggest the reasons for these provisions are to "*ensure the application of the data protection obligations to personal data connected with the EEA, even if the data are processed in a non-EEA country by a non-EEA established controller*" (Hon *et al.* 2011c). Under article 4 of the DPD three grounds for applying the European Union rules to an act of personal data processing are;

1. **Establishment** - According to art 4(1)(a) each EEA Member State must apply the DPD as implemented in that Member State if "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".* This implies that if a controller's EEA office processes data in the cloud in the context of that office's activities it must comply with the local requirements of the EEA country in which the branch or office is established when processing personal data, wherever in the world the processing takes place.

2. **International law -** Art 4(1)(b) provides that a Member State's data protection law apply where the controller is not established on that Member State's territory, but its law apply by virtue of international law. Hon *et al.* give the example here of a data center being housed on a ship, moored in international waters.

3. **Equipment** – Art 4(1)(c) states that if the data controller "*is not established on Community territory*", the application of a Member State's data protection law may nevertheless be triggered if it "*makes use of equipment, automated or otherwise, situated on the territory*" of that State for the purposes of processing personal data. Interestingly, in respect to this provision, the law applies even if the personal data is not that of an EEA individual.

These three subsections of article 4 demonstrate the broad reach of the DPD on cloud vendors. And it is clear to see why some commentators suggest these types of provisions laid down by the DPD discourage investment from American multinationals in Europe. It is suggested that the provisions are opaque and lack continuity across all EEA member states.

4.2.5 EU-US Safe Harbour Principles

The European Commission does sanction the transfer of personal data outside the EEA, but only to countries that they deem will provide an adequate level of protection. These countries include Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man and Jersey. America is not deemed a country where data will receive adequate protection. For data transfers to America a special agreement was drafted known as the EU-US Safe Harbour principles. The principles are in effect, a streamlined process in which American companies can comply with the DPD. The Safe Harbour principles have increased in popularity with the advent of cloud computing (Sanchez 2011). The principles do have their detractors though; some argue that as the regime is self-regulatory, abuses will be inevitable and ultimately the level of protection provided will on be a watered down version of the provisions in place in Europe.

The USA Patriot Act is also proving to be an obstacle to European Union cloud companies once willing to avail of the Safe Harbour principles to export data to America. The Patriot Act came into being shortly after the 2001 911 terrorist attacks on America. It is anti-terrorism legislation that gives the American authorities sweeping powers to access and confiscate electronic data. It is understood the Patriot Act would supersede any protection given to personal data of European Union citizens covered under the Safe Harbour principles. The fears of American authorities accessing such data under the framework of the Patriot Act were aired by the Dutch justice minister in 2011 "*Ivo Opstelten cited the Patriot Act when he told the parliament that his government would exclude American companies from bidding for IT services*"(compliancesearch.com 2012).

Some European cloud providers even seem to be going as far as guaranteeing their services won't risk data being subject to the Patriot Act, and will therefore guarantee data will not be stored in America. Deutsche Telekom T-Systems plans to lure customers to its cloud services by emphasising the security of its servers, and this includes shielding clients from the Patriot Act. Reinhard Clemens, T-Systems CEO, believes "*A German cloud*" would be a "*safe cloud"* (Businessweek.com 2011).

4.3 Intellectual Property Rights

JiscLegal defines Intellectual Property Rights (IPR) as "*rights granted to creators and owners of works that are the result of human intellectual creativity. These works can be in the industrial, scientific, literary or artistic domains."(*JiscLegal 2011a). JiscLegal go on to explain how "*copyright protects original works, and under international law copyright owner have rights to control the copying, adaptation, publishing, performance and broadcast of the work, and under what conditions this may be done*" (JiscLegal 2011a).

4.3.1 Copyright

The architecture of cloud computing environments leave cloud vendors exposed to IPR issues. As Nelson argues "*By giving customers access to almost unlimited computing power and storage, Cloud services could make it even easier to share copyrighted material over the Internet."* (Nelson M. 2009). Storing copyrighted material in a cloud environment not only runs the risks of being copied by users of the service, but cloud administrator will often backup data, sometimes several times. This further highlights the IPR issues. How many acts of copying a particular piece of copyrighting material are legal?

Creating copyrighted material in the cloud is also a complex issue. If a development team working across various jurisdictions create a piece of software in the cloud, what jurisdiction's laws apply to the final copyrighted work?, i.e. If the resultant copyrighted material is subject to a legal action after its creation, what jurisdiction's copyright laws will be applicable.

The nature of the cloud also makes it difficult for would-be plaintiffs wishing to sue for copyright infringement to produce physical evidence that their work was infringed. As Abe suggests it is "*Difficult for Plaintiffs to find the evidentiary trail…reproductions may exist anywhere at any point in time and then disappear…as can users/defendants/infringers…will a Plaintiff even know who to sue in the cloud?*" (Abe Lisa K. 2011).

Abe also points to the case of Apple Computer Inc. v. Mackintosh Computers Ltd., [1990] 2 S.C.R. 209 (S.C.C.), "*computer programs encoded on chips as a series of circuits were "copied" by copying the chips directly and without copying the written form of the programs. It was held that a copy made of a reproduction in a different form from the original, was still an infringement of the original*". Abe makes the point that "*applying this ruling to the cloud, a virtual infrastructure, platform, software or other work that is reproduced in a cloud, in a different form from the original, could be infringement.*" (Abe 2011).

It is not uncommon for a cloud provider to indemnify itself against legal action should copyrighted content become distributed in the cloud environment. But where policies are in place to remove infringing material, there is often no recourse to have the deleted data restored to the official/original owner.

4.3.2 Licence Restrictions

Cloud computing vendors offer users the ability to access the cloud service, particularly a SaaS service online on a computer. But wordpress.com makes the point that accessing online software on a computer without a license is copyright infringement (wordpress.com 2011). This means they argue that licenses granted by cloud operators will be very narrow and limited for the business' own purpose. And that businesses must understand that they have no right to modify the software in question or sub-license to third parties.

Again the use of virtualisation, common in cloud operations raises the licensing issue. Clouds can provision different application stacks dynamically in response to user demand, and very quickly providers can run the risks of license violations.

Open Source software is frequently a choice of cloud operators wishing to reduce costs, and can be deemed as a means of avoiding licensing issues. But open source software licenses vary significantly. Some require onward licensing of source code when incorporated into other software or deployed in a hosted environment. With this model the cloud vendor would effectively need to be a licensed reseller of the open source software, but many types of software do not permit resale.

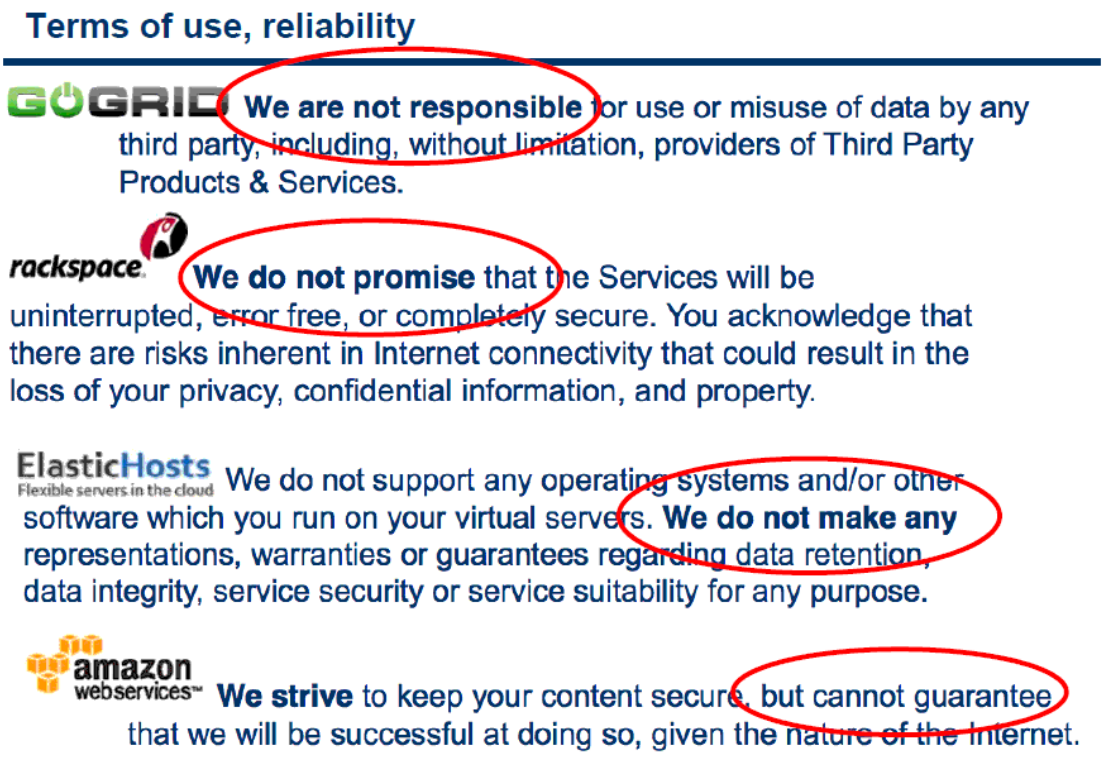
Another issue with licenses in the cloud is jurisdiction, JiscLegal make the point that software licences may be location specific, so care is required to ensure compliance is adhered to when using software in a cloud infrastructure (JiscLegal 2011a).

Finally, standard terms offered by many cloud providers allow them usage of content stored on their servers. This can result in material stored or created in the cloud being used by the cloud operator for self-promotion purposes or being sold on to third parties. This certainly might not be the desired arrangement for many cloud customers, particularly if they are storing personal data in the cloud environment, or if they are using the cloud facilities to generate material that they want to have exclusivity over.

4.4 Law of Contract/Liability

Most cloud providers want customers to be liable for problems which occur with the cloud service, be that downtime, loss of data, security breaches etc. O'Connor states "*Most cloud computing contracts will contain comprehensive limitation of liability provisions including both a financial cap on liability and an exclusion clause for indirect losses, and in most cases a separate exclusion clause for data loss and data breaches*" (O'Connor 2011). Such forfeiting of liability can have disastrous results for business as can be seen in the Armburst *et al.* article, where in 2009 several companies went out of business after suffering days of downtime when the data centers hosting their corporate data was raided by the FBI investigating criminal activity (Armburst *et al.* 2010).

The tendency to deny liability for direct damages in the cloud tends to differ between cloud providers on both sides of the Atlantic. Research carried out by Queen Mary University London School of Law found that cloud providers based in the US tended to seek to deny liability for direct damages as far as possible while European based cloud providers were less open about seeking to exclude direct liability, presumably on the basis that in most European legal systems it is difficult to do so. This difference in approach may be an important factor for companies to consider in their selection of cloud provider. This also raises the point that complete abdication of liability may not stand up to local state laws. In the UK for example, consumers feeling contract terms are unfair have some recourse under the Unfair Terms in Consumer Contracts Regulations. Figure 4.1 demonstrates some of the disclaimers built into some cloud vendor contracts.


GOGRID
rackspace
ElasticHosts
Flexible servers in the cloud
amazon
webservices™

Terms of use, reliability

We are not responsible for use or misuse of data by any third party, including, without limitation, providers of Third Party Products & Services.

We do not promise that the Services will be uninterrupted, error free, or completely secure. You acknowledge that there are risks inherent in Internet connectivity that could result in the loss of your privacy, confidential information, and property.

We do not support any operating systems and/or other software which you run on your virtual servers. **We do not make any** representations, warranties or guarantees regarding data retention, data integrity, service security or service suitability for any purpose.

We strive to keep your content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet.

Figure 4.1: Abdication of Liability

Whether a cloud provider *will* negotiate a limitation of liability, it is very much down to the type/size of company involved, and the service being provided. But O'Connor states that "*Typically, cloud providers will not enter into any negotiations regarding contractual provisions with small or medium sized customers, especially in relation to limitation of liability clauses – the contracts are offered on a "take it or leave it" basis*" (O'Connor 2011).

Some cloud providers though, do have mechanisms in place to compensate customers for failure to deliver particular services at set levels. This mechanism is generally known as Service Credits, and usually allows a customer a rebate against future billing. Service credits though will generally be covered under a separate service level agreement than the main cloud contract, and in practice tend to be very much at the discretion of the service provider.

Vendor lock-in is another area where potential cloud customers need to be diligent when negotiating contract terms and limitations of liability with cloud providers. There is occasion when a customer may wish to switch cloud providers. This can lead to interoperability issues. Different cloud infrastructures may not support migration from one cloud environment to another. Furthermore O'Connor makes the point that some cloud providers will require contractual provisions which "*obligate the cloud provider to assist the cloud customer to migrate its' IT requirements and data out of the cloud and back-in house with additional provisions governing the retention and destruction of all the cloud customer's data, particularly confidential or proprietary data.*" (O'Connor 2011).

For the reasons demonstrated in this section, it is obviously crucial that companies carry out extensive due diligence to assess potential risks before signing cloud service contracts. As JISCLegal suggest, "*Institutions should ensure that the contract terms with cloud providers reflect their legal obligations, responsibilities and the level of risk they are prepared to handle*" (JISCLegal 2011a).

4.5 Conclusion

The areas of IT law discussed in this chapter are not new, nor were they born as a result of cloud computing. Data Protection legislation for the IT industry has preceded cloud computing by at least 30 years. Intellectual property rights law and law relating to contract and liability have been debated and cited in the context of the IT industry since the advent of the commercial software industry in the early 1970s. Different technologies and trends have come and gone in the last half decade, challenging these areas of IT law to different degrees.

The emergence of the cloud computing in the last decade though, has thrown new light on many areas of IT law. The cloud uses the Internet exclusively to deliver its service. Data stored in the cloud can be fragmented and stored in multiple jurisdictions. Customers of cloud services can potentially share files with one another. Cloud computing is not quite a mature business concept, so contract for services still tend to shift liability completely away from the cloud vendor. All these elements demonstrate the role cloud computing is having in re-invigorating the legal debates in data protection, intellectual property rights and contract law.

Perhaps over time, as the technology matures, and contracts become more standard, perhaps when legislators stop playing catch-up and adapt laws to correctly cater for the legal challenges cloud has presented, the cloud computing environment might pose less of a legal minefield than it does for businesses today.

As cloud computing has evolved over the last 10 years, it has posed legal challenges for jurisdictions on a global basis. Different jurisdictions (even jurisdictions within the EEA), have interpreted the challenges presented in their own particular way, and have legislated likewise. In the next chapter, how states around the world have interpreted the legal questions presented by cloud computing, and how they have legislated for these problems will be analysed.

5. COMPARISONS OF INTERNATIONAL PERSPECTIVES ON CLOUD COMPUTING

5.1 Introduction

In Chapter three, important points relevant to IT law were addressed; concepts such as Intellectual Property and Data Privacy and Protection were explained and investigated. In chapter four, an attempt was made to explain some of the legal issues which are typically associated with cloud computing. The issue for example, whereby personal data in a cloud computing environment cannot be moved out of the EEA jurisdiction, except under exceptional circumstances was explained.

There is an argument that the full potential of cloud computing cannot be accomplished unless data is permitted to move between many jurisdictions; based on the premise that cloud providers will move data to different locations depending on where the most efficient resources are available. This notion is espoused as one of the cloud's major advantages over normal computing models. With new technologies from Intel and VMware (See Chapter six), the ability now exists for cloud providers to determine what jurisdictions data can be transferred to. Cloud vendors such as COLT, (www.colt.net), now allow clients choose which jurisdictions they want included in their cloud service. Clients can specify those countries they feel provide a favourable environment for their data and business processes. COLT can then ensure the customer's data remains within those locations. It seems prudent therefore to analyse the legal policies and procedures different countries have in place which affect cloud computing. Armed with this information, cloud customers may then be able to make a more informed decision as to which jurisdictions are suitable for data transfer under a cloud contract.

This chapter moves toward comparing and contrasting policies and regulations jurisdictions have in place that will affect cloud adoption. These policies and regulations will also have a determining factor on how legal cases are handled in those jurisdictions. Sample legal cases will therefore be identified to demonstrate how the policies and regulations in place in these jurisdictions affect the outcomes of legal cases involving cloud computing. The chapter will attempt to demonstrate an integrated legal framework, detailing what laws affect cloud in a sample set of countries, and how these laws affect the readiness of the countries concerned with fostering cloud take-up.

Unfortunately the scope of this document does not warrant a comparison of the legal perspectives on cloud in every country. The countries which will be analysed are; Ireland, America, The United Kingdom, Canada, Russia and China. It is important to note at this point that there is little or no law available in any jurisdiction which has been explicitly enacted as a result of cloud computing. More typically, laws and regulations in and around the areas of data privacy, intellectual property and cybercrime determine the treatment of cloud computing in those jurisdictions. Therefore this chapter will look at those laws and regulations relevant to cloud computing in three policy categories; Data Privacy, Security and Cybercrime and Intellectual Property. There will be a heavy focus on the area of Data Privacy, as the legal status of personal data in a cloud computing environment is the central theme of this dissertation, the other policy categories are also central to the growth and operation of cloud computing, and are included to give a more rounded view of laws affecting the cloud computing landscape.

5.2 Policy Categories

5.2.1 Data Privacy

As demonstrated in earlier sections of this document, under the guise of data protection laws, data privacy in a cloud environment is a fundamental legal concern for cloud vendors and customers alike. Many countries around the world have data protection laws in place and in some cases have established independent privacy commissioners. According to the Business Software Alliance (BSA 2012), many of these laws "*are based on a mix of the OECD Guidelines, the EU Directive or the APEC Privacy Principles*". The APEC Privacy Principles are a Data Privacy framework put forward by the Asia Pacific Economic Cooperation group. The framework attempts to improve information sharing among government agencies and regulators, in an order to foster e-commerce between different economies. Having a comprehensive set of data protection policies in place is seen as a vital step in reassuring and giving confidence to cloud users that their personal data, stored in the cloud, will be secured and handled correctly there. Figure 5.1 from Forrester (forrestertools.com 2012) gives a graphical representation of the scope of global regulations governing privacy and data protection. China for example, seen in red below does not have any substantial data protection laws in place, whereas substantial data privacy and data protection policies are in place in Canada, where the Canadian government impose wide reaching restrictions on the transfer and storage of personal and sensitive data.

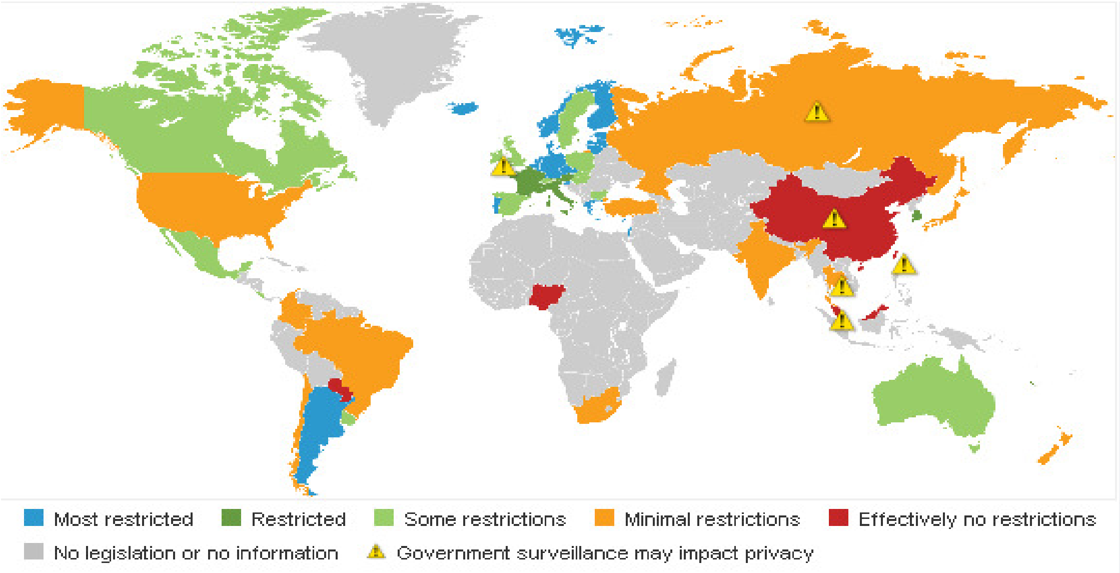

Most restricted
Restricted
Some restrictions
Minimal restrictions
Effectively no restrictions
No legislation or no information
Government surveillance may impact privacy

Figure 5.1: World Data Privacy and Data Protection map

5.2.2 Security and Cybercrime

Cloud adoption, and the manner in which cloud case law may be dealt with can also be determined by the policies and regulations in place in a jurisdiction concerning data security. Cloud consumers need assurance that cloud service providers understand and appropriately manage the security risks associated with storing their data and running their applications on cloud systems (BSA 2012). Laws determining electronic signature policies, Internet censorship or filtering requirements and laws governing e-commerce fall under the security umbrella. Again to some degree most jurisdictions around the globe have implemented some security requirements. The extent of the requirements again vary greatly, in China for example Internet filtering or censorship regimes may act as a barrier to the expansion of the digital economy and cloud computing, and will definitely determine the outcome of case law in relation to cloud. Conversely the United Kingdom is free from Internet censorship and filtering, and up-to-date laws are in place for e-commerce and electronic signatures, providing the confidence cloud vendors and clients require in order to invest in cloud services.

As recently as April 26 2012, the bbc.co.uk reported on a story in which the British Serious Organised Crime Agency (SOCA) carried out raids at premises in the UK, Australia, Europe and America, closing down dozens of websites offering credit card details and other private information for sale. The BSA suggest that as "*cloud computing involves the aggregation of massive amounts of data in large data centers, it creates new and highly tempting targets*." (BSA 2012). Criminals will no doubt turn their attention to the vaults of information that sit in cloud data farms, and it will be increasingly difficult to secure these facilities both from physical and cybercrime attacks in the future. It is up to local government to ensure domestic laws provide an effective mechanism for law enforcement. Many countries around the world have enacted cybercrime law. Some have signed the Convention on Cybercrime. The Convention on Cybercrime is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. Ireland signed the treaty in 2002, but disappointingly has yet to ratify the convention. America on the other hand signed the convention in 2001, ratified it in 2006, and the convention entered into force on the first of January 2007 (conventions.coe.int 2012).

Countries where rigid cybercrime policies and regulations are in place will give solace to cloud vendors and their customers. And perhaps such laws will act as a deterrent to criminals attempting to make use of cloud technologies in order to perpetrate cybercrime.

5.2.3 Intellectual Property

Intellectual Property laws adopted by any particular jurisdiction will have an enormous bearing on legal cases involving cloud computing. Customers of cloud vendors will look to these laws to protect their intellectual property. Cloud vendors and resellers also rely on a combination of patents, copyrights, trade secrets and other forms of intellectual property protection. In jurisdictions where there is clear protection and rigorous enforcement of IP law, cloud vendors and clients will once again feel confident that this is a jurisdiction where they can do business, and have proper recourse to the law should IP violations take place.

The Agreement on Trade Related Aspects of Intellectual Property Rights or TRIPS is an important and probably the most comprehensive international agreement on intellectual property rights. The agreement is an attempt to narrow the gaps in the way IP rights are protected around the world, and to bring them under common international rules (www.wto.org 2012). Again there are large discrepancies in regard to which countries have signed up to this agreement, Ireland (as part of the European Union) accepted the agreement in 2007, but nations not yet signed up include Russia, South Africa, Chile, Kenya and more.

The World Intellectual Property Organisation (WIPO) Copyright treaty is another international agreement that provides additional protections for copyright deemed necessary due to advances in information technology (wipo.int). Cloud vendors will also view countries that are signatories to the WIPO copyright agreement as being serious about IP concerns.

In October 2007, the US, Japan, South Korea, Mexico, New Zealand, Switzerland and the EU announced their intention to negotiate a new Anti-Counterfeiting Trade Agreement (ACTA) (Ruse-Khan, H.G. 2011). Ruse-Khan further makes the point that ACTA creates treaty obligations that go significantly beyond the existing international standards in TRIPS (Ruse-Khan, H.G. 2011). ACTA is definitely attempting to be the 'New Gold Standard' of International treaties on Intellectual Property law. Figure 5.2 below from wikipedia.org highlights the countries that have signed the treaty, it is also quite evident from the graphic that many jurisdictions around the world have not yet signed up to the agreement. This image further highlights how huge disparities exist between countries in regard to how laws central to cloud adoption and treatment are being employed.

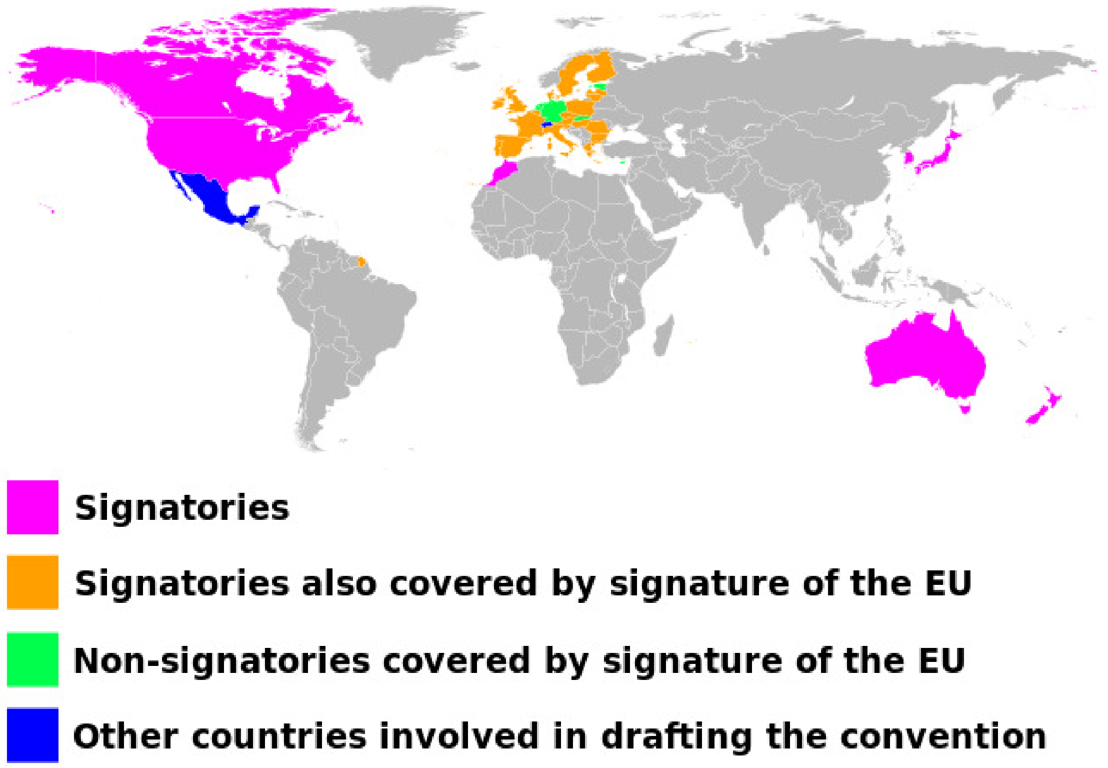

Signatories
Signatories also covered by signature of the EU
Non-signatories covered by signature of the EU
Other countries involved in drafting the convention

Figure 5.2: ACTA World Map (wikipedia.org ACTA 2012)

5.3 Countries Analysed

As mentioned earlier in this section, each country will be assessed based on the three category areas outlined. By investigating the degree to which each country has adopted or enacted policies and regulations in respect to the three categories, it will be possible to get an understanding as to how legal cases concerning cloud will be treated in that jurisdiction. The analysis will also help identify the similarities and disparities that exist within the six sample countries in respect to laws affecting cloud. And the analysis will enable the development of an integrated framework on international perspectives on cloud computing.

5.3.1 Ireland

Data Privacy – Under its 1988 Data Protection Act, Ireland established an office of Data Commissioner. In 2003, an amendment was passed updating the 1988 Act, implementing the provisions of EU Directive 95/46 (The Data Protection Directive or DPD). The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions (dataprotection.ie). The Irish data commissioner has been quite visible in the recent press, most notably when carrying out an audit of Facebook's European headquarters in Dublin. Ireland has a number of large IT multinational companies that have based their European headquarters there. Therefore the Irish Data Commissioner will investigate complaints relating to data protection and privacy matters from European citizens, made about these companies. The commissioner's work is therefore quite visible and the office of the Data Commissioner and the related Acts do provide a high level of data privacy and protection for cloud users. However whether the guidelines and obligations in respect to the data protection Acts are being fully adhered to by Irish businesses is another matter. Recent stories again in the news media relating to the theft of unencrypted Health Service Executive laptops and patient files dumped in hospital bins does nothing for Ireland's Data Privacy rating.

Several legal case studies exist on the Data Commissioner's web site, indicating that complaints are being fully investigated by the commissioner. For example the site gives examples where local authorities were reprimanded for displaying personal information of individuals relating to planning applications, and of cases where private businesses were sanctioned for disclosing personal data without data subject's consent.

One further point, In Ireland certain categories of data controllers are also obliged to register with the Data Protection Commissioner. This may be seen by some cloud providers as an unnecessary burden, but from an individual's perspective can only be seen as another positive in terms of the extent of data privacy rules in operation in the country.

Security and Cybercrime – On 10 July 2000 President Mary McAleese applied her digital signature on the Electronic Commerce Bill. In doing so, Ireland became the second country in the world to use a digital signature to sign a bill into law. The

Electronic Commerce Act, 2000 gave legal recognition to electronic signatures in Ireland (blogs.ics.ie 2009). The Act also defines legal recognition for electronic writing and electronic contracts so as to ensure that such electronic communications would not be treated any differently under the law, than traditional paper-based communications (kilroys.ie 2002). Ireland is also free from Internet censorship and filtering. However recent events at the now defunct Anglo Irish Bank, seem to indicate there are holes in Electronic Commerce Act. Gardai have had trouble decrypting bank documents in the course of their investigations into the bank's lending practices, and it seems the Commerce Act, and even provisions under the Criminal Justice (Theft and Fraud Offences) Act of 2001 don't seem to allow Gardai compel former bank employees to reveal passwords on encrypted material.

The last Bills enacted in Ireland with some provisions for computer crime were the Criminal Damages Act, 1991 and the Criminal Justice (Theft and Fraud Offences) Act of 2001. These Acts are seen as outdated. As mentioned earlier Ireland signed the Cybercrime Convention in 2002, but as yet has not ratified the convention. And as seen in the earlier paragraph, local legislation doesn't seem to hold water when it comes to obliging former employees of an organisation to disclose encryption passwords they have secured material with.

Intellectual Property – Irish law meets the requirements of leading international texts such as the Berne Convention, the TRIPS Agreement and the 1996 Geneva Copyright treaties, as well as all relevant IP European Union Directives. Ireland is also a member of the WIPO Copyright Treaty. Ireland is one of the world's largest exporters of computer software and appropriate protections have been enshrined in Irish law to protect Intellectual Property Rights (arthurcox.com 2010). Moreover, as recently as February 2012, the Irish government signed into law the European Union (Copyright and Related Rights) Regulations 2012, these regulations provide an explicit mechanism that will enable copyright right holders to seek an injunction against an intermediary service provider which provides facilities that may be used by third parties to infringe their copyright.

Conclusion – The Irish government sees rapid cloud adoption by business as a key driver of the 'smart economy'. In 2009 the then Minister for Communications, Eamon Ryan identified cloud computing as one of the six 'pillars' that would drive the creation of a smart economy. Mixed messages regarding cloud computing have since emerged from within government departments. The chief state solicitor's office in 2010 issued notice to public servants that "*issues such as data protection, confidentiality and security and liability are not necessarily dealt with in a manner that would be necessary for public-sector responsibilities by cloud services*" (tjmcintyre.com 2010). The government has since attempted to row back a little on the advice from the state solicitor, and government advisors have apparently moved to soothe the nerves of some of the major technology multinationals based here. In respect to the three policy categories with which cloud computing law in Ireland has been evaluated, Ireland definitely seems to have adequate IP policies and procedures in place to protect right holders in cloud computing environments. There also seems to be adequate Data Privacy and Data Protection law, to ensure data subject's rights will be upheld. However, a lack of explicit, up-to-date cybercrime law in Ireland will potentially hamper uptake of cloud by customers wary that computer crime in Ireland will go unpunished.

5.3.2 America

Data Privacy – As mentioned in a previous section America has a sectoral approach to Data Privacy and Data Protection. A wide range of privacy protection statutes has been enacted to regulate specific forms of information handling, but there are numerous gaps and overlaps in the coverage of these laws. America has no comprehensive laws that cover the protection of personal data. Combined with the sectoral laws, America uses rules on self-regulation of certain industries and a number of technological programs or systems that are designed to safeguard users' privacy (De Busser 2009). America does offer a version of the European Data Protection Directive known as US Safe Harbour (as discussed previously), but this scheme excludes some large business categories such as the financial services and telecommunications industries. Moreover, as the scheme is self-regulatory, enforcement and compliance differs from organisation to organisation.

Security and Cybercrime – America has comprehensive and up-to-date laws in place for e-commerce, and electronic signatures, these include the Uniform Electronic Transactions Act 1999 and the Electronic Signatures in Global and National

Commerce Act 2000, both providing for the legal equivalence of paper records for electronic records and signatures.

ISPs are free from mandatory filtering and censoring. According to the BSA, there are no general security requirements in US law. However, the numerous sectoral security requirements (mentioned earlier), along with standard consumer protection laws provide security assurances for citizens.

America has also signed and implemented the Convention on Cybercrime. There are also other relevant statutes in America dealing with cybercrime including the Federal Computer Fraud and Abuse Act (CFAA). The Patriot Act mentioned in earlier sections of this document also contains provisions dealing with computer-related crime.

Intellectual Property – America became a member of the TRIPS agreement in 1995 and has implemented the agreement in its copyright legislation. America is also a member of the WIPO Copyright Treaty. Legislation such as DMCA, the Digital Millennium Copyright Act, implements two 1996 treaties of the World Intellectual Property Organization (wikipedia.org DMCA). DMCA allows for take-down notices to be issued to ISPs found hosting or facilitating the illegal copying and distribution of copyrighted material. Sample legal cases such as the one proffered in earlier sections regarding Megaupload demonstrate the sincerity with which the American department of justice perceives IP issues.

Conclusion – Security and cybercrime considerations relating to cloud computing seem to have been well legislated for in America. Data privacy and protection laws though don’t seem to have been comprehensibly catered for, there are no definitive laws relating to intellectual property (comparable to the European Data Protection Directive). IP issues also tend to be well catered for in America. Recent negative public reaction to the proposed SOPA and PIPA legislation though may perhaps be indicative of future problems for American courts in dealing with IP issues relating to cloud.

5.3.3 The United Kingdom

Data Privacy – As a member of the European Union the United Kingdom did adopt the European Data Protection Directive, and transposed it into UK law with the Data

Protection Act of 1998. However debate has raged as to the way and manner in which the directive has been transposed into UK law. As late as June 2010, the European commission wrote to the UK authorities requesting the '*UK to strengthen powers of national data protection authority, as required by EU law'* (europa.eu UK). The United Kingdom is also a member of APEC, and has an independent data commissioner's office. One point of note though, is that data controllers are obliged under UK law to register their datasets with the data commissioner and must notify that office of their intention to process personal data. This requirement may be seen by some cloud vendors as unnecessary red tape, and may be regarded as an obstacle to some cloud services. In has also been recently reported that under a new proposed law Internet providers in the United Kingdom will have to install hardware at all ISP sites to allow the Government Communications Headquarters (GCHQ) access to the personal information (torrentfreak.com 2012). This will be seen by many as an attack on personal privacy, but is something seen by the UK government as vital so that security forces are able to obtain communications data in certain circumstances to investigate serious crime and terrorism.

Security and Cybercrime – The UK is a signatory to the Convention on Cybercrime, but only ratified the agreement in 2011, and the government is still criticised for not adopting an important component of the treaty relating to the misuse of devices, as required by Article 6 of the Convention (BSA 2012). Laws exist which give legitimacy to electronic signatures and documents (The Electronic Communications Act 2000). Filtering and monitoring of ISP traffic has to date not been in place. But the previously mentioned proposed law on the government having access to personal information may put a black mark on the United Kingdom's Internet Security reputation.

Intellectual Property – The United Kingdom became a member of the TRIPS agreement in 1995 and has implemented the agreement in its copyright legislation. The United Kingdom is also a member of the WIPO Copyright Treaty. There is an advanced set of IP laws that implement the WIPO Copyright Treaty provisions in the UK. There is scope in some of this legislation to ensure ISPs can be held liable for content that infringes copyright.

Conclusion – The UK is a member and has ratified all relevant international treaties on Data Privacy (European Data Protection Directive, APEC), cybercrime (The Cybercrime convention) and IP (TRIPS, WIPO). Sufficient local laws seem to be in place to implement the provisions in these treaties, and the laws seem to be regularly enforced. New regulations being proposed compelling ISPs to record and hand over personal customer data is a retrograde step from a cloud computing perspective though.

5.3.4 Canada

Data Privacy – Canada is deemed to have quite strong Data Privacy laws in place. The main law covering Data Privacy and Protection is the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. Canada is one of a small list of countries that the European Union deems as providing an adequate level of protection for personal data, and under the European DPD data is permitted to be transferred to Canada. Also as a member of APEC, Canada is an active participant in several APEC privacy initiatives (BSA 2012). Canada also has an Office of Data Commissioner, similar to Ireland and the UK, this office is known as the Office of the Privacy Commissioner of Canada, and this office acts as the national regulator for data privacy issues.

Security and Cybercrime – The Canadian Uniform Electronic Commerce Act (UECA) 1999 provides for recognition of electronic signatures. ISPs are not hindered from filtering or censorship by government. Canada has signed the European Convention on Cybercrime, but surprisingly has not yet ratified the treaty. In 2008 Deloitte carried out a report on cybercrime in Canada, and during the course of their investigation interviewed several key government agencies to gather information on cybercrime law, One government official, when asked about Canada's failure to ratify the European Convention on Cybercrime noted; "*We're not there in terms of the Canadian legislation, we have signed onto this Treaty, but we can't ratify as a Nation, until such time as we have the legislation in place in the Criminal Code that will allow us to respect every aspect of that Cybercrime Convention*" (capb.ca 2008).

Bills are currently going through the Canadian parliament in order to cater for the adoption of the Convention on Cybercrime, but those proposed bills are also subject to debate. In a letter to the Canadian Prime Minister Canadian privacy scholars and civil society organisations questioned the adoptions of the new legislation; "*We are particularly concerned that three of those bills will have serious negative implications for the privacy rights of Canadians*" (cippic.ca 2011).

Intellectual Property – Canada did become a member of the TRIPS agreement in 1995, but the country has not ratified the WIPO copyright agreement (one of the few developed nations not to have done so). The Copyright Act of Canada, first published in 1921, was amended in 1988 and 1997 but has not been amended since then. There are no sanctions or policies in place punishing or ordering ISPs to take down infringing content. Canada has been criticised for not updating its copyright laws, and even made America's 'priority watch list' of countries with the worst records of preventing the theft of copyrighted material (timesofindia.indiatimes.com 2012).

Conclusion – Canada will certainly encourage cloud customers concerned about the protection of personal data to allow their content reside in the country. The Data Privacy and Protection laws in place in Canada are certainly comparable to the best practice adopted in the European Union. On matters of Security, Cybercrime and IP, cloud vendors and customers may not be completely enthused. Serious gaps exist within Canadian law in respect to Cybercrime and IP. Recent bills going through parliament to address these issues are encountering obstruction. It remains to be seen what policies and regulations the country manages to put in place in the coming years to overcome these issues.

5.3.5 Russia

Data Privacy – The BSA suggest Russian privacy law is complicated and the inconsistencies and complexity presents barriers for both consumers and business (BSA 2012). Russia is a signed up member of the APEC Privacy Principles, but has refused to participate in any of the 'pathfinder projects'. Greenleaf describes the Pathfinder projects as having "*the goal of developing and implementing an accountable Cross-Border Privacy Rules (CBPR) system within APEC*" (Greenleaf 2009). Russia does have a regulator tasked with the enforcement of privacy laws, known as the Roskomnadzor. The Roskomnadzor periodically monitors activities of personal data operators, and therefore data protection laws and regulations are actively enforced (practicallaw.com 2011).

Security and Cybercrime – Laws giving legal rights to electronic signatures were adopted in Russia in 2002 (russianlaw.net 2005). Russia imposes no censorship or filtering on ISPs, but recent quotes from the Interior Ministry following protests after the general elections in Russia in December 2011, are broadly seen as a crackdown on broader government criticism. Major-General Aleksey Moshkov said, "*Social networks, along with advantages, often bring a potential threat to the foundations of society."* (eff.orgt 2011). Russia has not signed the European Convention on Cybercrime, but in spite of this it does have local legislation dealing with computer crime.

Intellectual Property – Russia is not yet a member of the TRIPS agreement, the country commenced its application for WTO membership in 1993 but is scheduled to be accepted in 2012 (wto.org Russia). The WIPO Copyright Treaty came into force in Russia in 2009. Details in respect to ISPs being forced to remove copyrighted material, or being prosecuted for hosting copyrighted material are patchy. Sample cases have occurred where the court concluded that the ISP was not responsible for the use of copyrighted material (jipitec.eu 2008). But other cases have arisen where the ISP has been held accountable for the infringing material (whioam.com 2010).

Conclusion – Data protection legislation in Russia seems to be adequate, and cybercrime legislation provides a moderate level of protection. But legislation in relation to intellectual property protection is patchy and may expose cloud computing services to risk, these gaps in IP legislation and enforcement need to be addressed.

5.3.6 China

Data Privacy – China has not yet enacted comprehensive laws or regulations governing the collection, use and transfer of personal data (mondaq.com 2011). Mondaq.com continue by commenting that although a draft *Personal Information Protection Law* has been pending since 2003, some observers are pessimistic about the likelihood of its enactment in the near future due to the complicated interplay between privacy protection and disclosures in the Chinese political system (mondaq.com 2011). China has not signed up to the APEC privacy principles. A Data Commissioner/regulator is not in place.

Security and Cybercrime – The Electronic Signature Law 2005 gives electronic signatures the same legal standing as handwritten signatures and seals (BSA 2012). China does recognise the legal standing of electronic signatures and documents. China is regarded as one of the Internet's 'black holes', signifying an area on the globe where censorship and filtering of Internet traffic is mandatory for ISPs. The apparatus of the People's Republic of China's Internet repression is considered more extensive and more advanced than in any other country in the world. The governmental authorities not only block website content but also monitor the Internet access of individuals (wikipedia.org China). China has not signed the Convention on Cybercrime but does have a host of local legislation that prohibit the unauthorised entry and use of computer systems.

Intellectual Property – China became a member of the TRIPS agreement in 2001, as yet though not all provisions have been adopted. The WIPO agreement has also been adopted by China and entered into force in 2007. Laws exist which hold ISPs responsible for copyrighted material and there are enforcement processes for ensuring ISPs remove infringing material.

Conclusion – China falls far short of International standards from a Data Privacy and Protection perspective. Legislation is under review that may plug the gaps in these policy areas, but much work needs to be done in this area for China to be seen as following best practice. In spite of the failure to ratify the Convention on Cybercrime, China has adequate cybercrime legislation in place. Unfortunately the extensive filtering and censorship of Internet data by ISPs is a huge negative for China's ICT sector, sure to act as a deterrent to cloud providers looking to use data centers in the country for cloud services. There does appear to be extensive IP legislation in place to ensure adequate protection for copyrighted material, but the enforcement of these laws poses significant challenges.

5.4 Legal Cloud Matrix

The following table attempts to represent the policies and regulations the six sample countries have in place in relation to cloud computing. By looking at the matrix it should be simple to determine where countries fall down or excel in the respective policy area affecting cloud. A legend is provided to explain the acronyms used.

Country	Data Privacy	Intellectual Property	Security & Cybercrime
Ireland	DPD implemented DP acts exceed APEC NR in place	TRIPS member WIPO full Signed ACTA	No Internet CEN ISP takedown ES recognition CoC member
America	Safe-Harbour APEC compliant SR in place	TRIPS member WIPO full Signed ACTA	No Internet CEN ISP takedown ES recognition CoC member
Russia	APEC compliant NR in place	WIPO full	No Internet CEN ES recognition
United Kingdom	DPD implemented DP acts exceed APEC NR in place	TRIPS member WIPO full Signed ACTA	No Internet CEN ES recognition
Canada	DPD compliant APEC compliant NR in place	TRIPS member WIPO – Not Ratified Signed ACTA	No Internet CEN ES recognition CoC – Not Ratified
China	Considering APEC	TRIPS member WIPO – Only Some Regions	CEN ISP takedown ES recognition

Table 5.1: Cloud Legal Matrix

5.4.1 Matrix Legend

ACTA	Anti-Counterfeiting Trade Agreement treaty
APEC	Member of the APEC Privacy Principles framework
CEN	Internet censorship taking place
CoC	Signatory of the Convention on Cybercrime
DP	Data Protection
DPD	European Data Protection Directive
DPD compliant	Country deemed to provide adequate protection for personal data by the European Union
ECC	European Convention on Cybercrime treaty
ES Recognition	Full recognition in the law exists for electronic signatures and documents
ISP takedown	Laws are in place ensuring ISPs remove material infringing copyright
NR	National Regulator responsible for enforcement of Data Protection policies
Safe-Harbour	US Safe Harbour policy in place to ensure compatibility with the DPD
SR	Sectoral (dealt separately by different industries) Regulator responsible for enforcement of Data Protection policies
TRIPS	Trade Related Aspects of Intellectual Property Rights treaty
WIPO	World Intellectual Property Organisation (WIPO) Copyright treaty
WIPO full	WIPO Copyright treaty fully signed and ratified

Table 5.2: Matrix Legend

5.5 Conclusion

This chapter has attempted to compare and contrast the different international perspectives on cloud computing. As noted earlier, little (if any) 'cloud law' exists. The perspective a country has on cloud computing can be gauged by analysing the policies and regulations that a country has in place for laws which affect the adoption, implementation and processing of cloud services. This chapter chose three policy areas with which to analyse jurisdictional cloud perspectives; Data Privacy, Intellectual Property and Security/Cybercrime. Due to the limitations of this document, only six countries were analysed under these policy areas. There are some similarities in the six countries chosen; all for example are members of the Asia Pacific Economic Cooperation group's Privacy Principles framework (China is at least considering APEC). But major differences between international policies can also be seen, Canada for example has not signed the World Intellectual Property Organisation (WIPO) Copyright treaty nor does it compel ISPs to take down infringing copyrighted material.

Technologies are now being advanced which will give cloud customers and vendors the ability to choose which jurisdictions their cloud service can avail of. But with little knowledge of the policies and regulations affecting cloud in different jurisdictions, cloud customers and vendors may find it confusing deciding which countries to consider including in their cloud service architecture. To aid comprehension and awareness of jurisdictional perspectives on cloud, a Cloud Legal Matrix has been provided in this chapter. This matrix is given physical form in a tangible artefact accompanying this document.

6. TECHNOLOGIES AROUND THE CLOUD

6.1 Introduction

Chapter five of this dissertation attempted to give some clarity to the different perspectives that exist in six sample countries with respect to legal policies and regulations affecting cloud. The cloud legal matrix resulting from chapter five can be used as a basis for informing cloud customers which jurisdictions would be suitable places to permit their data reside. Chapter eight will move towards providing other solutions to the legal shortcomings posed by cloud computing. Education and training for example can go a long way toward helping individuals understand the legal issues thrown up by cloud and how to avoid those issues. Business process maturity, i.e. the extent to which an organisation's processes and procedures are sufficiently mature and understood, also plays a part in determining if an organisation is capable of overcoming the legal shortcomings of cloud computing, and is 'cloud ready'. These concepts will be discussed further in chapter eight.

Technology though has a large part to play in assisting organisations and cloud vendors overcome some of the legal uncertainties that cloud computing brings about. Geotagging, the process of adding geographical identification metadata to various media will be put forward in chapter eight as technology that can form part of a technological solution to cloud jurisdictional issues.

Before advancing technology as a means of overcoming legal issues in cloud computing, it is important to have a more in-depth, broad technical understanding of cloud. To that end, this chapter will explore in more detail the infrastructure of a cloud computing environment. In chapter two the cloud delivery models, IaaS, PaaS and SaaS were explored, as were the cloud deployment models, Private, Public, Community and Hybrid cloud deployment. This chapter will attempt to explain in more detail how these services are provisioned (or orchestrated) by cloud vendors. The technology used to manage these cloud services, and the means by which these services are secured will also be explored. Geotagging technology will play an important role with databases residing in cloud environments, so the databases used in the cloud will also be examined in this chapter. Finally chapter six will explore the technical shortcomings that exist in the cloud computing environment.

6.2 Infrastructure

Earlier in this document, the definition of cloud computing by the NIST was put forward; *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources..."* Building on the NIST's definition of cloud computing, the following diagram in figure 6.1 (again from the NIST) demonstrates the fundamental high-level architecture of a cloud computing environment.

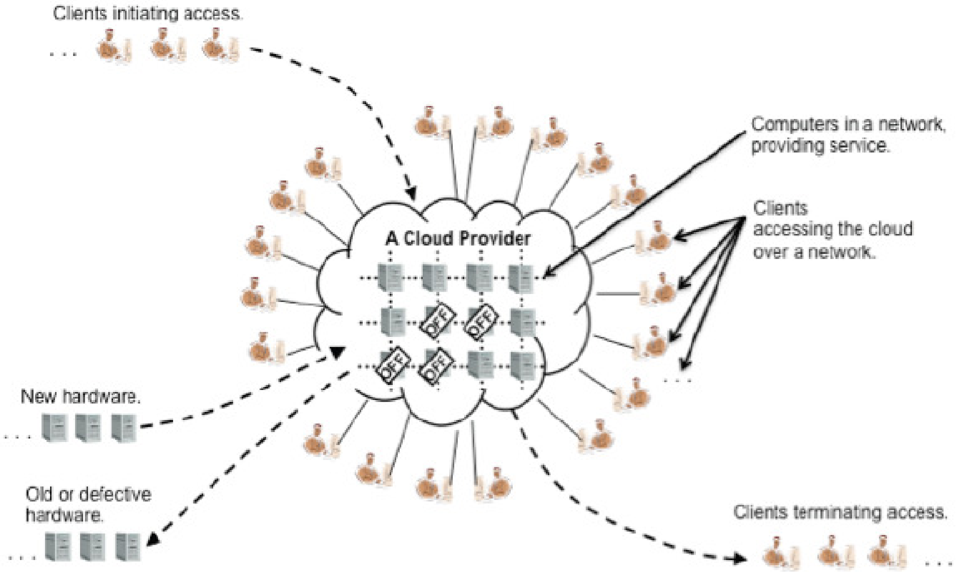

Clients initiating access.
Computers in a network, providing service.
A Cloud Provider
Clients accessing the cloud over a network.
OFF
New hardware.
Old or defective hardware.
Clients terminating access.

Figure 6.1: General Cloud and Subscriber View (Draft NIST SP800)

Figure 6.1 is fairly simplistic in terms of the detail it presents, but nevertheless highlights some of the fundamental components and activities that define cloud computing. The cloud's resources are portrayed as a networked grid of computer systems. Clients can access this cloud via network connections. Clients initiate and terminate sessions with the cloud environment, meaning the number of clients using the cloud resources at any one time is variable. Likewise, the cloud vendors must maintain a pool of hardware resources to maximise services and minimise costs. Hardware will fail, it will become obsolete and redundant and in order for a vendor to maintain a high availability of service, must be upgraded from time to time. Existing functional hardware is also managed to provide services cost effectively. The NIST suggests that in practice, customer workloads are moved within the cloud environment;

"*Whether for power management, or for hardware refresh, migration of customer workloads (data storage and processing) from one physical computer to another physical computer is a key strategy that allows a provider to refresh hardware or consolidate workloads without inconveniencing subscribers*." (Draft NIST SP800).

The following diagram (Figure 6.2) from kurzweilai.net (kurzweilai.net 2010) depicts at a lower level the main components that make up a typical cloud computing infrastructure. The cloud provider not only provides the delivery services (IaaS, PaaS etc.), but must also manage the resource abstraction technology running in the control layer, this typically constitutes virtualisation software running in what is known as the hypervisor layer. Hardware and facilities are also catered for by the vendor, as are cloud management services, usually involving software to manage the provisioning of resources to clients, providing business support systems and ensuring security mechanisms are in place and maintained.

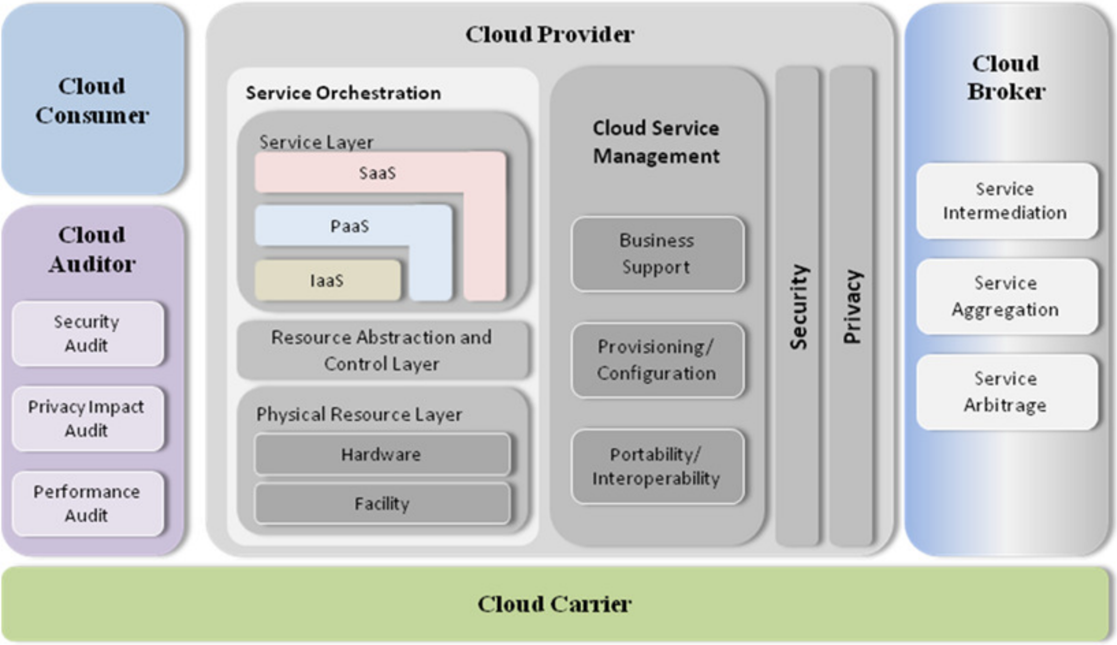


Figure 6.2: High Level Cloud Architecture (kurzweilai.net)

In chapter two of this document, the cloud delivery models were discussed at a very high level. In an effort to look more closely at cloud infrastructure depicted in Figure 6.2, in this section it is necessary to look at those delivery models at a more microscopic level, investigating what they provide and how each are managed by the cloud provider.

6.2.1 Service Orchestration

SaaS - SaaS can be considered to be at the top of the service delivery stack. With SaaS, the cloud provider will control most of the software stack, and the cloud customer will only possess control over the application-specific resources that a SaaS application makes available, Figure 6.3 from NIST depicts the scope of control between the SaaS provided and the subscriber/consumer;

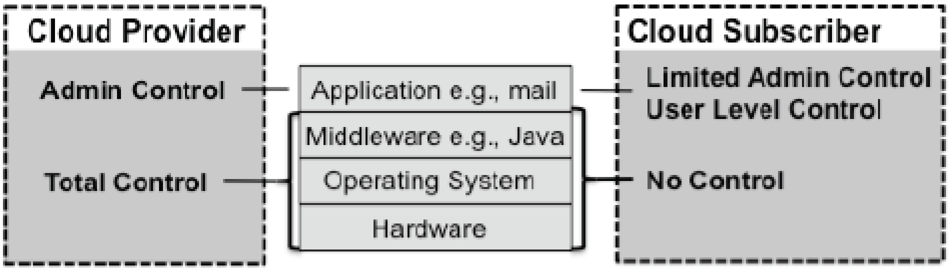


Figure 6.3: SaaS Provider/Subscriber scope of control (Draft NIST SP800)

A good example of this model is Google's email offering, Gmail. Gmail is a SaaS offering that will allow the consumer very limited control over the software service. General settings can be managed for the user's own email account, but no access can be availed of to gain control over lower layers of the cloud infrastructure. Taking this a step further might be a situation where an organisation signs up to Google's online collaboration suite. In this instance IT administrators from the consumer's organisations might have more control in respect to setting up and deleting user email accounts, but that is where the extent of control ends.

With SaaS, the computer application is being rented from the cloud provider. Access to that application is over a network connecting the SaaS provider with the cloud customer/consumer. In a public cloud deployment model, most application program logic is executed on the cloud provider's servers. The NIST describe the consumer's browser as providing: (1) the subscriber interface that captures subscriber keystrokes and other inputs, and produces output in the form of graphics/sound, and (2) the data export that outputs data to local storage devices such as USB devices or printers. Obviously application data exchanged between the consumer and cloud vendor need to be secured, so cryptography is usually used.

Managing the SaaS Service – Figure 6.4 demonstrates how the SaaS service is managed; in a typical configuration the SaaS application concurrently serves multiple clients and saves the data in a combined database. It is common for the SaaS application to be processing data belonging to multiple clients at a single time, so this configuration needs careful engineering to ensure different clients data is kept separate. Scheduling issues must also be managed to prevent the actions of one client from degrading the performance experienced by another.

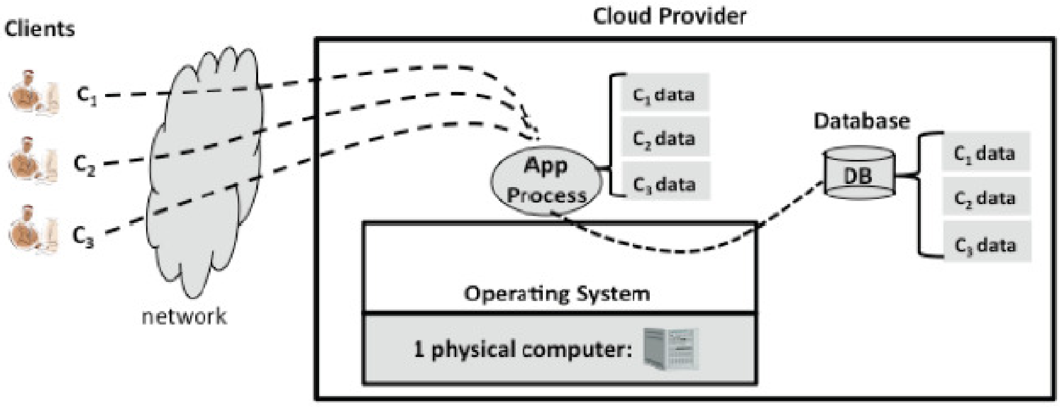


Figure 6.4: Managing the SaaS service (Draft NIST SP800)

PaaS - The next layer on the delivery stack, PaaS offers more than just a software application to cloud customers. Here, an application development environment is made available; customers can build, test, deploy and run applications in this layer. Oracle for example offers a PaaS service where clients can build and test their PLSQL or Oracle Forms applications in the PaaS cloud environment. But an advantage in Oracle's PaaS offering is that it is built on top of an Oracle database, if customers decide to move their applications back from Oracle's public cloud into their own private cloud environment, there are no compatibility or lock-in issues.

The following diagram shows the scope of control between Cloud provider and subscriber in the PaaS delivery model.

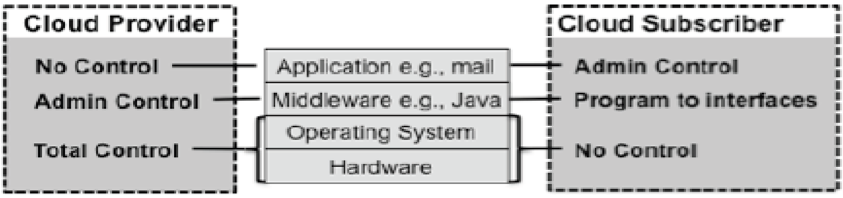


Figure 6.5: PaaS Provider/Subscriber scope of control (Draft NIST SP800)

Similar to the SaaS model the provider operates and controls the lowest layers, but unlike SaaS at the middleware layer, the provider makes programming and utility interfaces available to the subscriber.

Managing the PaaS Service – Figure 6.6 demonstrates how the PaaS service is managed; Clients will typically make use of development tools made available by the provider, they will use these tools to build applications, A, B, C and D in the diagram. The provider will also make available a number of execution environments, exr1, exr2 ... these are the environments where newly developed applications (A, B, C) will run. Figure 6.6 also demonstrates an administrator configuring the new application that has been made available, and client, C1 and C2, are shown using the new application.

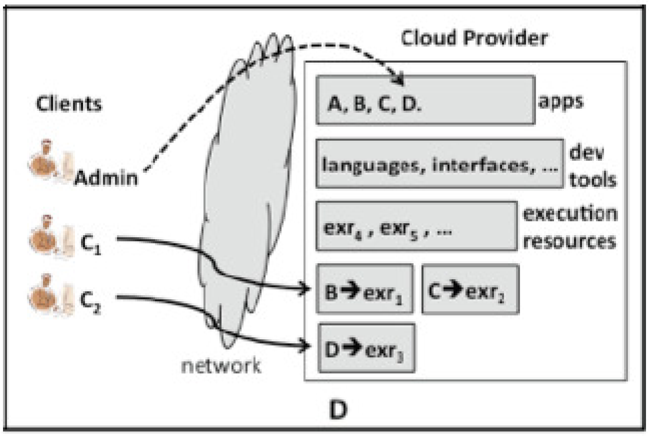


Figure 6.6: PaaS Service management (Draft NIST SP800)

IaaS - With the IaaS delivery model, cloud infrastructure in the form of virtual machines is made available to the cloud subscriber. Typical IaaS cloud systems also provide persistent data storage and stable network connectivity. Figure 6.7 shows the scope of control between Cloud provider and subscriber in the IaaS delivery model.

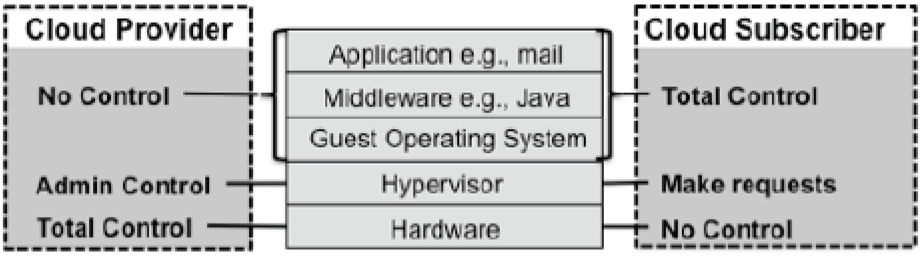


Figure 6.7: IaaS Provider/Subscriber scope of control (Draft NIST SP800)

As shown in Figure 6.7, the provider maintains control over the physical hardware and administrative control over the resource abstraction (hypervisor) layer. The subscriber makes requests to the cloud to create and manage new virtual machines (VMs). Through the hypervisor layer, the cloud provider will typically provide interfaces to networking features that subscribers may use to configure custom virtual networks within the provider's infrastructure. The subscriber will typically maintain complete control over the operation of the guest operating system in each VM, and all software layers above it (Draft NIST SP800).

Managing the IaaS Service – Figure 6.8 demonstrates how the IaaS service is managed by the cloud provider; In part A, Clients A and B access a number of virtual machines made available by the cloud provider. In part B of the diagram, a new client, C, accesses the cloud environment and the provider makes more virtual machines available from the virtual resource pool.

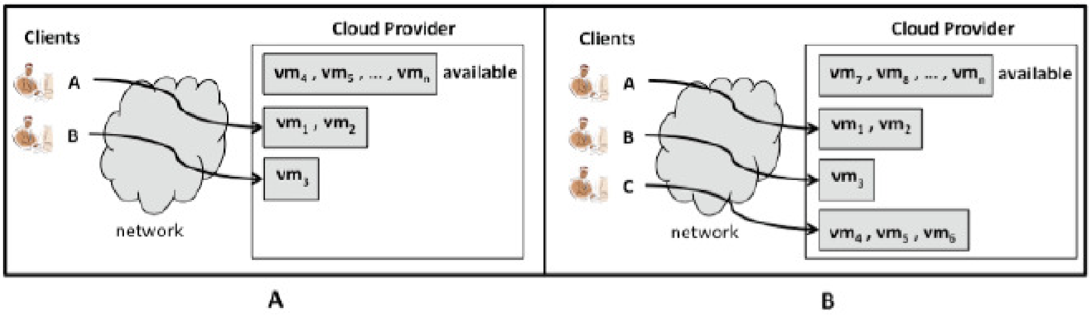


Figure 6.8: IaaS Service management (Draft NIST SP800)

6.2.2 Technologies Used to Manage Cloud Services

Figure 6.2 in the previous section gave a depiction of the main components that make up a typical cloud computing infrastructure. A core element of that architecture is the cloud management services. This element of the cloud infrastructure comprises software and technologies designed for operating and monitoring the applications, data and services residing in the cloud environment. Cloud management strategies typically involve numerous tasks including performance monitoring (response times, latency, uptime, etc.), security and compliance auditing and management, and initiating and overseeing disaster recovery and contingency plans (webopedia.com). Figure 6.9 illustrates in more detail the elements that make up cloud management services.

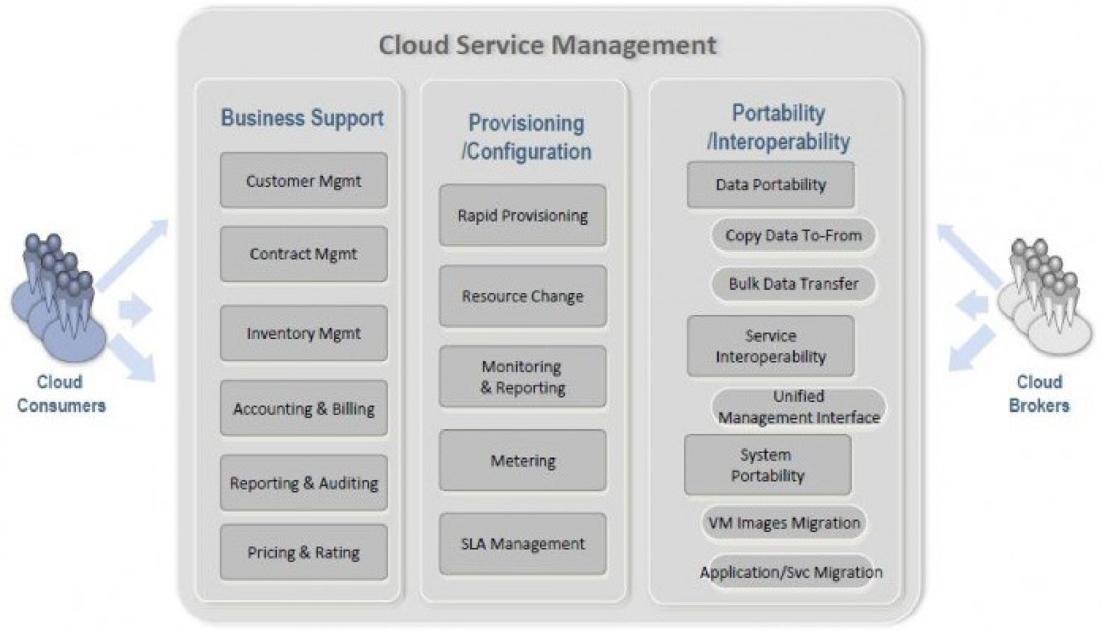


Figure 6.9: Cloud Service Management (NIST SP500-291)

The NIST break this model of cloud architecture into the three components depicted in Figure 6.9, but other cloud vendors and institutions define cloud service management in just two terms, *Business Support Services (BSS) and Operational Support Services*.

Business Support Services comprise all the software systems that play a key role in supporting the cloud customer's business activities. These range from automated billing systems, reporting facilities enabling clients view usage figures, customer management systems helping cloud vendors keep track of all customer data and more. Most large cloud vendors offer their own propriety software for handling BSS, but cloud management software is a relatively new phenomenon, Microsoft and others are acquiring smaller independent software houses that specialise in this type of software.

The prominence of virtualisation technology in cloud computing has increased the need for Operation Support Systems. With virtualisation technology cloud vendors can quickly create and deploy 'virtual' instances of a physical hardware devices, operating systems or network resources. This gives cloud vendors the 'elasticity' needed to respond to sudden demand for resources, but also to power down devices when they are not in operation. This 'provisioning' or 'orchestration' of virtual devises needs to be carefully managed though, and this is where Operation Support Systems step in. Software in this area also needs to ensure client service level agreements are being adhered to.

The software also needs to be able to capable of administrating a pool of physical computer devices, and for compliance purposes be able to manage what physical locations instances of virtual machines should be created in. This software service would also control and determine where data is transferred to, depending on where and when alternate resources became available.

Technology companies VMware, Intel and RSA are currently working on an embodiment of this type of cloud management technology. Leveraging Intel's TXT capability (which builds geolocation technology into the processing chip) with VMware's vSphere and RSA Archer cloud management tools, engineers have managed to build a concept capable of satisfying the most stringent compliance concerns. The technology proposed will allow cloud vendors work with clients to determine a set of geographical locations where client's data should be permitted to reside. The technology will allow VMware systems running in the hypervisor read geolocation information coming from the Intel chip, and based on that set of pre-determined 'safe' locations agreed between cloud vendor and client, the virtual machine will boot or not.

The bulk of other cloud management software functioning in the OSS sphere is dominated by a few key players, Amazon Web Services, RightScale, CA technologies and HP.

6.2.3 Securing Cloud Services

When an organisation runs and owns its own IT operations it will usually undertake a number of measures to ensure data and systems are secure. When that organisation subscribes to a cloud all the data generated and processed by that organisation will physically reside in premises owned and operated by a provider. In this context the NIST declare the fundamental issue at hand, is whether a subscriber can obtain an assurance that a provider is implementing the same or equivalent controls as to what the subscriber would have implemented (Draft NIST SP800).

Two fundamental security principals pertain to cloud computing, first, protecting the confidentiality and integrity of data, and second, ensuring data availability. The following section will list the areas of security vulnerabilities that can exist in a cloud environment, and will analyse how cloud providers are using security best practices to mitigate these risks and ensure the two fundamental security tenets in the cloud are provided for.

Isolation of networks – savvis.com suggests that the first responsibility of the cloud provider is to provide a level of isolation between all of the different networks that are part of the virtualisation infrastructure (savvis.com 2009). Virtualisation technology is used extensively within a cloud environment. Different customer's data can reside on the same physical device, but exist within different virtual machines. It is paramount that different customer networks are kept isolated. To achieve this separation, cloud administrators use a variety of methods; Virtual network switches in conjunction with network interface controllers (or NICs) that physically connect devices to the network can be used. Furthermore, firewalls are created between different networks in order to prevent any potential of traffic being routed accidentally between each other.

Isolation of management networks – Cloud providers access and manage cloud infrastructure via a cloud infrastructure management network. Again it is crucial that this network is properly secured from unauthorised admin staff, and of course from other cloud clients. Firewalls and physical network switches that separate the network environments again control security in this sphere.

Secure customer access to cloud-based resources - Where different clients attempt to access shared resources in a hosted environment, it is imperative that each set of customers are able to access and manage their own resources in a secure manner. To facilitate these needs cloud providers typically provide customers with a management portal that is encrypted. SSL encryption is often used for this task.

Secure, consistent backups and restoration of cloud-based resources – Depending on the cloud contract, backup and restoration services can be provided by the cloud provider. Where these services are part of a cloud contract, the cloud provider needs to provide the customer with a secure backup mechanism to allow the customer's cloud based resources to be backed up on a consistent basis and enable fast restoration in the event of downtime (savvis.com 2009). Cloud providers use the snapshot and cloning capabilities of virtualisation technology to accomplish these backup and restoration tasks. With these types of tools, providers can backup and restore not only client data, but also operating systems and applications running within those operating systems.

Strong authentication, authorisation and auditing mechanisms – A typical public cloud computing environment involves sharing of resources. It is therefore critical in this type of environment to properly authenticate system users and administrators. These individuals need only be provided with access to resources they need to carry out their approved duties. Cloud customers also need to have a mechanism of granting internal administrators access to resources. A logging mechanism, tracking what individual has accessed what resource also needs to be part of cloud security functionality. Cloud providers use a variety of proprietary and non-proprietary software to manage these tasks, following best practices laid down by the Security Technical Implementation Guide (STIG) and the Centre for Information Security (CIS).

A library of secure and up-to-date templates of base OS and applications – Misconfiguration of software within a cloud environment can lead to security holes emerging. To prevent this from happening, cloud providers use securely configured templates, or the 'gold image' of an operating system. These templates need to be kept up to date with all necessary security patches and anti-malware signatures. This 'gold templates' concept can be used in conjunction with lifecycle management tools to ensure proper approval is obtained before a virtual machine is provisioned; virtual machines can for example only be provisioned from a known, good template, approved by senior admin within the lifecycle management process.

Resource management to prevent denial of service (DoS) attacks – Another important aspect of security in a cloud environment is ensuring the continuity of service. If a client has paid for a service, it is the provider's responsibility to ensure that service is reliable and constant. DoS attacks seem to be a common mechanism used by cyber criminals to disrupt services in a hosted environment. Resource management in the cloud has an important part to play in preventing the potential of DoS attacks. If a virtual machine within the cloud is comprised by such an attack, resource management tools can be used to isolate that virtual machine, ensuring the attack does not spread to other machines within the cloud environment.

Cloud providers also rely on customers to follow security best practices when interacting with a cloud service; customers for example are encouraged to encrypt data they move to the cloud, data both at rest and in transit. Customers particularly availing of IaaS and PaaS services are expected to follow security best practices; cloud vendors will for example expect the customers to secure operating systems and applications that reside in the cloud to the same degree users would secure such resources in their own private environments.

6.3 Databases in the Cloud

Traditionally, relational databases were not deemed a good architectural fit for the cloud computing environment. Relational databases can be difficult to scale, they can be difficult to distribute, and the 'shared nothing' approach to traditional database architecture flies in the face of the elastic, virtualised, rapid scalability promises of cloud providers. Technological advances in the last decade have considerably contributed to removing some of these barriers to database migration to the cloud. In this section, these technological advancements will be explored. Whether these advancements are enough to remove all obstacles for the arrival of full, robust, feature rich DbaaS (Database as a Service) services will be discussed. Moreover, even if it is now much more feasible for an organisation to have its relational database system in the cloud, doesn't mean it makes commercial or practical sense to do so. The commercial and business concerns related to moving mission critical databases to the cloud will be covered in this section. And finally this section will take a look at the DbaaS services that exist in the market place.

6.3.1 Paving the way for Cloud Databases

Shared nothing architecture (SN) has been the price performance leader for database construction for decades. In this model, Shared-nothing databases split or partition the data so that each database server exclusively processes and maintains its own piece of the database. Shared disk (SD) architecture on the other hand is analogous to a single large trough of data, where any number of database nodes can process any portion of that data (scaledb.com 2009). SN architecture suited relational database architecture for multiple reasons, these reasons tended to preclude DBMS for the cloud, but that is changing:

Firstly Ethernet connection speeds, typically of 10Mbits, were far slower than the disks themselves, therefore drastically degrading connectivity between nodes if the database was architected in a shared-disk manner. Today though, Gigabit over Ethernet is standard, meaning shared-disk DBMS no longer lag behind the SN model in terms of performance.

Storage performance was another reason why the cloud environment didn't tend to make sense for the relational database. CPUs are obviously faster than the drive head on a storage disk, so it never made sense to distribute data across multiple disks. Faster media storage is now available though, and stripping the data across multiple disks has helped eliminate the constraints imposed by drive head movement (scaledb.com 2009).

Storage performance has increased, but the concept of Shared-nothing still proved attractive as storage costs were typically expensive. The scale of cloud data centers now makes this a redundant issue. Where an organisation might have typically shunned paying upwards of a hundred thousand dollars for a new SAN, disk space rental from the likes of Amazon's relational database services (RDS) now costs as little as $0.21 per hour (amazon.com).

One of the main cost drivers of cloud computing has been virtualisation. Virtualisation is the ability to create, operate and manage computing instances independent of the underlying hardware. Unfortunately shared-nothing databases don't suit the virtualised environment; instead shared-nothing databases need to be hardwired to specific physical servers. You would therefore need to size these database servers for peak load, and incur that upfront cost. Shared disk architecture on the other hand fits quite well with virtualisation technology. The technologies described earlier, quicker Ethernet, cheaper storage, have paved the way for a moved towards shared disk DBMS, and are enabling customers reap the full cost benefit that virtualisation brings.

6.3.2 Commercial and Business Concerns

The technical enablers for database migration to the cloud have been covered in this section, but organisations must allow business drivers decide if cloud is the correct environment for the relational database. DbaaS can seem very attractive to an organisation, backing up and maintaining a complex database system can be an expensive task. In a cloud environment, tasks such as file allocation, memory management, and high availability configuration are handled by the provider. Furthermore, if the database only needs to be provisioned for a short period of time, and then dropped (perhaps for a retail promotional event), the cloud model can prove very beneficial.

Business might still be a little reticent though about moving mission critical databases containing highly sensitive data that is subject to compliance regulations such as PCI or HIPAA into a cloud environment. While Cloud providers have made large strides in improving the reliability and security of Cloud data centers, it's not clear that compliance market is ready to approve sensitive data being stored outside the enterprise's control (thecloudtimes.com 2011).

Other impediments to moving database technologies to public clouds also exist, bandwidth for example can be an issue if an organisation moves a heavily used transactional database to the cloud. Latency may not be an option for mission critical transactional systems. Compliance issues too, might preclude organisations from moving databases of sensitive data outside the company boundaries.

6.3.3. DbaaS in the Market Place

Cloud database offerings generally range across the SaaS and PaaS service areas. In a SaaS model, cloud customers generally have no visibility of the database being used behind the scenes. Salesforce.com for example uses an Oracle database as a backend to its CRM platform. Amazon.com offer a variety of relational databases services under its AWS umbrella, including Oracle, Microsoft SQL Server and MySQL, and also offers its own propriety database, SimpleDB. Microsoft's SQL Assure service offers developers a platform to build applications on top of their SQL Server database, without the overhead of having to set-up or manage the database. Oracle too, offer their proprietary database as a PaaS offering as do IBM with their DB2 database.

6.4 Shortcomings of Cloud Computing

In section 2.5 of this dissertation, 'Business and Marketing in Cloud Computing', the many advantages of cloud computing espoused by marketing companies were explored. Indeed cloud computing does offer advantages over more traditional computer models in many circumstances, lower upfront capital expenditure costs, on-demand provisioning of resources etc. Cloud computing is not without its shortcomings though. Some of these issues are not unique to cloud computing, but have become more relevant since the emergence of cloud computing. The NIST have grouped cloud 'open issues' under the following five headings:

6.4.1 Computing Performance

The nature of cloud computing usually means that subscribers are dependent on the performance of the Internet to interact with the cloud service. Internet round-trips can be affected by congestion, system failures etc., that are very much out of the control of the cloud providers. These potential latency issues will therefore not suit migration of all applications to a public cloud environment.

Fair distribution of resources can also be discussed under the computing performance heading. In a shared pool of resources, subscribers expect providers to meet agreed SLAs, even when other clients sharing the resource pool require expanded computing resources due to a workload spike. Due to the opaque nature of providers cloud environments, it is difficult for a client to ascertain if cloud resources are being distributed equitably.

6.4.2 Cloud Reliability

Often cloud solutions involve a complex set of layered solutions, Provider A providing a client with their SaaS service, may be relying on Provider B to provide it with a PaaS service, Provider B may be depending on Provider C for an IaaS service. This multi-layered dependency model can have an impact on the reliability of cloud services. Provider A can promise reliability to its clients, but this promise will obviously be dependent on the underlying services delivered to that provider.

As with performance issues, cloud reliability is particularly network dependent. For most clouds, the Internet must be continuously available for a subscriber to access services. Network disruption can and does occur for a variety of reasons; coverage limitations can present themselves (airplanes, remote locations). Internet outages are also a possibility, whether they be due to natural disasters, user error, cyber crime activities or hardware failures.

Cloud providers themselves experience outages that affect cloud reliability, due to exactly the same issues that affect regular Internet outages, malware attacks, power failure etc. The important points for cloud subscribers to consider in this scenario are, first, what frequency and duration of outage can be tolerated before the outages begin to have a serious business impact, and second, what contingencies has the subscriber in place to deal with a prolonged outage.

6.4.3 Economic Goals

It is natural in any business environment for companies to fail. Cloud vendors will go out of business. For customers of cloud businesses that have ceased operations, business continuity can be a potential problem. How will data be returned? How can operations be moved to another cloud environment?

Portability of client workloads also falls under the Economic Goals banner; an initial barrier to cloud adoption can be the need to move local workloads into a provider's infrastructure. And presumably the same issues would arise if a subscriber wished to move workloads between cloud providers. Achieving portability among providers is complicating further if different architecture used in each environment is vendor specific. The portability issues lead to interoperability issues between cloud vendors, common agreed technology standards must be developed in order for smooth transitions of workloads between providers.

Disaster recovery can also be a concern with cloud computing, and must be considered carefully. Disaster recovery plans are applicable to all hosted IT services, but the nature of cloud, where client workloads have the potential of being fragmented over multiple data centers and jurisdictions make the process more complicated and costly.

6.4.4 Compliance

As has been seen in other sections of this document, when data is moved into a cloud environment much of the data compliance responsibilities lie with the data controller, i.e. the subscriber. The reality of the situation though is that the cloud vendor may be better placed to enforce compliance rules. But several issues make compliance more complicated in a cloud environment.

Again due to the opaque nature of a cloud environment, subscribers can find it difficult to see if their services are being delivered and managed in a secure manner. Adequate process logging (potentially required under compliance obligations) is not always available or verbose enough to meet compliance demands. These issues should be addressed in SLA contractual negotiations.

The distributed nature of the cloud environment will bring about compliance problems too. State statues and directive mentioned earlier in this document place restrictions on the physical locations that data can be moved to. Compliance issues are further compounded when subscribers are obliged to conform to jurisdictional and regulatory edicts, such as the European Data Protection Directive, the Patriot Act, the Sarbanes-Oxley Act etc. NIST suggest, *"Subscribers, who are ultimately responsible for their data processed on provider's systems, will need to require assurances from providers that they are aiding in compliance of the appropriate regulations"* (Draft NIST SP800).

6.4.5 Information Security

Information Security was touched on earlier in this section in respect to securing cloud services. Security in the cloud falls under two headings, first, protecting the confidentiality and privacy of data and, second, ensuring data availability. Section 6.2.3 'Securing Cloud Services' identified some of the pertinent security issues peculiar to cloud environments and how cloud vendors attempt to mitigate those security risks. Risks do remain though.

In any multi-tenancy environment complex technologies exists in order to keep client environment separate. The risks of isolation failure will exist. NIST suggest that building confidence that logical separation is a suitable substitute for physical separation is a long-standing research problem (Draft NIST SP800).

Many cloud subscribers use Internet browsers to access the cloud environment. Browsers are complex software applications and have been shown to harbour security flaws. Moreover, clients access cloud environments with a variety of Internet browsers from different vendors. Functionality present in one browser may not necessarily exist in another. If a browser is subverted maliciously and this action goes unnoticed, the entire cloud environment could potentially be contaminated.

Cryptographic key management in the cloud is another security concern. Virtualisation software makes the deletion of such keys more complex, particularly if for example the virtual machine is being serialised for migration to different hardware.

Data privacy is another security concern for cloud providers. Due to the distributed nature of a cloud environment, protecting the privacy of data becomes a more complex issue. There is the potential for a lack of subscriber awareness over where data is stored and who has access to that data.

6.5 Conclusion

In this section, a more in-depth look has been taken at the underlying architecture of a cloud computing model. The different delivery models were explored in more detail, examining how each services is provisioned, and how the control in each of those service models is shared between cloud provider and customer. To understand the cloud environment, it is important to understand the management services that control business support services, such as billing systems, and operational support services, which support metering and provisioning operations. These concepts have been explained in chapter six.

Security in the cloud environment is a major issue for businesses looking to move critical systems to the cloud. So it was prudent in this chapter to explain how cloud services are secured. Databases are becoming more and more part of cloud service offerings, most major database vendors are now offering DbaaS as part of their cloud suite. Databases were not always a natural fit for the cloud, and the technological advances that have made database migration to the cloud have been covered here. Finally, this chapter attempted to identify some of the shortcomings that perforate the cloud realm.

7. PERSPECTIVES ON CLOUD COMPUTING

7.1 Introduction

Chapters 2, 3, 4, 5 and 6 have covered much of the research problem questions through literature review; it is critical though to understand how legal and technical experts participating on a daily basis in the cloud sphere view the pertinent issues particular to cloud computing. In order to achieve this, a series of questions were complied, and put to six professional experts with the aim of understanding the challenges facing legal and technical professionals in their endeavour of advising, planning and consulting on cloud projects. It was also a valid exercise to observe the level of knowledge, both legal and technical demonstrated by each expert group. By examining the answers given to the question set, it was possible to gauge the general understanding of the main cloud concerns expressed by Irish businesses.

In this section the target audience used for the interview process will be out-lined, along with the methodology for targeting such individuals. The questions posed also had to be constructed carefully. In the short time allocated for each interview, it was vital to obtain as much information as was possible to inform the literature review and experiment elements of the dissertation. This chapter concludes by highlighting the key findings from the interview process.

7.2 Audience

This dissertation attempts to demonstrate the *legal* implications of storing data in a cloud computing environment. Cloud computing is a relatively new computing paradigm, with inherent *technical* complications and peculiarities that distinguish it from other computing models. To inform the literature review section of this document, it was therefore deemed necessary that both legal and technical cloud experts needed to be consulted. The experiment section of this dissertation involves the production of an artefact, a cloud user guide, explaining the legal, educational and business knowledge individuals should be aware of before availing of cloud services. This artefact needs to be examined by industry experts to evaluate its practical use in a real business environment. And again, as the artefact has both legal and technical themes, it was thought appropriate that the audience helping to inform the literature review section could also be used to evaluate the resulting artefact.

The audience sought was one who had a wide array of technical and legal skills particularly in relation to cloud computing. Legal professionals who had experience consulting and advising clients on cloud legal issues were preferred, as were technical experts, knowledgeable in cloud architecture and having practical experience designing and maintaining cloud environments. The final interview panel comprised the following candidates;

Legal Candidates		**Technical Candidates**	
Candidate2	Legal Associate at Mason, Hayes and Curran law firm, Dublin	Candidate1	Senior Manager at Ernst & Young, Dublin
Candidate3	Legal Associate at Dillon Eustace law firm, Dublin	Candidate5	Technical Director at Technology Consulting Firm, Dublin
Candidate4	Senior Partner, William Fry corporate law firm, Dublin	Candidate6	Operations Director at IT Infrastructure and Services Company, Dublin

Table 7.1: Audience of Interviewees

Candidates 2, 3 and 4 were sourced via articles each had published on the Internet relating to legal issues with cloud computing. They were employees of Dublin based legal firms, so were therefore accessible, and on first contact, via email, were very obliging, and willing to offer time to assist in the dissertation process. The articles they had each published on-line demonstrated an understanding of the important legal issues relating to cloud. Candidate 1 was sourced via an article written by his colleague in the Irish Times in relation to the business implications of adopting cloud computing. When the author of the article was contacted, they were unavailable but they suggested Candidate 1 as an alternative replacement. Candidates 5 and 6 work for IT technical services companies based again in Dublin city centre and were sourced via associates working in those businesses.

7.3 Interview Design

The questions for the interview process needed to be designed in such a way as to elicit (in the short time provided) the most salient, relevant and current issues affecting cloud computing from the interviewees. Although a separate set of questions for the legal and technical candidates was not devised, some of the questions put to the technical experts were of a much more technical nature. But the interview process was not so rigid that technical questions could not be posed to the legal experts. The interviews were semi-structured in nature; the question set was used as a guide, but if the legal candidates for example demonstrated a good understanding of the technical issues with cloud, then questions of a technical nature were also put to the legal experts. This was the same case with legal questions posed to the technical candidates.

Table 7.2 lists the question set, depending on time constraints, it was not possible to pose all these questions to each candidate, but in the main the majority of questions were asked.

Question No.	**Question Text**
Question 1.	I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?
Question 2.	How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?
Question 3.	I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?
Question 4.	Do you think cloud vendors are violating the DPD principles?
Question 5.	Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?
Question 6.	Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?
Question 7.	What do you think of cloud contract terms (abdication of liability)?, are clients willing to accept these terms and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?
Question 8.	Do you believe the cloud has made IP violations a bigger problem?
Question 9.	Jurisdiction - Again are clients aware of these issues in regard to cloud computing?

Question 10.	If the Irish government in the morning said they were putting a particular department’s data in the cloud, what would you think? Would it depend on the department in question?
Question 11.	Does the judiciary have the skills or how much do they need to understand about cloud computing to apply the law correctly?
Question 12.	What are the main technical issues with cloud implementations? Have you seen any issues with things such as vendor lock-in? Getting data back out if a provider goes bust?
Question 13.	Have you heard of this Geolocation technology, do you think it could help allay client’s fears if they had definitive knowledge of the whereabouts of their data?
Question 14.	Should my focus be directed in another area/should I be doing anything different?

Table 7.2: Interview Question Set

The interviews commenced with general cloud computing questions, warm-up questions (questions 1 and 2) in order to gauge the candidate’s general understanding of the area. Question 3 was the first legal based question. Without giving away what legal issues the dissertation process had already revealed, question 3 attempted to first get an understanding of what the candidates saw as being the most important legal issues relating to cloud computing were. Continuing the legal theme, questions 4 and 5 brought up the issue of the Data Protection Directive, and sought to understand what relevance (if any) the DPD has to cloud providers and clients. Question 6 delved more into the specifics of data storage in a cloud computing environment, and attempted to ascertain whether the candidates thought all data types were suitable for a cloud computing environment. Questions 7, 8 and 9 concentrate on the three main legal issues the dissertation process has encountered with cloud computing, jurisdiction, intellectual property and contractual liability. The candidates were asked what they thought of these issues, and if they or their clients had come across such concerns with cloud computing. Question 10 was a hypothetical question, and designed to see if the answers given to preceding legal questions were backed up with this practical conundrum. Question 11 was very much tailored toward the legal experts. Legal cases dealing with cloud computing will generally involve the judiciary making decisions based on precedents set in other technical cases, so it was vital to understand how the courts would arm themselves with the technical nous necessary to adjudicate any future cloud computing cases. On the other hand question 12 had the technical experts in mind, as it attempted to discover what the technical difficulties existed with cloud implementations. Question 12 was also attempting to see if the technical experts had also come across issues where clients found it difficult to extricate themselves or their data from a cloud vendor, and if any standard operating procedures existed dealing with these situations. Questions 13 and 14 moved on to the experiment section of the dissertation. The general area and make-up of the experiment was known at this point, but it was necessary to get a preliminary 'pre-evaluation' of the dissertation artefact at an early stage in the process. This would help to fine-tune and mould the final experimental artefact.

7.4 Summary of Findings

It is difficult to summarise the distinct individual opinions from six very different candidates, each with different levels of experience and expertise. Although the technical experts all had experience in cloud computing, Candidate1's background was more centred in the security and risk analysis fields of ICT. Candidate1's answers obviously then leaned more towards the security implications relating to cloud computing than candidate5 and candidate6. Candidate3 (second legal interviewee) had less technical experience that the other legal candidates, so the responses there were purely legal based, with little influence from technical opinion. Different patterns and trends could nevertheless be observed from the interview process.

7.4.1 Legal Experts

The majority of the legal experts had a good understanding of what differentiated cloud computing from other computing models which had gone before it. Each expressed the opinion, that being cynical they could describe the cloud phenomenon as marketing hype. But followed this up citing the 'use anywhere', 'utility computing' phraseology that distinguishes cloud. The legal experts in the main agreed that Irish businesses were interested in investigating cloud technologies, indeed some businesses were obliged to do so, following on from the 'cost-reduction' promises of cloud. But they also highlighted a nervousness they believed businesses suffered from when confronted with cloud adoption. Many Irish businesses, particularly larger organisations (with more to lose), were adopting a wait and see approach to cloud adoption. They wanted to see other businesses take the plunge first, and if the experience was a pleasant one, would perhaps follow thereafter. Business start-ups were seen as the organisations with most to gain from cloud computing. The low upfront costs and rapid scalability promises with cloud appeared incredibly attractive to start-up businesses. The candidates did express the notion though that start-up organisations do tend to ignore the legal perils of cloud computing. Issues are discouraging businesses from adopting cloud computing, and some of these highlighted by the legal fraternity included onerous one-sided cloud contracts, data protection issues and the 'newness' of the technology.

With respect to the legal issues that the candidates saw as being the most important in the cloud computing realm, data protection came out as the leading concern. The candidates believed many organisations were aware of the implications associated with moving personal data into the cloud environment. Recent high-profile cases before the Irish data commissioner concerning personal data and privacy violations were highlighting the DP issues very clearly to Irish businesses. Candidate3 expressed the opinion that DP issues were conflicting with the technological advances offered by cloud computing; the cloud computing model offered rapid provisioning and scaling based on the ability of the cloud provider to move data around the globe, but DP laws were perhaps blocking cloud customer from availing of these cloud features. Other issues with cloud offered by the legal candidates included the risks of 'vendor lock-in', and the inability to recover data in such a situation. Security too, was highlighted as a concern, whether that be the security of data or the security of supply of the cloud service.

On the question regarding what data types could be stored in the cloud the legal experts differed quite significantly. One expert believed any type of data could be stored in the cloud. The opinion was expressed that security in a cloud environment should be far superior to that existing in private enterprises. Cloud providers should after-all be security experts, with the most expert knowledge on the security concerns and threats facing IT infrastructure. The other legal candidates were more cautious though, expressing the opinion that initially only non-sensitive data was suitable for public clouds, but that with more risk analysis assessment, all data types could eventually be moved into cloud environments.

With respect to the abdication of liability in cloud contracts, all the legal experts expressed similar views. The technology is new, the contracts will become less one-sided as cloud computing matures and more providers enter the market. Also the concept whereby you pay for what you get was suggested as the cloud mantra in many of these contracts, and the situations where organisations were only receiving quite moderate compensation when cloud services were down, didn't seem strange or heavy-handed to the legal candidates. There was an opinion that a middle ground was developing in this area though, and as the technology was maturing, larger organisations certainly were getting the ability to thrash out terms and conditions more with the cloud providers.

As for cloud increasing the likelihood of intellectual property rights, the candidates differed here again. One expert believed cloud certainly was making more data available in the public environment, so it followed that more copyrighted material would be copied and distributed on the internet as a result of cloud computing. This candidate expressed the opinion that the entertainment industry would definitely need to change the process whereby they release material in jurisdictions at different times, as it was now virtually impossible to prevent illegal file sharing and distribution. But another legal expert opined that IP violations were not necessarily affected by cloud computing, and that he had certainly not came across any literature suggesting the situation had gotten worse because of cloud computing.

Two candidates believed jurisdictional issues with data was a concern with cloud computing, but most particularly where the organisation hosting the cloud service had a presence in the jurisdiction concerned. The local 'establishment' of that company is subject to the local laws of the jurisdiction. Candidate2 believed article 4 of the DPD, which deals with which governing law has jurisdiction over a body when there is a legal issue was badly drafted. Candidate2 works directly in this area, and predicts more and more problems emanating from article 4. The other area in respect to jurisdiction that Candidate2 highlighted were the rules concerning data export. Under Irish law these are covered by section 2 of the Data Protection Act. But these laws are approximately ten years behind the technological advances in IT. Candidate2 believed Irish businesses were certainly aware of these laws, but were continually finding themselves having to avail of solicitor firms like his own in order to ensure they were compliant with these laws.

The hypothetical question regarding the Irish government putting a department's data into the cloud extracted similar responses to the question regarding whether any data types could not be put onto a public cloud. Interestingly though, while some candidates believed any data type could feasibly be stored in the cloud, they also believed more precautions should be taken with more sensitive data, more due diligence and risk analysis would need to be carried out. And perhaps the Irish government could start by putting data in the cloud which was of public interest first, planning applications, Supreme Court decisions etc.

Each legal candidate was unanimous that the judiciary didn't need specific skills to deal with cloud cases, the judiciary would call on technical experts or barristers who specialised in technology to assist in such cases.

Moving into the experiment section of the questionnaire no legal candidate had heard of geolocation technology. But all agreed it sounded like an excellent way of mitigating some of the issues in relation to the jurisdictional issues with cloud computing. One candidate called in 'technical comfort'. Clients could build jurisdictional clauses into their cloud contracts, but a piece of technology ensuring data stayed in the jurisdiction it was meant to would allay fears greatly. One candidate believed logging jurisdictional changes was fine, but ultimately didn't go far enough, and that what was needed was a piece of technology to prevent data being moved from pre-agreed locations. With respect to the User Guide which will accompany this dissertation, again each candidate believed this was an excellent idea. There was the belief that such information could help educate companies thinking of moving to the cloud on the important legal matters which needed to be considered.

Finally two of the candidates believed the key literature sources already identified on the legal issues relating to cloud computing were extremely apposite. Queen Mary, University of London, was an institution where the candidates had also found excellent material relating to cloud matters. But there were also suggestions to look at cloud user groups on LinkedIn and the Irish Data Commissioners website for other good cloud and data protection material.

7.4.2 Technical Experts

The technical experts obviously had a more accurate assessment of what distinguished cloud computing from technologies that had existed heretofore. One candidate mentioned the NIST definition, the others talked of elasticity, access anywhere, flexible, scalability, cost reduction, pay-as-you-go usage models.

The technical experts differed a little in relation to the how Irish businesses view cloud computing. Candidate1 believed Irish businesses were very much interested in the technology, indeed from a capital expenditure point of view some were obliged to factor in cloud computing solutions, but he did say the level of excitement and interest was affected by the size and sector of the business involved. Small start-ups loved the idea of cloud, large corporations less so. There also existed a level of caution from Irish businesses though, particularly large corporations, who had HR and legal departments who were au fait with the legal issues relating to cloud computing. The other technical experts believed too that Irish businesses were interested in cloud. They were of the opinion that start-up businesses were particularly interested in the technology, but start-ups as a consequence were also the types of organisations who didn't fully investigate the legal issues with cloud, and as a result were falling foul to some of the common cloud shortcomings.

Interesting though, Candidate5 and Candidate6 both spoke about businesses lacking the maturity/know how/expertise/professionalism to understand or contemplate what additional benefits can be accomplished through cloud computing. Many organisations don't have a close alignment with IT, and don't understand how IT can be utilised to drive the business forward. Both candidates believed this ignorance, and lack of maturity was preventing many SMEs in particular from moving into the cloud. Candidate5 also noted that IT departments in businesses around the country are also proving to be an obstacle to organisations adopting cloud services. IT departments are scared of cloud computing, they see it as a way for their organisations to out-source IT. Candidate5 made the point that in many cases in order to sell a cloud service, it was necessary to go above the heads of IT, but in businesses that lacked the technical maturity to understand cloud, going above IT's head sometimes made little difference. Candidate5 went so far as to say that he believed the concept of the public cloud was dead for a couple of years at least. Businesses were more likely to look at private and hybrid clouds first, and if those scenarios proved cost affective and secure, perhaps public clouds would be re-visiting in the future.

The concept of ‘Shadow IT’ was also raised at this point, some business departments, without the clearance or knowledge of senior management or IT were purchasing cloud services. More and more of these departments were doing so because they were either ignorant to the implications of adopting cloud services, or they were impatient, and were not prepared for their IT departments to procrastinate any further.

Data protection was the main legal concern with cloud computing raised by the technical experts. In many cases the technical experts are the people informing business of their obligations in relation to data protection. Some businesses it seems, and in contrast to the opinion from the legal experts, still don’t fully understand their obligations under the Irish or European data protection acts. Businesses are content if their data is encrypted and whilst in the cloud environment, remains within the EEA. Other legal concerns mentioned by the candidates were E-Discovery, vendor lock-in, Shadow IT exposing the business to data protection law, the inadequacies of safe-harbour if your data is stored in America and abdication of liability in cloud contracts.

The technical experts did not believe that cloud vendors were deliberately violating DPD principles, but Candidate5 was able to give an example where Microsoft’s Azure cloud offering had violated the DPD in one circumstance by being unable to switch off replication of a user’s data to a foreign location. Other candidates believed violations with respect to the DPD would depend on the size of the vendor, and that most reputable vendors would certainly not deliberately violate any law. Whether clients had knowledge of the DPD principles was really down to what individuals the experts talked to in the organisation. The experience was that IT departments knew little of these laws, but senior management (certainly in the larger SMEs and corporations) were aware of the organisations responsibilities with respect to data protection.

No technical candidate believed there was any technical impediment to storing all data types in the cloud. Candidate1, the security expert certainly believed a higher level of due diligence was required when considering moving sensitive personal data to the cloud. The reputation of the vendor was again brought to the fore here, once the vendor used was a reputable one, data types should make no difference.

On the question of abdication of liability within cloud contracts the technical experts were in agreement that you get what you pay for, and that it was unrealistic for cloud providers to cover the costs of business losses if those organisations affected by a cloud outage were only paying a small sum for the cloud service in the first place. Compensation they believed was commensurate to the service costs. Candidate5 believed there were ways to avoid abdication of responsibility from a cloud provider, but this usually meant going to a provider who wasn't Amazon! Instead providers such as Nirvanix.com and colt.net would allow contracts be amended so more responsibility was borne by the provider. These types of provisions in a contract can be quite expensive though.

With regard to the jurisdictional issues with cloud Candidate5 in particular thought these concerns were being addressed, as more and more vendors were offering bespoke offerings which allowed cloud clients pick and choose which locations they wanted their data to remain in. Both Candidate5 and Candidate6 also expressed the opinion that a lot of mixed messages were emanating from the legal profession and the data commissioner in relation to these matters. The fact that the DPD was transposed differently by each European Union member was also a concern, and it made it very difficult to understand what needed to be considered in relation to data protection even within the European Union.

What the candidates thought of the hypothetical question of the Irish government moving a department's data in to the cloud provoked interesting responses; Candidate1 didn't see this as a huge issue, once he was able to view the risk analysis methodology the government used in order to choose the cloud provider involved. Candidate5 thought the only important consideration with this hypothetical question was the cloud provider. Candidate5 has had experience of some vendors, whose services from a security and protection perspective are not up to scratch. If the vendor on the other hand was a reliable one, with a proven track record in security, reliability and data protection measures, then moving government data to that vendor's public cloud would not be an issue.

Two of the technical experts were asked about the technical difficulties encountered with cloud implementations. One expert spoke of the lack of maturity on the client side, as was mentioned earlier, some businesses are just not technically mature, or have enough business agility/proper business processes in place to be able to move to cloud. The other candidate talked about the maturity of the cloud provider, she questioned whether cloud vendors had in place policies and procedure for clients wishing to migrate to another cloud provider or a client going bust, what is done with that client's data? Candidate6 also spoke about the lack of understanding on behalf of the potential cloud customers regarding what is required from a communications perspective for non-web based applications hosted by the cloud provider, and the resultant costs involved. Clients sometimes don't understand either about the risks associated with further migrations between cloud providers. And on this subject, both these technical experts thought vendor lock-in was a huge concern, neither of them had come across a standard operating procedure for cloud providers returning data back to clients in the event of a migration or termination of contract.

Moving on to the experiment element of this dissertation, two of the candidates were quite knowledgeable in relation to geolocation technology. Candidate5 was able to give me details on work Intel (Intel TXT - Trusted Execution Technology), VMware and the RSA were doing in this area in order to build compliance proof clouds. This technology involves geolocation information being retrieved from the Intel chip, and based on a pre-configured county list, virtual machines will boot if the geolocation information is on that list. Apparently this technology is approximately twelve months away, but is coming. One technical expert was not too familiar with geolocation, suggested an area worth considering for protecting data was DLP, Data loss prevention. There are many varieties of DLP that are designed to detect potential data breach incidents.

In regard to the User Guide that will accompany this dissertation, Candidate5 had the most interesting response. He believed this guide could be useful; however he suspected that there was a vested interest from some organisations that this information regarding cloud adoption was kept deliberately vague! Perhaps there are more billable hours achievable by consultants when all the information is not widely available and known. Candidate5 also believed it might be difficult to construct a generic guide on cloud computing. He spoke of cloud services being offered as generic services, but when it came to implementing any significant sized cloud projects, which were not pre-packaged services, the term generic is soon forgotten, and the client wants a bespoke service, quite particular to their needs.

7.5 Conclusion

This section of the dissertation has attempted to convey the necessity for the interview process conducted as part of this work. Having expert opinion from properly sourced and informed individuals was a vital component of this work. The questions that were put to these individuals also had to be constructed carefully. The dissertation was attempting to discovery what experts in the field thought the most challenging legal aspects of cloud computing were, and if the issue of data protection in the cloud was considered a significant concern. The questions needed to get answers to these questions. The interviews, and the questions posed though also needed to be conducted in such a way as to gauge the candidate's knowledge of the cloud area. There was also scope to tailor the questions, and their running order, in an attempt to allow the interviews flow more naturally, and hopefully gain the most pertinent information.

Overall, the spread of knowledge and expertise across the target group proved invaluable to the dissertation process. The majority of the interviewees were in senior management positions, and had a vast arrange of experience in consulting on large cloud infrastructure projects. The candidates involved had dealt with different business sectors looking to avail of cloud services and had witnessed first-hand the common day-to-day problems organisations encountered as they examined cloud adoption. This wealth of experience assisted greatly in the literature review sections of this work. Academic papers, books and web articles are excellent resources for research based work, but also having the ability to back up these resources with experts in the field is an invaluable addition to the dissertation process.

8. A COORDINATED SOLUTION TO THE JURISDICTIONAL ISSUES IN CLOUD COMPUTING

8.1 Introduction

This paper has attempted to identify just some of the issues that affect the adoption by businesses of cloud computing technologies. The issues have primarily been legal ones; intellectual property concerns, the abdication of liability in cloud contracts and more. The literature review undertaken in Chapters 2, 3, 4 and 6, and the serious of interviews with technical and legal experts outlined in Chapter 7 have informed the dissertation. The literature review and interview process have identified concerns regarding data protection compliance as being the most important legal concern businesses face with the adoption of cloud computing, and particularly the jurisdictional issues which arise when personal data is moved between different countries. What has become clear though, through the course of the dissertation process, is that no single solution exists to mitigate or solve problems of data protection compliance in the cloud computing sphere. It has become clear that solutions to solving jurisdiction issues in cloud computing must come from several sources. To that end, this chapter details three areas where solutions can be derived from. These areas are; Technology, Education and Business Processes. Chapter 8 will look at each of these areas in turn and identify how solutions that are needed to solve the jurisdictional issues of data protection can be achieved.

The identification of these three headings as areas where solutions can emanate from will lead to the production of an artefact, detailed in Section 8.4. This artefact will be a summation of the three pronged approach to solving the legal challenge out lined in Sections 8.2.1, 8.2.2 and 8.2.3. The artefact will be physical in nature, a short guide for business to assist them in acquiring the information they need before moving personal data into a cloud environment. It will help educate business to the legal issues they should be concerning themselves with prior to cloud adoption, and the guide will identify technical means, businesses can avail themselves of that can help alleviate some of the legal uncertainties regarding cloud jurisdictional issues. Section 8.3 describes one other feature that makes up an important component of the user guide, the ‘Cloud Adoption Wheel’. The artefact will be evaluated by the interviewees outlined in Chapter 7, and their feedback, evaluation and criticism will be presented in Section 8.5.

8.2 Three faceted co-ordinated solution

8.2.1 Education

Section 2.5 of this dissertation, 'Business and Marketing in Cloud Computing', outlined the many advantages of cloud computing espoused by marketing companies. Indeed many of these advantages are noteworthy, and certainly make cloud computing an attractive prospect for some businesses. In Section 6.4 though, the shortcomings in cloud computing were touched on. Many of these shortcomings highlight the legal issues that mire cloud adoption. Interviews with legal and technical experts in Chapter 7 of this work have also highlighted the dearth of legal knowledge that exists within businesses wishing to adopt cloud.

It is an argument of this dissertation that with proper education of the relevant legal issues, businesses, both cloud providers and subscribers, will in many cases be able to navigate the legal issues with the adoption of cloud computing. This paper has chosen to focus on one important legal uncertainty in relation to cloud computing, the legal standing of personal data in a cloud computing environment. By understanding the important legal implications of moving/storing and exporting personal data, users can make a much more informed decision prior to making a move into the cloud. To that end, this section of the dissertation provides three educational recommendations. These recommendations are intended as a stepping-stone for individuals to pursue further investigations into these areas, and the jurisdictional guide accompanying this paper will provide users with websites where they can access further information relating to these topics. The first educational recommendation gives the definition of personal data as per European Directive 95/46/EC. If this definition is known and understood, along with the eight obligations concerning data storage that accompany the directive, businesses will have a better understanding of their legal obligations. Education recommendation number one is;

1 – Understand Personal Data obligations – Under European Directive 95/46/EC, Personal data is defined as any information relating to an identified or identifiable natural person. Under the directive, organisations have key responsibilities in relation to personal data they store; these obligations can be summed up in the following eight rules;

1. **Obtain and process the information fairly**
2. **Keep it only for one or more specified and lawful purposes**
3. **Process it only in ways compatible with the purposes for which it was given to you**
4. **Keep it safe and secure**
5. **Keep it accurate and up-to-date**
6. **Ensure that it is adequate, relevant and not excessive**
7. **Retain it no longer than is necessary for the specified purpose or purposes**
8. **Give a copy of his/her personal data to any individual, on request.**

The second recommendation relates to where responsibility lies for the protection of personal data once it is put into a cloud computing environment. Again the literature review and expert legal opinion informed this recommendation. Sometimes organisations believe their responsibility for personal data is absolved when the data is moved into the cloud environment, but this is not true. As the data controller, the institution who moves the data into the cloud must still assume full responsibility for the protection of this data. This fact further highlights the need for businesses to educate themselves about the legal implications of moving data into a cloud environment. Educational recommendation two is;

2 – Responsibility –Institutions that move data to the cloud environment, are deemed data controllers, and as such are required to ensure that all processing of personal data within the cloud environment is fair and lawful.

Therefore, while negotiating with the cloud provider, ensure all legal obligations in respect to personal data in the cloud are provided for, and are documented in the contract and ensuing service level agreements.

The final recommendation is concerned with transferring personal data. Under Directive 95/46/EC personal data cannot be transferred outside the EEA, unless the data is being exported to countries that the European commission feels provide an adequate level of protection. The third educational recommendation;

3 – Transferring of Personal Data – Personal data can only be transferred outside the EEA to countries where an adequate level of protection is seen to be applied. These countries are Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man and Jersey. Compliance may be achieved through using EU approved contract terms with a provider. Alternatively, using a provider in the US who has signed up to the Safe Harbour provisions will be necessary.

If attempted to transfer personal data outside this approved list, it is advisable to consult the attached country legal matrix. By looking at the matrix it can be determined where countries fall down or excel in three respective policy areas affecting cloud; Data Privacy, Intellectual Property and Security & Cybercrime.

It is envisaged that these three recommendations will act as a starting point for individuals wishing to adopt cloud services. Website links provided in the jurisdictional guide will point towards further assistance on each recommendation.

8.2.2 Technology

Geolocation

The paper has identified geolocation technology as a key area that can mitigate against the issues relating to jurisdictional concerns with personal data in the cloud. Geolocation for the purposes of this paper can be defined as the detection of the physical location of a physical computing device.

Different technologies are combined that enable geolocation services to accurately determine a computer device's location, these include IP addresses, GPS and WIFI. IP addresses assigned to a device by an ISP can be referenced against on-line databases that hold corresponding location co-ordinates for that IP. GPS technology is now built into computer chips, and use satellites in space to help triangulate the exact position of a device. By determining which WiFi networks are available at different locations, and combining this information with GPS data, applications can also determine the exact location of a computer device.

In the past geolocation technology has been used mainly by content delivery networks and targeting advertising companies. In these cases it was necessary to determine a customer's location in order to route application requests to the nearest data center for optimal user performance or to more effectively deliver relevant location based advertising. Now however, this technology can be used to satisfy compliance and security issues related to cloud computing.

This leads to the first technical recommendation for the 'Jurisdictional Guide to cloud computing';

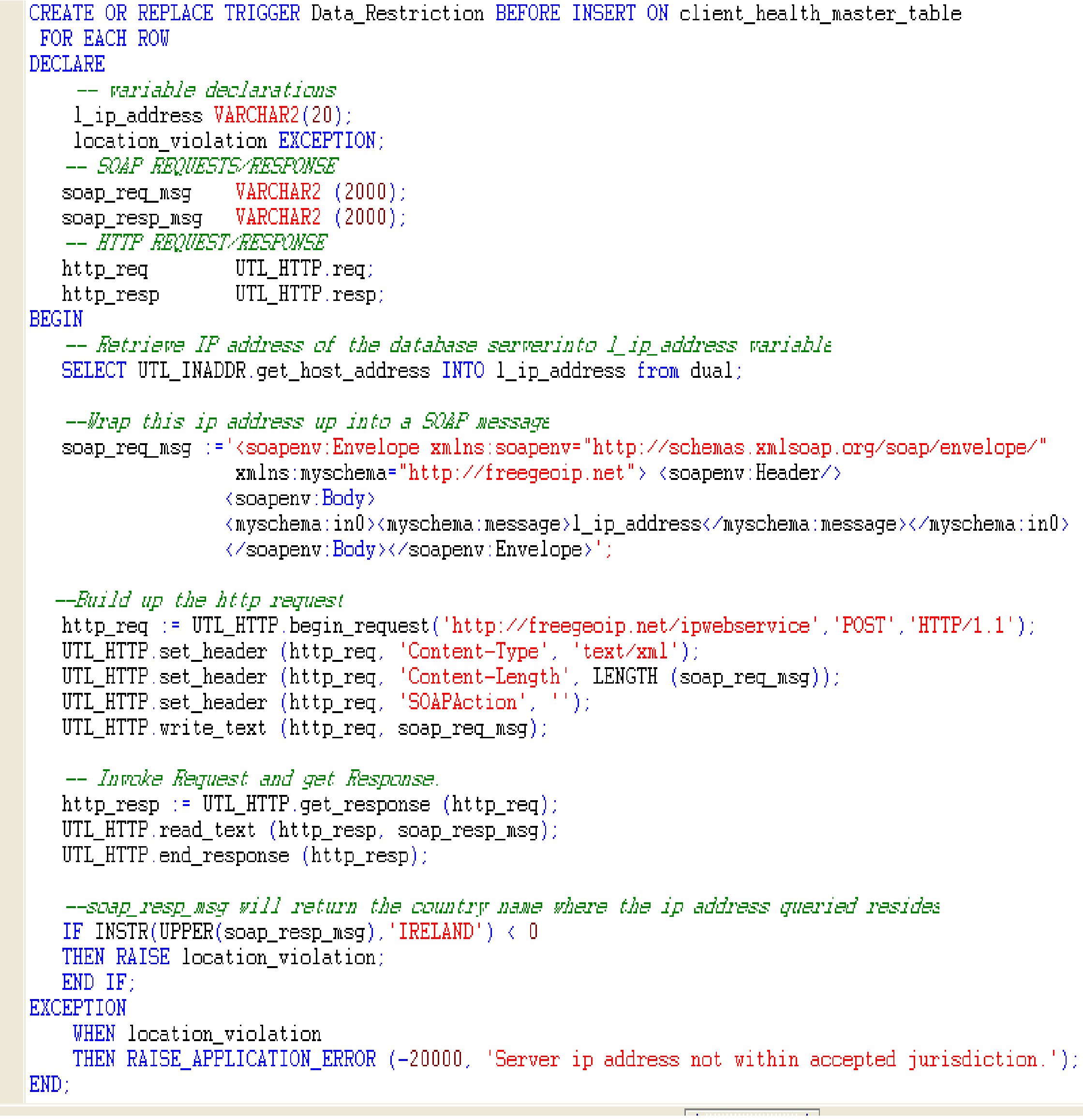
1 – Where data to be housed in a cloud environment is of a personal nature, ensure the cloud provider utilises geolocation technology to lock-down your data to jurisdictions you have pre-chosen in consultation with that provider.

Cloud providers are using geolocation technology. As mentioned previously in Chapter 6, technology companies Intel, the RSA and VMware have developed technology which ensures instances of virtual machines only boot if they can determine that their physical location is a 'trusted' one. Microsoft's PaaS offering, Microsoft Azure offers clients the ability to determine locations where their data is to be stored. 'Microsoft Azure Geolocation' gives clients assurance that their sensitive data is only stored in jurisdictions where they feel adequate data protections laws apply. Other cloud providers identified in the expert interview process who provide geolocation options in their cloud offerings include Colt, www.colt.net and Nirvanix, www.nirvanix.com. Links to websites detailing important information regarding geolocation technologies and to cloud companies advertising geolocation options in their cloud offerings will be detailed in the jurisdictional user guide.

Geolocation in Databases

Databases – as seen in Section 6.3, technological barriers preventing full migration of relational database systems to the cloud have been overcome in the last decade. Now, more and more cloud providers offer data storage via database technology in their cloud environment. Fortunately modern database systems enable geolocation information to be retrieved from the computer system they run on. For situations where cloud providers do not offer geolocation services upfront, additional functionality bundled with some database systems can be utilised in order to discover geolocation information for the particular database. Oracle for example, provides development packages such as UTL_INADDR and UTL_HTTP that can be used to make applications more location aware. UTL_INADDR for example can be used to obtain the ip address of the database server. Once the ip address of the database server is known, this information can be queried utilising ULT_HTTP against any one of many on-line web databases which store lists of ip addresses and their corresponding GPS coordinates. Some on-line ip address databases provide a web service or API (application programming interface) to allow developers build functionality into their applications to directly query these on-line databases. This is usually achieved by the hosting site providing the WSDL (web service definition language) XML details it will accept in order to return the GPS coordinates of a given ip address.

The application requiring the geolocation information for a particular ip address then builds an XML message (usually called a SOAP (Simple Object Access Protocol) message), then submits this XML message via a http request to the hosting service (the on-line ip address database) and the resulting location information is returned to the calling application. This can all be achieved within the Oracle database. The fully commented code below from a 'Before Insert' table trigger gives an example of how an Oracle table trigger can use the technology described to prevent data being inserted into a database residing on a server which is not located in a particular destination.



```
CREATE OR REPLACE TRIGGER Data_Restriction BEFORE INSERT ON client_health_master_table
 FOR EACH ROW
DECLARE
    -- variable declarations
    l_ip_address VARCHAR2(20);
    location_violation EXCEPTION;
   -- SOAP REQUESTS/RESPONSE
   soap_req_msg    VARCHAR2 (2000);
   soap_resp_msg   VARCHAR2 (2000);
   -- HTTP REQUEST/RESPONSE
   http_req        UTL_HTTP.req;
   http_resp       UTL_HTTP.resp;
BEGIN
   -- Retrieve IP address of the database serverinto l_ip_address variable
   SELECT UTL_INADDR.get_host_address INTO l_ip_address from dual;

   --Wrap this ip address up into a SOAP message
   soap_req_msg :='<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                   xmlns:myschema="http://freegeoip.net"> <soapenv:Header/>
                  <soapenv:Body>
                  <myschema:in0><myschema:message>l_ip_address</myschema:message></myschema:in0>
                  </soapenv:Body></soapenv:Envelope>';

  --Build up the http request
   http_req := UTL_HTTP.begin_request('http://freegeoip.net/ipwebservice','POST','HTTP/1.1');
   UTL_HTTP.set_header (http_req, 'Content-Type', 'text/xml');
   UTL_HTTP.set_header (http_req, 'Content-Length', LENGTH (soap_req_msg));
   UTL_HTTP.set_header (http_req, 'SOAPAction', '');
   UTL_HTTP.write_text (http_req, soap_req_msg);

   -- Invoke Request and get Response.
   http_resp := UTL_HTTP.get_response (http_req);
   UTL_HTTP.read_text (http_resp, soap_resp_msg);
   UTL_HTTP.end_response (http_resp);

   --soap_resp_msg will return the country name where the ip address queried resides
   IF INSTR(UPPER(soap_resp_msg),'IRELAND') < 0
   THEN RAISE location_violation;
   END IF;
EXCEPTION
    WHEN location_violation
    THEN RAISE_APPLICATION_ERROR (-20000, 'Server ip address not within accepted jurisdiction.');
END;
```

Figure 8.1: Oracle Trigger Code blocking data movement

These technical means of blocking data insertions into databases not residing in particular jurisdictions leads to the second technical recommendation for the jurisdictional guide;

2 – Where geolocation services are not offered as part of the initial cloud offering, and a database service is being availed of, in the SLA negotiations ensure the cloud vendor uses geolocation functionality inherent to those databases to lock down database transactions to pre-agreed jurisdictions.

These mechanisms for returning geolocation information from the database server and preventing data insertions can also be used to write log files detailing the geolocation information as it has been recorded. These log files can then be inspected by cloud clients for compliance purposes. This leads to the third technical recommendation;

3 – Where data is stored in databases in the cloud, ensure geolocation information from the database server is recorded as data is moved between databases/database tables, and ensure the cloud provider make this data freely available.

It is hoped these three technical recommendations will assist cloud subscribers and providers build cloud solutions that ensure adherence to compliance issues relating to personal data in the cloud computing environment.

8.2.3 Business Processes

Cloud computing technology is not suitable for all businesses. Also, some businesses are not mature enough to successfully move their applications and data into a third party cloud environment. Some organisations simply do not have the technological know-how or business experience to understand the implications of cloud computing, what benefits it can bring, and the pitfalls inherent in the technology that need to be avoided. These businesses usually lack four important ingredients necessary for cloud adoption;

1 - There is no experience within the business of dealing with third party IT vendors.
2 - A strong partnership between business units and IT does not exist.
3 - There is no evidence of agility within the business in terms of being able to react quickly to new advances in technologies and innovations.
4 - Data governance and compliance processes within the organisations are usually ad-hoc or non-existent.

This section of the dissertation will make three recommendations that organisations should consider, in order to begin to gain the maturity required to evaluate cloud technology as a viable alternative to traditional IT business models. Again, in the jurisdictional guide accompanying this paper, these recommendations will be backed up with website links to material providing further guidance and information. The first Business Process recommendation focuses on the necessity of an organisation to have an up-to-date and functioning Data Governance (DG) policy. Data Governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. DG concerns itself with asset management, data being the asset in question. Where organisations have an efficient DG framework in place, data will tend to be managed, understood and secured more effectively. And where data is managed properly by an organisation in-house, the more likely it is that that organisation will have the wherewithal to demand commensurate protection for that data if it is moved to a cloud environment. This leads to the first Business Process recommendation;

1 – Data is an asset, If not already in place, begin the process of developing a Data Governance framework for your business that matches the business goals of your organisation.

It is clear that many businesses view IT as just another cost centre, albeit a necessary one. But many organisations don't use IT effectively to achieve business objectives. The full benefits with which IT could bestow upon the business are neglected. There is little Business/IT alignment. Understanding the benefits a properly funded and managed IT department can bring to an organisation is a vital pre-requisite to comprehending the complexities inherent in an outsourced cloud service. In an effort to bridge this disconnect between Business and IT, some institutions have built IT Capability Maturity frameworks. These frameworks provide a mechanism for organisations to derive the full value from IT to deliver business value. This leads to the second Business Process recommendation;

2 – Understanding IT – Begin the process of adopting and implementing an accredited IT Capability Maturity Framework. Such models provide a concise management roadmap to optimise business value derived from IT investments. These models can help the organisation deliver business value from IT in the following ways;

Provide insight into crucial relationships between business and IT

Provide an understanding of IT spending

Show how to leverage existing assets and funds to further business goals

The final Business Recommendation is related to a recent concept in business known as ‘Shadow IT’. Shadow IT is a term often used to describe IT systems and solutions built and used inside organisations without organisational approval. Two of the three expert technical interviewees mentioned Shadow IT as being a serious problem in small to medium sized businesses. A scenario was painted whereby certain business departments decided independently to avail of a cloud service without the knowledge of IT or HR staff within the organisation. This happens for many reasons; the business unit in question may have no working relationship with the IT department, the business unit believes it can avail of the service it needs more cheaply by going outside the company structures, the business unit may be ignorant that the in-house IT department has the knowledge to provide the service itself, IT may be perceived as being too slow, and the business unit does not have the time to wait for in-house IT to provide the necessary solution. Whatever the reason, bypassing the legal and technical structures within an organisation, opening up the entire business to security and legal threats is a serious matter.

SMEs tended to be more susceptible to Shadow IT than larger organisations. SMEs in some cases tended to have more lax security measures in place, meaning networks could be opened up by business units to cloud providers.

3 – It is imperative that policies and procedures are in place ensuring correct guidelines are followed when business require the delivery of any IT service. Avoid business units going outside the organisation for IT services by ensuring:

IT networks and system are adequately locked down, preventing unauthorised access both from within and outside the organisation.

Work towards building open communication channels between IT and the business, to demonstrate the services IT can provide.

When a service cannot be facilitated by in-house IT, ensure business and IT work together to ensure the proper solution is provided, in a secure and cost-effective manner.

These three business recommendations are intended to provide guidance to organisations whether they are seeking to avail of cloud services or not. The principles set out here can benefit any organisation, even those never intending of availing of any outsourced IT service. Implementing a Data Governance policy, establishing an IT capability maturity model and ensuring 'Shadow IT' practices are prevented are all prudent measures organisations can take to improve general efficiencies within the organisation.

8.3 Cloud Adoption Wheel

This dissertation has discovered many legal issues clients face when moving applications and data into a cloud computing environment. The legal issues concerned often depend on the types of data being stored and the types of applications being used within the cloud environment. For example laws relating to data protection are not generally a concern when data being stored in the cloud is of a public nature. The suitability of cloud to certain organisations can also depend on the type of organisation in question, and the business sector that organisation is involved in. For example, for start-up business, in the web hosting or web development sector cloud is attractive. For large corporations or government departments running mission critical applications or storing sensitive data, cloud is not necessarily unsuitable, but the risks involved are greater, and the due diligence and risk analysis assessment required upfront are increased.

The cloud adoption wheel in Figure 8.1 attempts to give a visual representation of the types of business and business sectors who might use cloud, the type of data and applications that might be run in a cloud environment. The graphic then attempts to plot the level of risk and the related laws which may affect those businesses within the course of migrating to the cloud environment.

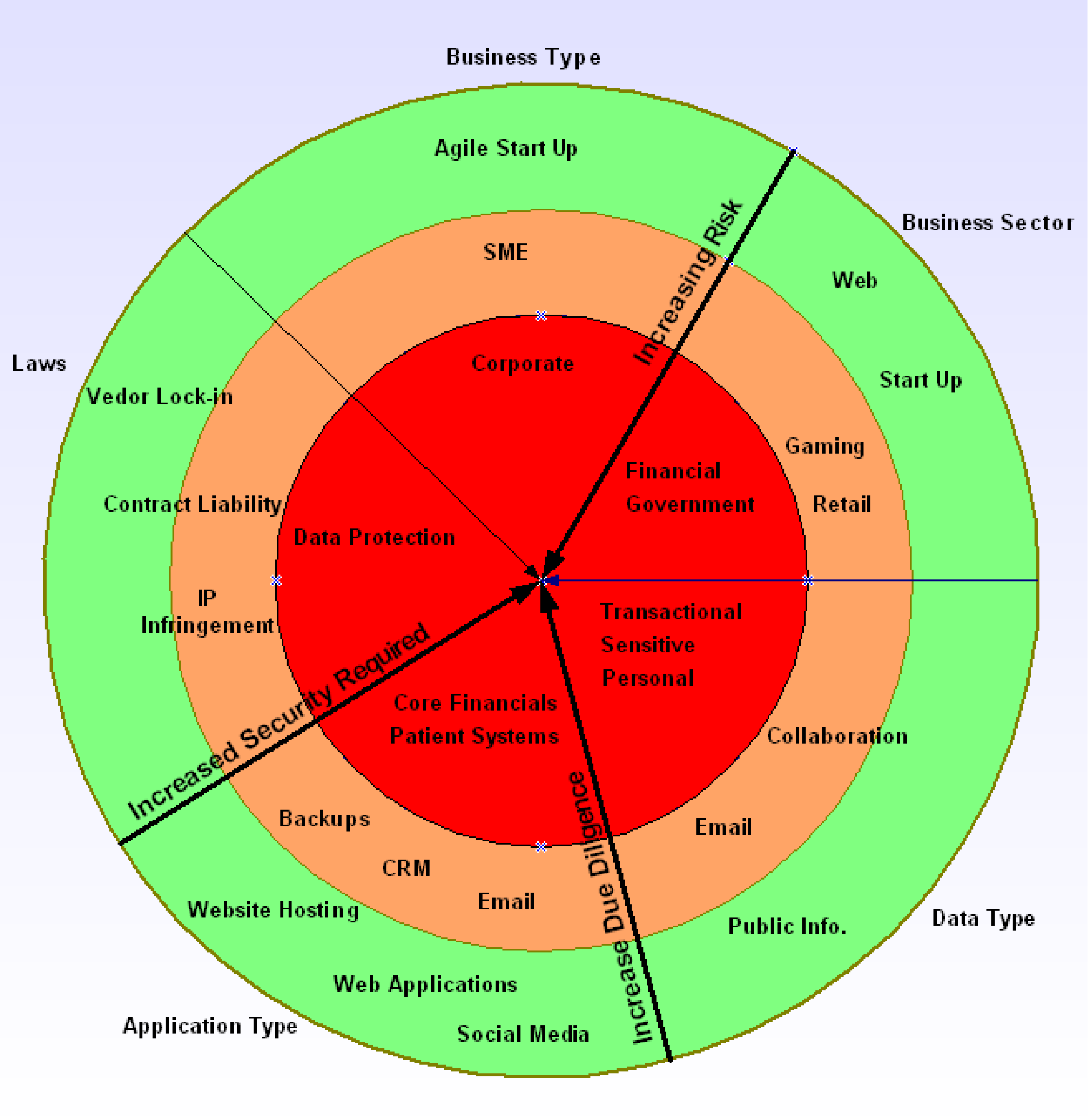


Figure 8.2: Cloud Adoption Wheel

The graphic is intended just as a quick visual guide for users thinking of migrating to the cloud. It demonstrates the heightened risks and different laws which may be applicable as different business types move data and applications into the cloud environment. The content depicted in the wheel is not intended to be definitive; other issues exist with cloud adoption. Moreover, there can be great risk posed to start-up businesses who do not fully investigate the cloud service they avail of. The wheel is purely intended as a general guide, a visual aid to demonstrate the laws that may apply to different types of businesses as they avail of cloud services and the increased level of risk assessment organisations should endeavour to complete prior to the adoption of a cloud service.

8.4 Artefact

The physical artefact accompanying this document is entitled, ‘User Guide – Jurisdictional Issues in Cloud Computing’. It comprises 13 pages, delivered in booklet form. Contents include an Introduction, explaining the three-pronged approach to tackling jurisdictional issues with cloud computing, there are then three sections, each offering recommendations under the Educational/Technology and Business banners for businesses to review. Each of these three sections is accompanied by a ‘Further Guidance’ page, listing websites where more information can be found on the selected topics. Under the technology section, there also includes information on geolocation technologies in database systems, and an example is given of how an Oracle before-insert table trigger can be coded to prevent data being moved to an undesired location.

FINAL YEAR PROJECT MANUAL

User Guide: Jurisdictional Issues in Cloud Computing

Student:

Alan Harris

D04106023

Supervisor:

Ronan Bradley

Ronan.Bradley@dit.ie

May 31, 2012

Table of Contents

Figure 8.3: User Guide Artefact

The final section of the artefact displays and explains the Cloud Adoption Wheel explained in Section 8.3.

8.4.1 Artefact Evaluation Process

In order to have the artefact evaluated it was sent to all interview candidates in both electronic form, via email, and in physical form, by express post. The evaluation questions detailed in Table 8.1 were constructed and emailed to each candidate. The candidate responses would provide the experiment evaluation component of this work. Candidate Evaluation can be viewed in the next section, 8.5.

Evaluation Questions

The artefact generated and emailed to each candidate was a result of the research carried out by this dissertation. The research identified jurisdictional issues as being the most likely cause of concern for businesses putting personal data into the cloud. And the guide highlights these concerns and attempts to give practical advice under Education, Technical and Business banners for mitigating these jurisdictional concerns. The questions posed attempt to have the artefact evaluated under three headings, 'General', 'Structure' and 'Specifics'. 'General' attempts to evaluate the over-all practicality and usability of the guide. 'Structure' attempts to evaluate the format of the guide and 'Specifics' endeavours to understand if the more precise detail on items such as the section on geolocation in database technologies and the Cloud Adoption Wheel warranted inclusion. The questions are listed in Table 8.1.

Question No.	Question Text
General Question 1.	Do you believe businesses thinking of availing of cloud services would find this guide useful?
General Question 2.	This guide could be the first of a series of practical booklets outlining the legal concerns around cloud computing. Other guides might be developed to advise on Contract liability or Intellectual Property issues. Do you think this guide, and subsequent guides of this nature would prove useful to businesses?
Structure Question 1.	The guide is broken into three sections, giving practical advice on how to mitigate against the jurisdictional concerns with cloud computing. Do you think structuring the guide in this manner is useful, or does it provide too much information in one booklet?
Structure Question 2.	The booklet is only meant as a very general guide to the jurisdictional issues in cloud computing, is it too concise and summarised to provide any meaningful guidance?

Specifics Question 1.	Do you think the 'Further Guidance' sections of the booklet, with links to web sites providing more information on the section topics are useful?
Specifics Question 2.	What do you think of the country legal matrix on page 4, if this was expanded, so many more countries were available, do you think it would prove useful to businesses trying to decide what jurisdictions were suitable for public clouds?
Specifics Question 3.	Page 7 gives very specific details of how geolocation information can be used within an Oracle database to stop data moving between different jurisdictions. This is there just to show that geolocation technologies do exist, even within databases, and the trigger code is included to give IT staff an idea of how such technologies can be applied. Is this information useful, or is it too technical?
Specifics Question 4.	Page 11 displays the Cloud Adoption Wheel. As a visual aid to cloud computing concerns, did you find it informative? Confusing? Did it provide any practical, usable information?
General Question 3.	Where do you think the guide falls down, what would you have liked to have seen that is not included?
General Question 4.	Are there any other general remarks you would like to make about the booklet?

Table 8.1: Evaluation Question Set

8.5 Evaluation

The majority of the technical and legal experts interviewed as part of the research question analysis were happy to take part in the evaluation process. As described in Section 8.4.1, in order to have the artefact evaluated it was sent to all interview candidates in both electronic format, via email, and in physical format, by express post. Each candidate was asked to answer ten questions relating to the user guide. Response to each question varied across the group, but in general reaction to the user guide was very positive. Table 8.3 summarises the responses from the expert group.

Question No.	Answer Text
General Question 1.	Candidates thought businesses thinking of availing of cloud services would find this guide useful. They noted that the guide quickly established the main areas of consideration that businesses should look at before making any decisions about moving their data out of the company domain. They also suggested the guide provided some

	excellent links for businesses to drill down into areas that they needed to investigate fully before adopting the cloud services.
General Question 2.	The candidates believed this guide could certainly be the first in a serious of legal guides on cloud. The area of cloud contracts and liabilities was mentioned as an area of particular interest and concern to businesses due to the uncertainty of ownership and liability if data is corrupted/lost or unavailable when residing in the cloud. Many of the candidate's customers don't know where to start when looking at the suitability of cloud services for their IT functions. These 'lite' guides could simplify and ease customers into the whole area of cloud and what pitfalls to look out for.
Structure Question 1.	On the structure of the guide and the volume of information in the booklet, candidates found the level of information on the three topics ideal for businesses and individuals who already had a basic understanding of cloud. However for businesses with little or no knowledge of cloud, future guides might include more basic definitions and guidance. Some of the detail in the guide was considered too complicated for novices.
Structure Question 2.	The guide was not considered too concise; candidates understood that the booklet was only intended to give general guidance. They believed the links provided more than made up for the summarised nature of the content. The links they believed were an excellent way of directing businesses to further information on the topics.
Specifics Question 1.	On the further guidance pages, as suggested earlier, the experts found the links extremely useful. The links allowed candidates delve into specific areas that were of particular interest to them without having to wade through all the information in one large document.
Specifics Question 2.	On the question regarding the legal matrix, candidates believed it was extremely useful. It was described as an extremely practical visual aid that allowed the candidates to see at a glance which jurisdictions they would definitely not recommend to their customers for specific types of applications and data types. The technical candidates commented that many of their customers have bases in US/Ireland/UK and many have their Asia/Pac base in Australia, so for future drafts they would be interested to see Australia included in the matrix.
Specifics Question 3.	The technical candidates received specific details on geolocation more favourably than the legal experts. The technical experts commented that as representatives of IT services companies, and having many customers running relational databases, this level of information was highly valuable to their customer set. The legal candidates appreciated the pointers towards technical solutions for legal issues, and felt these kinds of suggestions would greatly assist them when they were advising clients. The trigger code was irrelevant to them though.
Specifics	On the cloud adoption wheel, most candidates felt this was the correct level of detail to be providing to general businesses who are

Question 4.	considering cloud adoption. The wheel was not too complicated, and at worst, at least suggested to first time adopters of cloud services that legal issues concerning cloud computing do exist, and that risk analysis should be carried out prior to cloud adoption. Legal experts did suggest that the wheel would have to include disclaimers indicating that users should only look on it as a heuristics wheel! Not to be taken completely as fact.
General Question 3.	On the question regarding where the guide fell down, technical experts believed there should be more technical information, legal candidates believed there should be more legal content! But both sets of candidates understood that a unique aspect of the guide was that it attempted to tackle the jurisdictional issues from different angles. There was a suggestion that the guide was too specific, and perhaps a more general guide on the legal issues affecting cloud computing would be more appropriate. It was pointed out that it was important to consider the intended audience prior to rolling out the guide, so it could be simplified or made more specific.
General Question 4.	General comments. Candidates found the guide useful, and indicated their desire for a copy of the full dissertation on completion. Candidates considered the guide a concise overview, to the point and suggested it would be very helpful to businesses to do the 'at a glance' look to see if cloud adoption is something they should explore at a more detailed level.

Table 8.2: Summary of Expert Responses

8.6 Conclusion

Chapter 8 of this work has attempted to out-line the experiment component of the dissertation. The experiment detailed is the result of the completion of the literature review in Chapters 2, 3, 4 and 6, the analysis of different jurisdictional perspectives on cloud computing in Chapter 5, and an interview process carried out with technical and legal experts outlined in Chapter 7. The research carried out and presented in those chapters highlighted the jurisdictional concerns related to storing personal data in a cloud computing environment, as the most important concern expressed by businesses contemplating cloud adoption. The experiment component outlined in this chapter centred on the production of a cloud computing user guide, tailored toward addressing how businesses can prepare themselves for the jurisdictional challenges when moving personal data into a public cloud. This chapter has explained how the resultant artefact tackles the jurisdictional issues under three headings, Education, Technical and Business. This chapter has also outlined the recommendations for businesses under each of these headings that are presented in the user guide booklet. A section of the booklet is also concerned with database technologies which can be adapted to lock down data to approved jurisdictions, and the Cloud Adoption Wheel, also presented in the booklet has been explained and demonstrated in this chapter.

The booklet accompanying this chapter is entitled, ‘User Guide: Jurisdictional Issues in Cloud Computing’. This user guide makes up the experiment component of this work. Details of how it was sent and the questions used to evaluate its usefulness to businesses have been outlined here. As has a summary of the resulting evaluations from each of the interview candidates. The evaluation process suggested the guide would prove very useful to business wanting to take a ‘first glance’ at the potential issues which exist around cloud computing. The guide was considered a little too specific for many businesses who would want only a very high overview of ALL the legal issues affecting cloud. But as one of a series of guides, the artefact could prove useful to businesses. The legal matrix was singled out for praise, as a very easy means of identifying which jurisdictions are suitable for areas where it is safe to move data to, a suggestion for more countries to be included in this matrix was aired from both expert groups.

9. CONCLUSIONS AND FUTURE WORK

9.1 Introduction

This chapter reviews the dissertation and research carried out during its production. The research project aimed to answer three main questions:

1. What are the key legal challenges facing businesses who put data into a cloud computing environment?
2. What means, whether legal, technical or other, can be harnessed to lessen the impact of these legal challenges?
3. What different international perspectives exist on cloud computing.

The three questions have been explored and answered in Chapters 2, 3, 4, 5 and 6. The research was critically evaluated and recommendations drawn from the analysis. The project attempted to have the following hypothesis evaluated; that the developed user guide to jurisdictional issues in cloud computing would enable businesses investigating cloud technologies to;

1. Become familiar with the pertinent legal issues affecting data once it is put into a cloud computing environment.
2. Become more educated and informed on the means of mitigating against the legal challenges facing cloud adoption.
3. Easily find other resources where more information relating to these topics could be discovered.

The evaluation of the hypothesis is detailed in Chapter 8. This was made possible by having the user guide reviewed by the technical and legal experts interviewed as part of this dissertation. Candidate6 was also re-interviewed for the purpose of evaluating the user guide produced.

Whilst Chapter 8 placed all the research recommendations from the six preceding chapters in the context of a cloud user guide, this chapter set apart three high level areas of focus. These recommendations are important to successful cloud computing data migration projects. The recommendations came under three headings:

Education – Recommendations here focused on individuals knowing the pertinent legal information they should be familiarising themselves with prior to moving data into a cloud computing environment.

Technology – Here recommendations focused on what technical means could be availed of to mitigate the jurisdictional issues of data in the cloud.

Business – Finally recommendations for business process changes were highlighted; outlining the business processes and policies that should be in place to ensure the jurisdictional pitfalls in the adoption of cloud services could be avoided.

Education Recommendations	1	Under European Directive 95/46/EC, Personal data is defined as any information relating to an identified or identifiable natural person. Under the directive, organisations have key responsibilities in relation to personal data they store; and these obligations have eight rules.
	2	Institutions that move data to the cloud environment, are deemed data controllers, and as such are required to ensure that all processing of personal data within the cloud environment is fair and lawful.
	3	Personal data can only be transferred outside the EEA to countries where an adequate level of protection is seen to be applied. These countries are Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man and Jersey. Compliance may be achieved through using EU approved contract terms with a provider. Alternatively, using a provider in the US who has signed up to the Safe Harbour provisions will be necessary.
Technology Recommendations	1	Where data to be housed in a cloud environment is of a personal nature, ensure the cloud provider utilises geolocation technology to lock-down your data to jurisdictions you have pre-chosen in consultation with that provider.
	2	Where geolocation services are not offered as part of the initial cloud offering, and a database service is being availed of, in the SLA negotiations ensure the cloud vendor uses geolocation functionality inherent to those databases to lock down database transactions to pre-agreed jurisdictions.
	3	Where data is stored in databases in the cloud, ensure geolocation information from the database server is recorded as data is moved between databases/database tables, and ensure the cloud provider make this data freely available

Business Process Recommendations	1	Data is an asset, If not already in place, begin the process of developing a Data Governance framework for your business that matches the business goals of your organisation.
	2	Begin the process of adopting and implementing an accredited IT Capability Maturity Framework. Such models provide a concise management roadmap to optimise business value derived from IT investments.
	3	It is imperative that policies and procedures are in place ensuring correct guidelines are followed when business require the delivery of any IT service. Avoid business units going outside the organisation for IT services by ensuring; IT networks and system are adequately locked down, preventing unauthorised access both from within and outside the organisation. Work towards building open communication channels between IT and the business, to demonstrate the services IT can provide. When a service cannot be facilitated by in-house IT, ensure business and IT work together to ensure the proper solution is provided, in a secure and cost-effective manner.

Table 9.1: Key Recommendations

9.2 Research Definition & Research Overview

Section 2.5 of this document, 'Business and Marketing in Cloud Computing', identified the marketing spin put on cloud services. The advantages of cloud computing espoused by marketing companies were explored. There is little doubt cloud computing does offer advantages over more traditional computer models in many circumstances, lower upfront capital expenditure costs, on-demand provisioning of resources etc. Cloud computing is not without its problems though. Some of these issues are not unique to cloud computing, but have become more relevant since the emergence of cloud computing. Some of these shortcomings are technical, and in Chapter 6, some of the technical difficulties relating to databases in the cloud were addressed. Many of the problems though relating to data in a cloud computing environment are legal ones.

The aim of the research project was to investigate the legal challenges faced when data was placed in a cloud computing environment, and to produce a user guide on the jurisdictional issues in cloud computing. The user guide will assist businesses attempting to determine the salient legal issues relating to data in the cloud, and provide direction as to ways these legal challenges can be ameliorated.

9.3 Contributions to Body of Knowledge

The challenges facing businesses moving data into a cloud computing environment were identified as the main research area of this project. The motivation for this is the slow adoption and nervousness of cloud computing by many large organisations such as financial institutions and government departments. Following this, a user guide making recommendations on the important legal information which should be known prior to moving data to the cloud was created. The motivation for development of the user guide was the need to address the identified challenges and provide businesses with a guide to understanding the legal implications of putting data in a cloud computing environment. There was also a need for businesses to understand ways of circumventing these legal challenges.

In order to achieve this, an extensive literature review on cloud computing, the law as it relates to IT, IT law as it relates to cloud computing, international perspectives on cloud computing, geolocation technologies and database technologies was conducted. A serious of interviews with technical and legal experts, having experience and practice in cloud computing projects was also carried out. The objective was to ascertain what organisations understood to be the most important legal concerns facing the adoption of cloud computing, and in particular, what they understood to be the legal concerns facing data moved to a cloud computing environment.

An extensive exploration of regulations on privacy and data protection, intellectual property and contract liability was carried out, as was an investigation into international perspectives on cloud computing. Technologies around the cloud were also analysed in an attempt to understand what technologies would be suitable to address the legal challenges facing cloud computing.

The literature and interview process revealed data protection as the most prominent legal issue the business community felt hampered the adoption of cloud technologies. Jurisdictional issues were also highlighted as reasons why businesses were nervous and reluctant to move data into the cloud environment. Businesses and even the legal fraternity felt that European Union and national regulations on data protection were not totally clear. Businesses were not totally sure who was responsible when legal issues arose with data in the cloud. Businesses too were not completely familiar with the concept of personal data, and the obligations they had in ensuring personal data they possessed was kept safe and secure. There also seemed to be a lack of knowledge on the differing international rules and regulations that affect cloud computing.

The aim of the research was to develop a user guide composed of a set of recommendations that would assist organisations in navigating through the legal difficulties brought about when data is put into a cloud computing environment. The user guide was evaluated by technical and legal experts and proved to be applicable in a real world business context.

Following the evaluation of the user guide, it is clear that with some minor modifications, the guide, and subsequent guides of this nature would be very positively received by business, and would go some way to helping organisations get ready for the adoption of cloud services.

9.4 Experimentation, Evaluation & Limitations

The interview process carried out as part of this dissertation served two purposes, first, it served to back up the research done in the literature review, helping to identify what the most crucial legal issues businesses have encountered with cloud computing. Second, it identified individuals who had the knowledge and experience required to evaluate and critique and artefact culminating from the interview and literature review process. The questions for the interview process were designed in such a way as to find out what the interviewees thought were the most salient, relevant and current issues affecting cloud computing adoptions. The dissertation was attempting to discovery what experts in the field thought the most challenging legal aspects of cloud computing were, and if the issue of data protection in the cloud was considered a significant concern.

The interview process helped mould the user guide detailed in Chapter 8. The user guide attempted to offer recommendations to business on the legal challenges faced when putting data into the cloud environment, and steps that could be taken to successfully navigate those legal challenges. A second set of questions had to be constructed to have the user guide evaluated. These questions attempted to gauge the suitability of the artefact for the modern business environment. These questions were emailed to all candidates who took part in the interview process. Criticisms of the artefact were encouraged. Responses were mainly positive and recommendations were made on how the user guide could be improved and changed to more fully address the legal issues businesses are encountering while considering adopting cloud services.

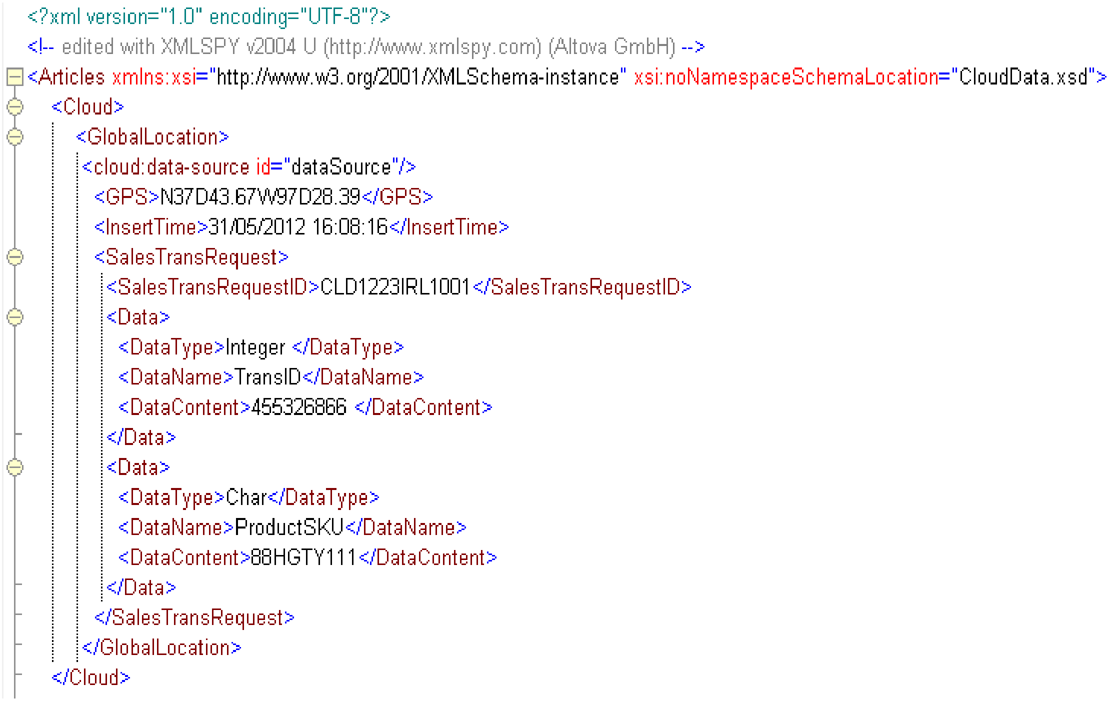
9.5 Future Work & Research

Cloud computing is a relatively new computing paradigm. The technologies that underscore many cloud computing services have been around for decades, as has the notion that computing resources could be sold as a service, on a pas-as-you-use basis. Only in the last decade though, have the technologies, the marketing and the environmental factors come together to make cloud computing a reality. Seen then as a 'new' computing model, potential for research and future work in the area is enormous.

This work focuses heavily on the legal implications of putting data into a cloud computing environment, and on the jurisdictional issues which arise when that data is moved between countries in the cloud environment. This is only a tiny component of the legal challenges that face businesses moving data into the cloud. There are also other legal challenges, issues with Intellectual Property, Contractual Liability, Vendor lock-in, E-Discovery etc. There are also other non-legal issues involved with cloud adoption, security for example remains a huge concern for businesses moving data into the cloud. The booklet generated in chapter 8 could feasibly therefore become a serious of booklets assisting business on all the legal issues they need to consider before adopting cloud.

This dissertation also focused on one technical area which could help overcome the legal challenges of cloud computing; geolocation technology was put forward as technology which could assist in locating data and preventing data from being moved to jurisdictions outside the agreed scope of a service level agreement. The scope for advancing other technical solutions to the legal issues inherent in cloud computing is vast.

Standards for data residing in cloud environments also need to be researched. This standard could involve meta-data being added to all data formats, enabling geolocation to become an easier task. Standards too need to be researched for more general cloud topics, such as cloud security, cloud contracts, movement of data between cloud vendors, retrieving data when the cloud provider becomes insolvent, deletion of data once the cloud contract is terminated. Figure 9.1 depicts sample XML code that could demonstrate components of a new protocol for cloud data.



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v2004 U (http://www.xmlspy.com) (Altova GmbH) -->
<Articles xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="CloudData.xsd">
  <Cloud>
    <GlobalLocation>
     <cloud:data-source id="dataSource"/>
      <GPS>N37D43.67W97D28.39</GPS>
      <InsertTime>31/05/2012 16:08:16</InsertTime>
      <SalesTransRequest>
       <SalesTransRequestID>CLD1223IRL1001</SalesTransRequestID>
       <Data>
         <DataType>Integer </DataType>
         <DataName>TransID</DataName>
         <DataContent>455326866 </DataContent>
       </Data>
       <Data>
         <DataType>Char</DataType>
         <DataName>ProductSKU</DataName>
         <DataContent>88HGTY111</DataContent>
       </Data>
      </SalesTransRequest>
     </GlobalLocation>
  </Cloud>
```

Figure 9.1: Sample XML code for cloud data.

Figure 9.1 demonstrates the use of ‘cloud data-source id’ tags, which could represent a global standard for locating data centers, each data center being assigned a unique id as they register with an approved body. ‘GPS’ and ‘InsertTime’ tags could be populated as data is moved between data centers. If standards were applied such that data in a cloud environment could only exist in this format, tracking the location of data could become a less arduous task. Having a standard for cloud data would also aid cloud-to-cloud integration, for situations where a client wishes to change cloud vendors. Retrieval of data from the cloud would also become a more standardised task.

There is also scope for incorporating the Cloud Adoption Wheel into a Cloud Maturity Model. This would allow organisations to determine how ready they are to engage with what level of cloud. The tool could be interactive in nature, allowing variables representing particular features to be entered into a system; data type, application type, business size, business sector, etc. Based then on the cloud maturity algorithm, the suitability of the business to migrate to the cloud could be determined. Recommendations too could be presented; outlining what actions the organisation needs to take to ensure they become more 'cloud ready'.

Another area for future investigation is visualisation. Visualisation tools could be developed to show the locations of all user data on the cloud. This tool could provide a graphical representation of where data had resided over a period of time. The tool could potentially be adapted to display country information on where attempts were made to move data, but where geolocation policies in place blocked this data transfer.

Education is also another viable area for further research. Accredited training courses on Cloud for Mangers need to be investigated. These courses could give invaluable legal and technical information on cloud computing, informing managers of the legal pitfalls inherent in cloud, and educating them on the technical mechanisms that cloud providers can and should be using to ensure cloud services follow the best practice standards possible.

Time constraints meant only six countries could be analysed to assess different international perspectives on cloud computing. This would certainly need to be broadened out to cover at least all first and second world countries, or countries that at least had the suitable infrastructure for hosting cloud data centers.

9.6 Conclusion

This chapter has attempted to present an overall conclusion of the research carried out and the recommendations for future research. The Research Definition and Research Overview were outlined, explaining how the purpose of the dissertation was to investigate the legal challenges faced when data was placed in a cloud computing environment, and to produce a user guide on the jurisdictional issues in cloud computing. The research contribution to knowledge was identified as the user guide – advancing recommendations to business on the legal implications of placing data into a cloud computing environment.

Research evaluation methods were presented and the results and recommendations from the evaluation process were discussed. Future areas of research were also highlighted, these focused on the following areas; other legal areas that affect cloud computing, Intellectual Property, Contractual Liability, Vendor Lock-in and more, Other technological solutions to tackle the legal issues with cloud computing, Increasing the country list for examining different international perspectives on cloud computing, and looking at implementing a set of standards for data stored in the cloud, and indeed standards for other more general cloud areas.

10. REFERENCES

Abe Lisa K. 2011’ Cloud Computing: Copyright Law’[Online] Available at:
http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/71540bd9-c5d8-4683-8186-2c7ccf2c0f00/Cloud_Computing_Copyright_Law_Mar_31_2011_Lisa_Abe.pdf
[Accessed: 22 March 2012]

Adams A. 2010 'Law for Business Students', 6th edition, Pearson 2010

amazon.com 'Amazon Relational Database Service (Amazon RDS)'
[Online], available at:
http://aws.amazon.com/rds/#pricing
[Accessed 10 May 2012]

arthurcox.com 2010 'Choosing Ireland as a location for your Intellectual Property Trading Company'[Online].Available at:
http://www.arthurcox.com/uploadedFiles/Publications/Publication_List/Arthur%20Cox%20-%20Choosing%20Ireland%20as%20a%20location%20for%20your%20Intellectual%20Property%20Trading%20Company,%20December%202010.pdf
[Accessed 28 April 2012]

Bainbridge D. 2004 'Introduction to Computer Law', 5th Edition, Pearson 2004
blogs.ics.ie 2009 'Electronic signatures'
[Online]. Available at: http://blogs.ics.ie/itlaw/2009/11/02/electronic-signatures/
[Accessed 28 April 2012]

BSA 2012 'Global Cloud Computing Scorecard'
[Online]. Available at: http://portal.bsa.org/cloudscorecard2012/index.html
[Accessed 25 April 2012]

Businessweek.com 2011 ‘Deutsche Telekom Wants ’German Cloud’ to Shield Data From U.S.’ [Online]. Available at:
http://www.businessweek.com/news/2011-09-14/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html
[Accessed 21 March 2012].

capb.ca 2008 'Canadian Association of Police Boards - A report on cybercrime in Canada'
[Online] Available at:
http://www.capb.ca/FCKeditor/editor/fileCabinet/CAPB_Report_on_Cyber_Crime.pdf
[Accessed 1 May 2012]

cippic.ca 2011 'RE: Omnibus Crime bill'
[Online] Available at: http://www.cippic.ca/sites/default/files/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf
[Accessed 1 May 2012]

cloudtweaks.com 2012 'Cloud Infographic: Cloud Drivers For Adoption'
[Online], Available at:
http://www.cloudtweaks.com/2012/02/cloud-infographic-cloud-drivers-for-adoption/
[Accessed 10 April 2012]

Cloudmarketing.org 2012 'what is cloud marketing?'
[Online], Available at:
http://www.cloudmarketing.org/
[Accessed 10 April 2012]

compliancesearch.com 2012 'Europe Leverages Consumer Distrust Patriot Act's Data Turnover Requirements' [Online]. Available at:
'http://compliancesearch.com/wallstreetjobreport/current-affairs/europe-leverages-consumer-distrust-patriot-acts-data-turnover-requirements/[Accessed 21 March 2012]

computerworlduk.com 2012 'Banking giant BBVA moves internal apps to Google cloud'
[Online], Available at:
http://www.computerworlduk.com/news/cloud-computing/3329429/banking-giant-bbva-moves-internal-apps-to-google-cloud/
[Accessed 11 April 2012]

conventions.coe.int 2012 'Convention on Cybercrime'
[Online]. Available at:
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG
[Accessed 26 April 2012]

CSA (2009) 'Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance'
[Online]. Available at: https://cloudsecurityalliance.org/csaguide.pdf
[Accessed 08 April 2012]

C. Ian Kyer Gabriel M.A. Stern 2011, 'Where in the World is My Data? Jurisdictional Issues with Cloud Computing' March 30, 2011.
[Online], Available at 'http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf'
[Accessed 12 March 2012]

dataprotection.eu '3.1. First generation data protection norms'
[Online]. Available at:
http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.FirstGeneration
[Accessed 05 March 2012]

dataprotection.ie 'About Us'
[Online]. Available: http://dataprotection.ie
[Accessed 27 April 2012]

De Busser, Els 'Data Protection in EU and US Criminal Cooperation' Maklu, 2009.

Ditka Reiner 2011 'The Cloud And The Hype'
[Online], Available at:
http://www.mypurchasingcenter.com/technology/technology-blogs/the-cloud-and-the-hype/
[Accessed 10 April 2012]

europa.eu UK 'Press releases RAPID'
[Online]. Available at:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/811
[Accessed 30 April 2012]

Draft NIST SP800 2011 'DRAFT Cloud Computing Synopsis and Recommendations'
[Online], Available at:
http://csrc.nist.gov/publications/PubsDrafts.html
[Accessed 08 May 2012]

eff.orgt 2011 'This Week in Internet Censorship'
[Online], Available at :https://www.eff.org/deeplinks/2011/12/week-internet-censorship
[Accessed 01 May 2012]

finance.yahoo.com 'Facebook To Boost Privacy After Investigation'
[Online]. Available at http://uk.finance.yahoo.com/news/facebook-boost-privacy-investigation-115901698.html [Accessed 05 March 2012]

forrestertools.com 2012 'Global Heat Map'
[Online]. Available at: http://heatmap.forrestertools.com/
[Accessed 25 April 2012]

Goldman, S.R., Dyer, M. & Flowers, M., 1987. Precedent-based legal reasoning and knowledge acquisition in contract law: A process model. In *Proceedings of the First International Conference on Artificial Intelligence and Law*.

Greenleaf, Graham , Five Years of the Apec Privacy Framework: Failure or Promise? (June 30, 2009). Computer Law & Security Report, Vol. 25, pp. 28-43, 2009. Available at SSRN: http://ssrn.com/abstract=2022907
[Accessed 1 May 2012]

Jaeger, P.T., Lin, J. & Grimes, J.M., 2008. Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information Technology & Politics*, 5(3), pp.269-283. [Online]. Available at:
http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479
[Accessed 10 March 2012]

JISCLegal 2011a ‘Report on Cloud Computing and the Law for UK FE and HE (An Overview)’[Online] Available at:
http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/Report%20on%20Cloud%20C

omputing%20and%20Law%20UKFEHE%20-%202011.pdf [Accessed 16 March 2012]

Hon, W. Kuan, Hörnle, Julia and Millard, Christopher, Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3 (September 7, 2011c). Queen Mary School of Law Legal Studies Research Paper No. 84/2011. Available at: SSRN: http://ssrn.com/abstract=1924240 [Accessed 21 February 2012]

Hon, W. Kuan, Millard, Christopher and Walden, Ian, The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1 (March 10, 2011 a). Queen Mary School of Law Legal Studies Research Paper No. 75/2011. [Online] Available at: SSRN: http://ssrn.com/abstract=1783577 or http://dx.doi.org/10.2139/ssrn.1783577 [Accessed 18 March 2012]

Hon, W. Kuan, Millard, Christopher and Walden, Ian, Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2 (March 21, 2011b). Queen Mary School of Law Legal Studies Research Paper No. 77/2011. Available at: SSRN: http://ssrn.com/abstract=1794130 [Accessed 21 February 2012]

ICC 2005, International Chamber of Commerce ‘Intellectual Property:Source of innovation,creativity, growth and progress’[Online]. Available at:http://www.iccwbo.org/uploadedfiles/ICC/policy/intellectual_property/Statements/BASCAP_IP_pub.pdf [Accessed 03 March 2011]

itwire.com 2012 'Gartner: Top 5 Cloud Computing trends'
[Online], Available at:
http://www.itwire.com/press-release/53841-gartner-top-5-cloud-computing-trends
[Accessed 10 April 2012]

jackofallclouds.com 2011 'State of the Cloud – January 2011'
[Online], Available at:
http://www.jackofallclouds.com/2011/01/state-of-the-cloud-january-201/
[Accessed 09 April 2012]

jipitec.eu 2008 'Kontent i Pravo v. Masterhost'
[Online], Available at :http://www.jipitec.eu/issues/jipitec-1-3-2010/2796/labesius-masterhost.pdf
[Accessed 01 May 2012]

kilroys.ie 2002 'Electronic signatures'
[Online]. Available at:
http://www.kilroys.ie/library/it/electronic_commerce_act_2000.htm
[Accessed 28 April 2012]

Kuner, C., Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1).
SSRN eLibrary. [Online] Available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496847
[Accessed 10 March 2012].

kurzweilai.net 'Cloud Architecture'
[Online], Available at:
http://www.kurzweilai.net/images/Cloud-Computing.png
[Accessed 08 May 2012]

Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas 2011 'DRAFT Cloud Computing Synopsis
and Recommendations'
[Online], Available at:
http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
[Accessed 08 April 2012]

Lloyd, Ian J. 2011 'Information Technology Law', 6th Edition, Oxford 2011
Michael Armbrust, Armando Fox, Rean Griffith,Anthony D. Joseph, Randy Katz, Andy Konwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,and Matei Zaharia 2009 'Above the Clouds: A Berkeley View of Cloud Computing'
[Online], Available at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf [Accessed 23 March 2012]

Michael Armbrust, Armando Fox, Rean Griffith,Anthony D. Joseph, Randy Katz, Andy Konwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,and Matei Zaharia 2010 ‘A View of Cloud Computing ‘
[Online], Available at:
http://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext
[Accessed 23 March 2012]

Michael D. Scott.2008 ‘History of Computer/IT Law’
[Online] Available at:
http://singularitylaw.com/technology-law/history-of-computerit-law-1960-1969
[Accessed 11 March 2012].

Mike Gray 2010 'Cloud Computing: Demystifying IaaS, PaaS and SaaS'[Online], Available at:http://www.zdnet.com/news/cloud-computing-demystifying-iaas-paas-and-saas/477238[Accessed 08 April 2012]

mondaq.com 2011 'China: Recent Data Privacy Law Developments'
[Online], Available at
:http://www.mondaq.com/x/158186/Privacy/Recent+Data+Privacy+Law+Developments
[Accessed 01 May 2012]

morganstanley.com 2011 'Cloud Computing Takes Off Market Set to Boom as Migration Accelerates'
[Online], Available at:
http://www.morganstanley.com/views/perspectives/cloud_computing.pdf
[Accessed 09 April 2012]

Nelson M 2009 ‘The Cloud, the Crowd, and Public Policy‘ [Online] Available at:
http://www.issues.org/25.4/nelson.html [Accessed 22 March 2012]

Newman J. 2012, ‘SOPA and PIPA; Just the facts’ [Online]. Available at: http://www.pcworld.com/article/248298/sopa_and_pipa_just_the_facts.html [Accessed 04 March 2011]

NIST SP500-291 'NIST Cloud Computing Standards Roadmap'
[Online], Available at:
http://csrc.nist.gov/publications/PubsDrafts.html
[Accessed 08 May 2012]

no.more.racketware.info 2012 ‘Hardware-software bundling crumbles in France’
[Online] Available at:
http://no.more.racketware.info/news/hardware-software-bundling-crumbles-france
[Accessed 14 March 2012].

O'Connor J. 2011 'Ireland: Computing In The Cloud: Clear Skies Ahead Or Clouds On The Horizon? '[Online], Available at:http://www.mondaq.com/x/152578/Cloud+Computing/Technology+and+Commercial+Contracts+Newsletter [Accessed 23 March 2012]

practicallaw.com 2011 'Data Protection: Russian Federation'
[Online], Available at:
http://www.practicallaw.com/2-502-2227?q=*&qp=&qo=&qe=#a362235
[Accessed 01 May 2012]

Rajkumar Buyya,Chee Shin Yeo,Srikumar Venugopal 2008 'Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities'
[Online], Available at:
http://arxiv.org/ftp/arxiv/papers/0808/0808.3558.pdf
[Accessed 23 March 2012]

Ratnadeep Bhattacharjee 2009, 'An analysis of the Cloud Computing Platform'
[Online], Available at:
http://dspace.mit.edu/handle/1721.1/47864
[Accessed 08 April 2012]

Reidenberg, J., Technology and Internet Jurisdiction. *SSRN eLibrary*. [Online]. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=691501
[Accessed 12 March 2012].

Ruse-Khan, H.G. 2011, From TRIPS to ACTA: Towards a New “Gold Standard” in Criminal IP Enforcement? SSRN eLibrary. Available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1592104
[Accessed April 26, 2012].

russianlaw.net 2005 'Electronic signatures in Russian law'
[Online], Available at :http://www.russianlaw.net/en/
[Accessed 01 May 2012]

savvis.com 2009 'Securing the Cloud A Review of Cloud Computing, Security Implications and Best Practices'
[Online], Available at:
http://www.savvis.com/en-us/info_center/documents/savvis_vmw_whitepaper_0809.pdf
[Accessed 08 May 2012]

scaledb.com 2009 'Database Virtualization and the Cloud'
[Online], Available at:
http://www.scaledb.com/pdfs/Cloud_Databases_WhitePaper2.pdf
[Accessed 10 May 2012]

Scott Sanchez, 'Location, Location, Location - Storing EU Data with Safe Harbor' (*Cloud Computing Journal* 2010) . [Online]. Available at: http://cloudcomputing.sys-con.com/node/1562070
[Accessed 21 March 2012]

Shimba, F., 2010. 'Cloud Computing: Strategies for Cloud Computing Adoption.'
[Online] Available at:
http://arrow.dit.ie/cgi/viewcontent.cgi?article=1028&context=scschcomdis
[Accessed 08 April 2012].

smartplanet.com 2012 'BBVA dumps Microsoft for Google cloud'
[Online], Available at:
http://www.smartplanet.com/blog/global-observer/bbva-dumps-microsoft-for-google-cloud/2555
[Accessed 11 April 2012]

techtarget.com 2002 [Online] Available at:
http://searchdatamanagement.techtarget.com/definition/Patriot-Act
[Accessed 10 March 2012].

techtarget.com 2009 'Who's who in cloud computing: Understanding the market's players'
[Online] Available at:
http://searchcloudcomputing.techtarget.com/news/1355062/Whos-who-in-cloud-computing-Understanding-the-markets-players
[Accessed 09 April 2012]

telegraph.co.uk 'Google 'sneaking away citizens' privacy' says EU commissioner'
[Online]. Available at:
http://www.telegraph.co.uk/technology/google/9117810/Google- sneaking-away-citizens-privacy-says-EU-commissioner.html
[Accessed 06 March 2012]

thecloudtimes.com 2011 'The pros & cons of DbaaS'
[Online], Available at:
http://thecloudtimes.com/2011/11/27/the-pros-cons-of-dbaas/
[Accessed 10 May 2012]

theinquirer.net 2012 'Lenovo loses French lawsuit over Windows bundles'
[Online] Available at:
http://www.theinquirer.net/inquirer/news/2144392/lenovo-loses-french-lawsuit-windows-bundles
[Accessed 14 March 2012].

thenewsmanual.net 2012
[Online] Available at:
http://www.thenewsmanual.net/Manuals%20Volume%203/volume3_63.htm
[Accessed 14 March 2012].

timesofindia.indiatimes.com 2012 'US puts India on copyright pirates "priority watch list'
[Online] Available at: http://timesofindia.indiatimes.com/tech/news/internet/US-puts-India-on-copyright-pirates-priority-watch-list/articleshow/12948861.cms
[Accessed 1 May 2012]

Tim Weber 2012 'Google persuades Spanish bank BBVA to use the cloud'
[Online], Available at:
http://www.bbc.co.uk/news/business-16486796
[Accessed 11 April 2012]

tjmcintyre.com 2010 'Cloud computing controversy won't clear '
[Online].Available at:
http://www.tjmcintyre.com/2010/03/cloud-computing-controversy-wont-clear.html
[Accessed 28 April 2012]

torrentfreak.com 2012 'UK Government Plans Web and Email Monitoring Law'
[Online]. Available at: http://torrentfreak.com/uk-government-plans-web-and-email-monitoring-law-120401/
[Accessed 30 April 2012]

webopedia.com 'cloud management'
[Online], Available at:
http://www.webopedia.com/TERM/C/cloud_management.html
[Accessed 08 May 2012]

whioam.com 2010 'Will the site owners responsible for their content?'
[Online], Available at :http://www.whioam.com/will-the-site-owners-responsible-for-their-content.html
[Accessed 01 May 2012]

wikipedia.org ACTA 2012 'Anti-Counterfeiting Trade Agreement'
[Online]. Available at: http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement
[Accessed 26 April 2012]

wikipedia.org China 'Internet censorship in the People's Republic of China'

[Online], Available at :http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China
[Accessed 01 May 2012]

wikipedia.org DMCA. ‘Digital Millennium Copyright Act ’
[Online] Available at:
http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
[Accessed 30 April 2012].
wipo.int 'WIPO Copyright Treaty'
[Online]. Available at: http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html
[Accessed 30 April 2012]

wisegeek.com ‘What is Legal Liability’ [Online]. Available at
http://www.wisegeek.com/what-is-legal-liability.htm
[Accessed 07 March 2012]

wordpress.com 2011, ‘Cloud Computing: legal dos and don’ts’ Online] Available at:
http://mariaipexpert.wordpress.com/2011/06/07/cloud-computing-legal-dos-and-don%E2%80%99ts/
[Accessed: 22 March 2012]

wto.org Russia 'Russian Federation'
[Online], Available at :http://www.wto.org/english/thewto_e/acc_e/a1_russie_e.htm
[Accessed 01 May 2012]`

www.wto.org 2012 'Overview: the TRIPS Agreement'
[Online]. Available at: http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm
[Accessed 26 April 2012]

zdnet.com 2009 'Eight ways that cloud computing will change business'
[Online], Available at:
http://www.zdnet.com/blog/hinchcliffe/eight-ways-that-cloud-computing-will-change-business/488
[Accessed 10 April 2012]

Zollers, F., Shears, P., McMullin, A, 2005.'No More Soft Landings for Software: Liability for Defects in an Industry that Has Come of Age' Santa Clara Computer and High Technology Law Journal, 21, 745 [Online]. Available at:
http://www.chtlj.org/sites/default/files/media/articles/v021/v021.i4.Zollers.pdf
[Accessed 07 March 2012]

APPENDIX A

Expert Interview Transcripts

Interview No.	1
Date	29-March-2012
Institution	Ernst & Young
Individual	Senior Manager
Comments	Interview candiate1 was happy for me to say I talked to Interview candiate1, senior manager, Ernst Young, but if I wanted to directly quote him, I would need to ask him about this as he would need to go thru the correct channels in E&Y concerning this. Very happy to review any artefact I send him, can call him too, if I have further questions. Recording didn't happen because of a fire alarm, and us having to leave the building! And then go to a busy coffee shop... also ate into our time, Interview candiate1 had to go at 11, so didn't get the full hour.
Question 1.	I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?
Answer 1. Interview candiate1 takes his concept of the cloud from the NIST definition, believes Cloud Computing is just a more complex iteration of hosting services. Cloud has the look and feel of a hosted service, but he points to the difference in that data could be stored anywhere. But essentially it's just terminology. It's running a 3rd party application from another location. There are however indirect dependencies which is also different he believes that other non-cloud models. Indirect dependencies insofar as you sign up to a cloud SAAS option, but then that SAAS provider must in turn sign up to a IAAS option ... etc. so there are multiple layers which add to the complexity. Recommended I look at the IIA.ie site, lot of good cloud stuff there, and also a cloud tool there to help business get ready for cloud adoption.	
Question 2.	How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?
Answer 2. Interview candiate1 believes cloud is a huge area of conversation now, Irish businesses are excited, they do want to get on board, but they are also cautious. The level of excitement and interest is predicated by the business sector and size. Some businesses wouldn't exist without it, e.g. oudlesvault.com (by ventisys), a company providing encryption services for files on mobile devices, but also backs up your data from mobile devices into the cloud. They wouldn't have an offering without the cloud. Cloud is front and center for start-ups. Larger businesses are ALL talking about the cloud, some businesses are obliged to look at the cloud because of strategic sourcing commitments, directors have heard there is cost savings associated with the cloud and they want it investigated. Large businesses are cautious though, they have the HR depts. Who know about issues of data protection, they have large IT expertise, so they know the technical pitfalls. Cloud has been around for a long time, but he believes a real watershed is coming in EMEA with BBVA bank of Spain adopting a cloud service, first big bank to do so, and this is being watched, using Google's	

suite of collaborative applications. http://www.bbc.co.uk/news/business-16486796

Interestingly BBVA are not putting any sensitive client data in the cloud, Interview candiate1 said they were criticised by cloud providers for this decision, as they wouldn't reach optimal savings, but Interview candiate1 said so what, they save 1 million, instead of 2, they're still saving a million. First bank to embark on this. BBVA did a huge amount of due diligence on this, had huge swathes of security people looking at it, in the end it was down to a risk based decision.

Others up to now only using niche cloud services like metalabs, cloud email hygiene filtering.

He felt big cloud providers (Microsoft/Google) are going after big organisations. But we are in the early days of the cloud maturity curve. Right now it's a big deal to move your email into the cloud, so there is a perception within industry that the up-take is slow but this will ramp up.

Question 3. I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?

Answer 3. Interview candiate1 talked about Data Protection being a concern of organisations, and they want to follow the DP principles. Clients know there is less protection for personal data when it goes outside the EU.

Whole scenario in DP about data controller and data processor is confusing for business.

Businesses believe they need to go with reputable providers in order to overcome DP issues and they place the trust there, but they also carry out intense due diligence, risk analysis. Interview candiate1 still reckons organisations need to thread very carefully, insofar as if they are putting data in the US. Ensure cloud company is signed up to safe harbour, but still this is not as good as European Data Protection arrangements. Safe-harbour is self regulated, and those espousing to have it are not audited.

Clients can get a little more peace of mind by using model contracts, Approved Arrangements for transferring personal data to third countries, and many clients are using model contracts.

The point was made about 'Shadow IT', a business group within the org by passing HR and IT and utilising a cloud service without the main business' knowledge. This is where DP problems may arise, but if there are proper controls in place in the org this shouldn't happen.

Citing Paypal as a crowd with an excellent data governance policy, they have a lot of stuff in the cloud, use downstream services for data processing. But they regularly visit cloud sites around the world (Philippines for example). This is fine, they have indirect control over the data in those data centers, but they don't have ultimate direct control at an operations level. What happens when they are not visiting the sites?

Interview candiate1 sees investigative issues (E-Discovery) as a big problem, a crime was committed, data in the cloud needs to accessed and tracked back to users, this is very difficult and difficult pinning down which laws apply. Forensic analysis in a public cloud. There is an extra consideration if your data is with a third party.

Another problem is 'lock in' if you have to break a contract, 30 days notice etc. and provider says ok, where do you want us to put your data, this is a huge issue.

Made the point about US company giving you choice of choosing an EEA location for data so you still are covered by the DPD. But said a US engineer might have to access your data if there is a problem, this issue of the data being looked at from the US for maintenance purposes can be covered in contracts.

Question 4. Do you think cloud vendors are violating the DPD principles?

Answer 4. This is a big statement, not the reputable suppliers, their terms are very open, you can see everything they espouse to be doing, they are open. So should be easy enough to see if they have done what they said they are doing.

E.g. Amazon for example is ISO 27001 certified, PCI certified.

Question 5.	Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?
Answer 5. Definitely, as with the BBVA decision to only move some data into the cloud. Maybe the model is not mature enough to cater for all data types yet.	
Question 6.	Again are clients aware of jurisdictional issues in regard to cloud computing?
Answer 6. If you had asked the question of jurisdiction to cloud providers like Microsoft or Google 18 months ago, they would have been fuzzy, now they bring it up, where do you want your data stored?, so that's a good thing.	
Question 7.	What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?
Answer 7. Interview candiate1 said the way cloud vendors look at it is this, if I charge you 100 euro per week for the service, and we are down half the week, we will give you back 50 euro. So the compensation model is not based on the loss the service will cost your business, more a return of the money you had paid for the service to be up when it was down. Bigger providers are reluctant to change their TOCs.	
Question 8.	If Irish government in the morning said they were putting a particular department's data in the cloud, what would you think?, would it depend on the dept. in Question?
Answer 8. Interview candiate1 would be fine with the move to the cloud, if he could see the steps the government took to make the decision that moving the department's data into the cloud was a good idea. I.e. look at the steps they took, how much investigation of the provider did they do, let's look at their risk analysis, how did they carry out due diligence. It's also a generational thing, my 17 year old nephew would think it's a great idea, my70 year old mother would be kept awake at night worrying about it, Interview candiate1 himself would be cynical about it, but his fears could be allayed if he saw the thought process around coming to the decision.	
Question 9.	Geolocation - Have you heard of this technology (explain if not), do you think it could help allay client's fears if they had definitive knowledge of the whereabouts of their data?
Answer 10. Wasn't sure about this, asked if I was looking to add some metadata tags to the data, and explained maybe looking at table insert triggers to grab geolocation info from the server and write to logs or email users, told me to look at DLP, data loss/leak prevention.	
Question 11.	Are there any other technical solutions you think I should be looking at?
Answer 11. Sounds fine, the IIA have something similar, a decision support matrix, have a look.	

Interview No.	2
Date	31-MAR-2012
Institution	Mason, Hayes & Curran
Individual	Legal Associate
Comments	Similar to the EY interview, Interview candiate2 was happy for me to say I talked to Interview candiate2, Associate at Mason, Hayes and Curran, but if I wanted to directly quote him, I would need to ask him about this later, as he would need to go through

<table>
<tr><td></td><td>the correct channels in MHC.Very happy to review any artefact I send him, can call him too, if I have further questions.Recording didn’t happen as meeting was in busy cafe in Stephen’s Green.</td></tr>
<tr><td>Question 1.</td><td>I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?</td></tr>
<tr><td colspan="2">Answer 1. Interview candiate2 said he had a short cynical answer to this and that was marketing. But being less cynical he said that contracts were the biggest difference from his point of view, he certainly didn’t think the difference was technical. In the old days when companies signed up to store data in a third party facility, or availed of some grid computing infrastructure the contracts which needed to be worked out were often arduous, ad-hoc and complicated. He felt cloud computing services were much more ‘off the shelf’ services, pre-packaged contracts, with just the click of a mouse to sign your signature, in that regard the contracts were nearly ‘automatic’. He also felt that cloud services were much easier to understand and use for the general office worker, this was a difference too, pre-cloud perhaps only technical experts had exposure to what was going on when availing of storage space or grid computing facilities.</td></tr>
<tr><td>Question 2.</td><td>How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?</td></tr>
<tr><td colspan="2">Answer 2. Interview candiate2 thinks it’s huge for start-ups, they obviously save an extraordinary amount of money by availing of cloud services, but they can be a little naive from a legal perspective and leave themselves open to some of the legal pitfalls that prevail with cloud computing.
Interview candiate2 believed that larger companies are cautious, they are very aware of the Irish Data Protection acts more so than the European Data Protection Directive. With facebook/google et al. being in the news lately, Billy Hawkes, the data commissioner in the papers etc., there is much more general awareness of dp issues with cloud. These issues have also been brought more to the fore with web 2.0, social media etc.
Businesses are also aware of new ‘General DP regulations’, coming down the track that will hit would-be violators in the pocket. Provisions are being proposed such that a fine of 3% of a company’s global turnover will be charged if the company violates DP laws. Interview candiate2 told me to look here for more on this:
http://www.irelandip.com/2012/03/articles/privacy-1/government-launches-consultation-on-new-data-protection-law-proposal/</td></tr>
<tr><td>Question 3.</td><td>I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?</td></tr>
<tr><td colspan="2">Answer 3. One area which Interview candiate2 thinks will become huge in the coming years is the concept whereby the cloud vendor goes bust or is shut down, or a company utilising cloud services for private data storage or application development is shut down or goes bust. The clients will want their data back, how will they get it back, in what medium, to what destination? He envisages huge problems with this.
Jurisdiction is a big one for Interview candiate2 and perhaps because he works directly in the area. He identified 2 areas of concern with jurisdiction; 1, is the governing law, covered by Article 4 of the DPD, ‘National law applicable’, It is to do with which governing law has jurisdiction over a body when there is a legal problem. Interview candiate2 believes Art 4 of the European DPD is a really badly drafted piece of legislation.
From St. Mary’s of London paper, Art 4, In a cloud computing context, determine the extent to which a user or provider of cloud computing services, even if not incorporated, resident or headquartered in an EEA Member State, may become subject to obligations under EU data protection law as a result of:
1. having a subsidiary, branch or agent, or even just a data center, in the EEA; or
2. Making use of a data center located in the EEA, or other equipment located in the EEA.</td></tr>
</table>

<table>
<tr><td colspan="2">For problems with Art 4, Interview candiate2 sees more of an issue with the location of the company's office than the actual data. Art 4 has been transposed into local law very differently across the EU so it is very difficult to see how harmonisation in EU law has been achieved here.

Interview candiate2 told me to take a look at the full report by Gary Davis (deputy data commissioner) on Facebook. He said there are some technical annexes here which demonstrate art 4:

http://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

The second part of jurisdiction which Interview candiate2 said was very important were the rules concerning data export. Sections 2 of the Irish data acts cover this apparently. Interview candiate2 believes the law is about 10 years behind technical advances and when laws were drafted concerning the export of data it was probably more to do with stopping people putting data CDs in their luggage and boarding a flight with them.

Interview candiate2 said that companies are very aware of their obligations in respect of the Irish data protection acts and are therefore quite cautious before exporting data out of the state. He said that in order for companies to do this legally, they are coming to firms like his and paying lawyers a lot of money to have contracts drafted up carefully so they can export their data without falling foul to any legal ramifications.

He said the Irish government have at their disposal, a legal mechanism known as a prohibition order, which they can use to stop a body exporting data outside the state, and larger companies are aware of this, and don't want to fall foul of it.</td></tr>
<tr><td>Question 4.</td><td>Do you think cloud vendors are violating the DPD principles?</td></tr>
<tr><td colspan="2">Answer 4. Unlikely to be violating, particularly the larger more reputable organisations.</td></tr>
<tr><td>Question 5.</td><td>Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?</td></tr>
<tr><td colspan="2">Answer 5. Clients are aware of it, but even more aware and cognisant of the Irish acts pertaining to data protection.</td></tr>
<tr><td>Question 6.</td><td>Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?</td></tr>
<tr><td colspan="2">Answer 6. Would definitely have more concern over sensitive data being put into a cloud environment.</td></tr>
<tr><td>Question 7.</td><td>What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?</td></tr>
<tr><td colspan="2">Answer 7. Interview candiate2's take on this was that these were 'AS IS' contracts, you take the service and conditions as is, if you don't like them, don't sign them. He felt that cloud vendors could get away with a lot of this stuff because it's a fairly closed market right now, not enough competition in the space, just some huge players, when the market opens up more, vendors will have to start accepting more liability. He did agree the terms in some contracts were shocking, but if the client is large enough the terms will and can be changed, if you are a smaller company you have NO CHANCE. But some of the abdication he believed is mitigated by the fact that the services are so easy to use and simple to understand, yes they can be crucial to some businesses (start ups for example) but you know the deal going in, and if it goes bad you have been warned.

The other side to this of course was whether these contracts would stand up in the Irish courts, as far as Interview candiate2 was aware there has never been an Irish cloud case. But there are provisions in place in Irish law to protect people against completely onerous contracts. The nature of contracts means there should be some mutual obligations on both parties, if one party completely attempts to abdicate ALL responsibility then this isn't a contract.</td></tr>
</table>

He also said vendors are very smart about the final clause (usually the final clause) in the contracts, which usually designates the company's place of business, and this is usually in a state in the US where contract law is heavily biased towards the vendors. This is important apparently in a legal context if these TOCs are ever debated.	
Question 8.	If Irish government in the morning said they were putting a particular department's data in the cloud, what would you think?, would it depend on the dept. in Question?
Answer 8. Interview candiate2 said this would really depend for him on the sensitivity of the data. He would really like to make sure the data is being handled by a reputable cloud vendor, and he would want 'audit rights' to be written into the contract. Audit rights he believes would not be entertained for a small company, but a government department or agency should have much more sway with the cloud vendor. He would also feel a lot happier if the data was staying within the jurisdiction of the state, or at worst was staying within the EEA. He told me to look at AL goodbody, guy there Mark Rasdale, writing some good stuff on this.	
Question 9.	Does the judiciary have the skills or how much do they need to understand about cloud computing to apply the law correctly.
Answer 10. Interview candiate2 spoke of the judiciary being incredibly intelligent, and he had seen many examples of where IT concepts had been explained to them and they understood the concepts very quickly. He said if a cloud case came before a judge he or she would not have to know the complete ins and outs of the technology, they would most likely get in legal impartial experts to give them advice, and they would make decisions based on that.	
Question 11.	Have you heard of this Geolocation technology, do you think it could help allay client's fears if they had definitive knowledge of the whereabouts of their data?
Answer 11. Interview candiate2 loved the technical solution to data being where it was supposed to be .. and alerts if it goes to a jurisdiction it shouldn't ... he said he is working in this area now and that they are constantly having to build this stuff into contracts, so he said if there was a technical side to help this, he called it 'technical comfort' ... that would be a real winner for his clients .... I explained the technical side whereby cloud vendors would have to install scripts etc. on their dbs so this could happen and this wouldn't be easy, but he made the point that maybe I'm going into the business side of it too much ..... if the concept is a good one .. the business side would take care of itself.	
Question 12.	Should my focus be directed in another area/should I be doing anything different?
Answer 12. Interview candiate2 definitely thinks I am reading in the correct area and that the Queen Mary's college of London have produced the best papers on the legal side of the cloud.	

Interview No.	3
Date	17-APR-2012
Institution	Dillon Eustace
Individual	Legal Associate
Comments	Unlike other candidates Candidate3 had no opinion on whether he wanted to keep any level of the interview confidential, although candidate didn't think we would discuss anything that would be controversial or peculiar to Dillon-Eustace's opinions on Cloud .Very happy to review any artefact I send him, can call/email him too if I have further questions.
Question 1.	I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?

<table>
<tr><td colspan="2">Answer 1. Interview candiate3 just had a bog standard view of cloud, ‘computer power delivered like a utility over the internet’, didn’t think it really represented any other difference at all to the likes of grid computing/ storing data on rented server space. Didn’t feel either that cloud had made much of a difference to legal issues he dealt with on a day to day basis relating to IT. As far as he was concerned cloud was just another way IT companies were badging and selling a service they were already selling.</td></tr>
<tr><td>Question 2.</td><td>How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?</td></tr>
<tr><td colspan="2">Answer 2. Candidate 3 seemed to focus on the cautious aspect of this question, he thought businesses were interested in cloud, but many businesses were playing a wait and see game. He commented that there was such bad press coverage for an organisation when there was a data breach and that companies were conscious of this and were therefore incredibly cautious about what they do with cloud. They want to see other big players dip their toe in the water and then see if it’s safe for them to do the same.

He actually thought that some of the cloud contracts were putting businesses off cloud. The take it or leave it approach to some of the contracts was in his opinion very off-putting for some businesses and they were deciding to leave it.</td></tr>
<tr><td>Question 3.</td><td>I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?</td></tr>
<tr><td colspan="2">Answer 3. Candidate3 believed Data Protection was the biggest issue with cloud. He said Irish businesses are very aware of the data protection acts 1988 and 2003, and are aware of their obligations under those acts. Candidate3 talked very much about the role of the Data Controller and Data Processor explaining that the company deciding to put their data into the cloud remained the controller and were very much in charge (particularly from a legal perspective) of what happened with the data. It was therefore the customers of the cloud vendors who were responsible for the protection of the data. He said Irish companies were aware of the Data Controller responsibilities bestowed on them by the law. He said ignorance of the law (ignorance of your responsibilities as the Data Controller) was no excuse if you find yourself in court for a breach of data protection law. He said the recent cases with Facebook for example highlighted the importance with which data protection is regarded in Ireland.

Candidate3 didn’t really know if cloud had made Intellectual Property issues more of a concern for business, perhaps no more so than the problems already affecting IP rights posed by the internet.

He said Contracts were certainly a legal concern, but answers the contract problems more fully in question 7.

Candidate3 was aware that there were some jurisdictional issues with cloud, and noted interestingly that he had read that many people were not very happy with the EU-US safe harbour principles for getting around data protection laws whilst storing data in the US. And therefore companies were looking at other ways to ensure their data was safe when it was moved outside the EEA.</td></tr>
<tr><td>Question 4.</td><td>Do you think cloud vendors are violating the DPD principles?</td></tr>
<tr><td colspan="2">Answer 4. Again here Candidate3 pointed out that the client of the cloud vendor is the data controller, so it was their responsibility to make sure there was no breach of DPD principles once the data went into the cloud. He said cloud vendors will issue contracts where they try to completely indemnify themselves against any responsibility for the data. He said if organisations are signing these contracts then tough luck, client is responsible. So in short, no, he didn’t believe cloud vendors were violating DPD principles, but if they were it was their client’s fault/responsibility!</td></tr>
<tr><td>Question 5.</td><td>Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?</td></tr>
<tr><td colspan="2">Answer 5. Probably similar answer to question 3, clients are more aware of the Irish data protection acts 2003, 1988 more so than the European directive. And clients are certainly asking cloud vendors about data protection, but clients understand their role as the data controller.</td></tr>
</table>

<table>
<tr><td>Question 6.</td><td>Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?</td></tr>
<tr><td colspan="2">Answer 6. Candidate3 said he thought certain data was perfect for the cloud. Dail debates, planning applications, supreme court decisions, certain types of data registers, generally information that is intended to be in the public domain anyway, so no harm and more convenient for it to be in a cloud environment.
He said that is not to say he didn’t believe sensitive data could be put in the cloud. He said the sensitivity of the data would determine the level of upfront risk analysis that would have to be completed prior to that data being moved to the cloud environment. He said if the risk is eliminated he saw no reason why the data could not be moved into the cloud. Once proper precautions were taken anything could be moved to the cloud.</td></tr>
<tr><td>Question 7.</td><td>What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?</td></tr>
<tr><td colspan="2">Answer 7. Candidate3 said some cloud vendors are huge, Amazon for example, and they know they can get away with these types of contracts, so that’s why they issue them like this. They feel so what; if a customer doesn’t like it, let them move on, the next customer will sign up. He also said these contracts may depend on the negotiating power of the parties involved. If the client is huge, and the costs involved are huge, then the cloud vendors may move to accommodate more responsibility. He said the only way to ameliorate some of the ‘funny terms [sic]’ within the contracts was to have clauses inserted specifically saying what must happen in certain circumstances, i.e. if the vendor goes bust and you need your data back, if you go bust and your clients need their data returned, that you need access to your data within a reasonable time etc., he said if you can’t build these terms in, and you sign a contract for service without them in, then hard luck.
He did mention though that he did believe a limitation on the jurisdictions your data would be liable to be moved to was becoming the norm in these contracts, so that was one less ‘funny’ clause.</td></tr>
<tr><td>Question 8.</td><td>If Irish government in the morning said they were putting a particular department’s data in the cloud, what would you think?, would it depend on the dept. in Question?</td></tr>
<tr><td colspan="2">Answer 8. Candidate3 agreed that this would depend on the department in question, and perhaps we had covered a lot of this in question 6 about what data types you could put into the cloud. He mentioned that the State Solicitor’s office had mooted a year or 2 ago that government should not touch cloud, but that they had had to row back a little on that, when it was explained that the government were attempting to encourage adoption of cloud as a way to incentivise inward investment (into Ireland) from cloud companies. He said perhaps private cloud would be perfect for departments working with medical records etc., and this would be a safer way for governments to still be in with the cloud mantra, but eliminating some of the risk that would go with public cloud.</td></tr>
<tr><td>Question 9.</td><td>Does the judiciary have the skills or how much do they need to understand about cloud computing to apply the law correctly.</td></tr>
<tr><td colspan="2">Answer 10. Candidate3 said that the judiciary don’t need to have the skills. He said they will bring in IT experts to explain the technology, he then said the judiciary would apply the law as the law stands, i.e. it didn’t matter what the technology was, if it was deemed to be braking a law then it would be dealt with accordingly.</td></tr>
<tr><td>Question 11.</td><td>Have you heard of this Geolocation technology, do you think it could help allay client’s fears if they had definitive knowledge of the whereabouts of their data?</td></tr>
<tr><td colspan="2">Answer 11. Candidate3 hadn’t heard of this type of technology, but certainly thought it would be a great idea if something like this was in place, say as a piece of software installed by the cloud vendor in order to ensure your data stayed where they said it would. He said you could build this into the contract, i.e. I’m signing up, once you install this piece of software on the database where my data is. Candidate3 also believed the other artefact proposed by the dissertation, a tool whereby clients could assess the risk before</td></tr>
</table>

<table>
<tr><td colspan="2">adopting cloud would be an excellent tool.

One interesting point made was that under the data protection laws, if a piece of technology (reasonably priced) was available in the market to provide a certain level of security, then companies storing data were obliged to be using that technology to protect the data, i.e. the vendor couldn't claim ignorance that a particular piece of software wasn't on the market that could solve the security hole. He said if my proposed piece of software ever made it to market, then cloud vendors may be obliged to use it.</td></tr>
<tr><td>Question 12.</td><td>Should my focus be directed in another area/should I be doing anything different?</td></tr>
<tr><td colspan="2">Answer 12. No, candidate3 thought I was in the exact area I needed to be, and couldn't suggest me doing anything differently. He said he had gotten most of his cloud knowledge from a conference put on by IBEC last year, and by Google searches, so he said the material I had found was certainly as good as anything he had come across.

Candidate3 did say though that I should be looking at the Data Commissioner's website as there was lots of interesting cases there and great general guidance in terms of data protection.</td></tr>
</table>

<table>
<tr><td>Interview No.</td><td>4</td></tr>
<tr><td>Date</td><td>19-APR-2012</td></tr>
<tr><td>Institution</td><td>William Fry</td></tr>
<tr><td>Individual</td><td>Candidate4, Partner, accompanied by a trainee solicitor</td></tr>
<tr><td>Comments</td><td>Busy café at lunchtime on Baggot Street, recording not an option (giving up on recordings!). Candidate4 very happy to assist in the dissertation process and very eager to look at any documents/artefacts that comes out of the process. Will gladly give feedback, email if I have any further questions etc. Gave me a handout from William fry detailing the 10 top legal issues relevant to cloud that they as a law firm have come across.</td></tr>
<tr><td>Question 1.</td><td>I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?</td></tr>
<tr><td colspan="2">Answer 1. Candidate4 believes Cloud is utility computing, like the ESB or Bord Gais, he said it will mean different things to different people depending on the circumstance. He said it's accessing computer resources anywhere, anytime any place…. I.e. a global distribution. He said some vendors will not have gone as far with their cloud services, i.e. making them freely available all over the globe, for example a private cloud, but it can still be cloud in his opinion if it using underlying cloud technologies.</td></tr>
<tr><td>Question 2.</td><td>How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?</td></tr>
<tr><td colspan="2">Answer 2. Candidate4 believes cloud is being considered by Irish business, but that there is a lot of caution out there. Caution because the technology is new, he said nobody will get fired for using existing 'safe' technology, but that some businesses were somewhat obliged to look at it because of the promise of cost savings. He said it can be seen as a brave decision to move to the cloud. Organisations want to know if this is something their organisations can find a use for. Organisations are looking at it too because they don't want to be left behind. He said it is more attractive to small and medium sized businesses where the risk would not be so great, they may have less to lose, so there is less risk involved. But for larger organisations with critical business systems cloud is seen as a little more risky. He said some companies like that are looking at hybrid clouds.</td></tr>
<tr><td>Question 3.</td><td>I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?</td></tr>
</table>

<table>
<tr><td colspan="2">Answer 3. Candidate4 said there was a list of about 10 in the handout he gave me, but the big ones he sees are Security, and there are 2 aspects to security, 1, making sure the data was not accessible to others (he gave the recent breach of credit card details at SONY), and 2, that there was security of supply, if you are dealing with critical systems, there can be requirements that those systems don't go down.
Data Protection was also another area right at the top of the legal issues. He said to get the full advantages of cloud, vendors and clients alike might want to allow data to be moved around jurisdictions, for example, if in the morning there is available space in Singapore, use those servers to burst into, if in the afternoon it makes more resource sense to use servers in America use those. But he said DP laws might prevent the cloud from being used like this. Perhaps DP issues are preventing people from getting the full efficiencies from cloud. So he said it's maybe up to IT to make sure we can benefit from the bulk of efficiencies that cloud affords without breaking any DP rules, for example IT would ensure the data stays in Europe. He said this is a balance, ensuring you get the full benefit from cloud advantages without crossing the legal boundaries.</td></tr>
<tr><td>Question 4.</td><td>Do you think cloud vendors are violating the DPD principles?</td></tr>
<tr><td colspan="2">Answer 4. Candidate4 does not believe they are not breaking these rules intentionally, but he would be surprised if they were not breaking them to some degree. He said some of these cloud vendors are only beginning to start to get their heads round the legal implications of what the technology is doing. He said the legal side of data protection is extremely complicated. He said a lot of the DP issues stem from the level of understanding reached between users and vendors concerning the control users will have over their data once it is in the cloud.</td></tr>
<tr><td>Question 5.</td><td>Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?</td></tr>
<tr><td colspan="2">Answer 5. Candidate4 believes cloud clients are becoming more aware of DP issues, he said there is an increased level of engagement between people and the DP office (Commissioner's office) to find practical issues to problems brought about by new technologies. He said I must remember that all the existing DP laws in Ireland were drafted before cloud came along, so there is an element of trying to understand how new technology affects DP issues and vice versa.</td></tr>
<tr><td>Question 6.</td><td>DP - Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?/ 6B sectors not suitable for cloud</td></tr>
<tr><td colspan="2">Answer 6. Candidate4 believes all data types can be stored in the cloud. He believes cloud can be safer than a normal company's environment where the security expertise may not be as good as it should be. He said in theory cloud data centers should be employing the best security people and ensuring those security people are kept up to date with the latest and best security equipment. If you like, cloud data centers should be a security center of excellence. He said normal companies can't go the nth degree from a security perspective, but cloud vendors can, because that's their business.
Likewise with sectors Candidate4 believes all sectors can move to the cloud. For the same reasons given in part 1 to this question. He said obviously the level of risk analysis that needed to be done would be higher for more sensitive data types, but he saw no reason why everything could not be put into a cloud environment.</td></tr>
<tr><td>Question 7.</td><td>Abdication of Liability/Contract Issues
What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?</td></tr>
<tr><td colspan="2">Answer 7. Candidate4 said in reality a lot of people don't read terms and conditions, for example we all use Gmail, it is a cloud service, he asked if I had read the terms and conditions for Gmail. He said if the service is not critical to a business people won't even bother with the TOCs. They will just click yes. He said this space is evolving though, there is a middle ground emerging where clients looking to move more</td></tr>
</table>

<table>
<tr><td colspan="2">critical systems into the cloud environment are getting the ability to have TOCs amended, and that these users wouldn't obviously accept the normal TOCs on offer. He said it is very much down to what you pay for the service. He quoted an example of a professional photographer in America who sued Flickr because the hosting site deleted his photographs by mistake. The photographer was unable to retrieve the images and sued Flickr for loss of earnings. Candidate4 said he would send on details of this case, but he believes the photographer lost his case based on the fact that he was only paying $15 a month for the Flickr service. And Flickr losing his data didn't mean they were obliged to pay for loss of earnings, more likely they were obliged to give him his last month's subscription money back! So therefore the argument is you get what you pay for. He said he had heard of clients paying more for a higher level of commitment on behalf of the vendors, but this costs money. If you want a more tailored service you need to pay for it.</td></tr>
<tr><td>Question 7b.</td><td>Do you believe the cloud has made IP violations a bigger problem?</td></tr>
<tr><td colspan="2">Answer 7b. Candidate4 does believe cloud is contributing to IP being a bigger issue. He said obviously cloud is making more intellect property available to more and more users, so obviously the problems with IP will increase. It is easier now to distribute content…. People have more access to copyrighted material. He said record and film companies are approaching this in 2 ways, some are keeping up the old method of releasing their films/music jurisdiction by jurisdiction, they release something in America in January and then release it in Ireland in May. But he said by May, 10000 people in Ireland will already have seen/ heard it because they have downloaded the material illegally off the web, the other approach is where entertainment companies are trying to come up with business models whereby the product is released in one go, and people all over the world have an opportunity to access that product from 1 location for a fee. He said moving to this model is a huge challenge, but he sees no other alternative for these businesses. He said the old methods of distribution are not sustainable. He believes SOPA/PIPA and ACTA (Anti-Counterfeiting Trade Agreement) have died a death because of public outcry, so entertainment companies need to rethink their business models in light of web and cloud technologies.</td></tr>
<tr><td>Question 7c.</td><td>Jurisdiction - Again are clients aware of these issues in regard to cloud computing?</td></tr>
<tr><td colspan="2">Answer 7c. Candidate4 believes jurisdiction issues really arise when the business have a presence in the country where the legal action arises. I.e. if your data moves to India, and that cloud vendor has some level of office in India (they are using a sub-cloud provider for data center in India) then the vendor can be in trouble if there is a data breach. That local office is subject to local law enforcement. He believes if data is just in transit in a particular country where it is not supposed to be he doesn't believe it is such a big issue. However he is aware there is an issue in Germany surrounding the transfer of certain data outside the country, so he said all countries are not the same. He said the whole issue of the things like the patriot act are 'cloud neutral', i.e. they apply to faxes, emails etc. too, so those kind of legal instruments are not cloud specific, so he doesn't see them as huge issue to cloud computing.</td></tr>
<tr><td>Question 8.</td><td>If Irish government in the morning said they were putting a particular department's data in the cloud, what would you think?, would it depend on the dept. in Question?</td></tr>
<tr><td colspan="2">Answer 8. Believes this was answered earlier in question 6 re. Data types and sectors. He'd be fine if the Irish government was moving data into the cloud, once the appropriate security controls were in place.</td></tr>
<tr><td>Question 9.</td><td>Does the judiciary have the skills or how much do they need to understand about cloud computing to apply the law correctly.</td></tr>
<tr><td colspan="2">Answer 9. Candidate4 believes the judiciary don't need to have these skills. He said the barristers do. He said some barristers will be experts in technical matters; some will be experts in banking etc., so if his firm need somebody to argue a cloud case they will call on a barrister with that experience, it is up to the barrister then to explain the intricacies to the judge. But he said it will come down to a matter of law (a determination in law) with the judge, it won't be a technology decision the judge will have to make. He said barristers and judges will follow commercial trends, and if there are new technologies involved, expert counsel will adapt their general understanding to the new area.</td></tr>
<tr><td>Question 10.</td><td>Have you heard of this Geolocation technology, do you think it could help allay client's fears if they had definitive knowledge of the whereabouts of their data?</td></tr>
<tr><td colspan="2">Answer 10. Candidate4 liked the idea and said it does have merit, but said this sounds like a part solution. He said this problem is not just down to knowing where the data is or if it has been moved. He said he</td></tr>
</table>

<table>
<tr><td colspan="2">would like to see this go a step further though, whereby the software/technical solution produced could stop the data being transferred and not just alert users if it is being moved. Version 1.1. maybe ! Version 1.0 is fine from an audit perspective, but maybe not going far enough.
As for the artefact whereby we provide a would be cloud adopted with a serious of questions, then presenting them with a list of things they should be doing before they sign up for the service … he said this is good too, but that I would need to make sure this information was accurate (and not out of date). If it wasn't I could be sued!!</td></tr>
<tr><td>Question 11.</td><td>Should my focus be directed in another area/should I be doing anything different? – what stuff should I be reading ;</td></tr>
<tr><td colspan="2">Answer 11. Candidate4 believed my focus was very good, I'm hitting all the hot topics, he believed the information from the Queen Mary University in London was excellent and this was definitely the stuff I should be reading, he had not heard of JISC. He suggested I look at LinkedIn, there are a lot of cloud user groups there sharing a lot of useful information.</td></tr>
</table>

<table>
<tr><td>Interview No.</td><td>5</td></tr>
<tr><td>Date</td><td>20-APR-2012</td></tr>
<tr><td>Institution</td><td>Technology Consulting Firm, Dublin</td></tr>
<tr><td>Individual</td><td>Candidate5, Technical Director</td></tr>
<tr><td>Comments</td><td>I explained that most of the questions would have a legal slant, and that if Candidate5 didn't have a view or have knowledge of a certain legal issue that was fine, explained that I just wanted to have some impression of what legal issues (if any) technical experts believed existed within the legal landscape of cloud. Candidate5 was very happy to review any artefact I send him, can call/email him too if I have further questions.</td></tr>
<tr><td>Question 1.</td><td>I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?</td></tr>
<tr><td colspan="2">Answer 1. Candidate5 believes what differentiates cloud is flexibility; the fact that you can access cloud services anywhere, anytime etc. Elasticity too was another differentiating factor, the fact that retailers could use cloud services to 'burst' into the cloud when there are times of high sales, then retreat back out of the cloud when sales are leaner, these kind of things define cloud. Candidate5 believes cloud has paved the way for business models which couldn't have existed without cloud. Cloud too also introduces a certain element of cost reduction.</td></tr>
<tr><td>Question 2.</td><td>How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?</td></tr>
<tr><td colspan="2">Answer 2. Candidate5 believes businesses are interested, particularly start-ups who view cloud as a cheap way to got an IT infrastructure up and running quickly, some of these companies get themselves burnt because they don't understand the full implications of having an IT infrastructure that is not completely within their control. The big issue in regard to cloud adoption is the technological maturity of an organisation. Some organisations don't have the maturity/know how/expertise/professionalism to understand or contemplate what additional benefits can be accomplished through IT. IT in the past was seen as a siloed area of the business, draining costs. There is still a certain level of this thinking within Irish organisations, not understanding that IT can drive a business forward. Also IT departments in organisations are scared of cloud, they believe it has the possibility to make them redundant. This has even made some IT people to ignore using cloud type technologies. The thinking is, if I use virtualisation for some of the systems here, what's to stop management from moving the whole infrastructure into a virtualised environment in the cloud? So IT guys are scared, to sell cloud you need to go above their</td></tr>
</table>

<table>
<tr><td colspan="2">heads, but then you hit the maturity/ignorance problem. So yes businesses are interested, but many organisations are too immature to understand the benefits that could come from cloud, and are too slow to adapt to these new possibilities. There isn't the necessary close alignment between IT and the business allowing for fast agility and take up of new IT concepts. Candidate5 suggests I look at the IVI (Innovation Value Institute) in Maynooth who have done some work on maturity models for managing business capabilities through IT; *http://ivi.nuim.ie/itcmf.shtml*
VMware have done some good work in this area too, they call their model ATA, Accelerate Transformation Assessment, and there is a good article on their stuff here;
http://blogs.vmware.com/files/vmw-wp-accelerate-trans-assmnt-scale-uslet-103-web.pdf
Very interestingly Candidate5 believes the public cloud is dead in the water for a couple of years at least. More businesses are looking at private clouds, perhaps as a test bed, if I can't run my business in a private cloud environment, then what chance do I have running it in a public one. Public cloud is just a little too far beyond people's comfort zone.
But yes, interest is growing organically, potentially through 'Shadow IT', people within the organisation who bypass the IT department and sign up for cloud services to help manage a particular task within their own department, availing of things like dropbox/some basic Amazon services etc.</td></tr>
<tr><td>Question 3.</td><td>I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?</td></tr>
<tr><td colspan="2">Answer 3. Candidate5 is aware of some legal issues, data protection being the most predominant one, and Candidate5 finds they he is often the one bringing it to the attention of organisations when he is going in to consult on a cloud service. In many cases the IT department won't be aware of the legal implications, so he is obliged to bring them up. He said there are many mixed messages doing the rounds about cloud, so sometimes it is difficult to get the full, coherent picture. The basic premise though seems to be that once the data is in Europe, then you are covered from a data protection perspective.
Candidate5 is doing a lot of work with the hospitals. He finds that they have huge quantities of data that they just can't afford to keep on-site and back up continually. So hospitals are looking at putting this data into the cloud. They appear to be happy with this decision once they are assured the data is staying in the E.U. and it is encrypted. He said hypothetically what can happen is IT engage with the cloud provider and data is moved, the systems are in place and are up and running, he comes in and advises on the legal implications a little later, management get word of potential legal concerns, they write off to minister Reilly, he's too busy, and the letter sits under a pile of other letters on his desk .... the process continues.</td></tr>
<tr><td>Question 4.</td><td>Do you think cloud vendors are violating the DPD principles?</td></tr>
<tr><td colspan="2">Answer 4. Candidate5 believes cloud vendors are not intentionally violating the DPD principles, but there have definitely been incidents. Microsoft had a problem with their Azure platform some time ago, where a user had asked for and was promised that replication of their data to a non EU jurisdiction was being turned off, but it transpired that Microsoft had a technical problem and couldn't switch the replication off. I don't think the likes of this thing would happen with a provider called Nirvanix, *www.nirvanix.com* are a leading cloud provider who consult with clients on tailoring a service to suit their particular needs. Colt, *http://www.colt.net* is another cloud vendor offering tailored services. With Colt you can choose the destination up front where you want your data to go or not to go. They currently advertise a public cloud offering where a selling point is that the data will not leave the EEA (Even though they are a U.S. company, or owned by one, they understand clients want their data to remain in the E.U.).</td></tr>
<tr><td>Question 5.</td><td>Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?</td></tr>
<tr><td colspan="2">Answer 5. Probably covered earlier, in many circumstances Candidate5 is bringing up legal issues with clients, larger organisations are aware of the DPD and the Irish data protection acts, where there is a decent HR or legal department. Many smaller companies, SMEs don't fully appreciate the legal implications and in many circumstances go with the cheapest cloud provider, not fully understanding the impacts of problems which may arise if such a vendor for example goes bust, and they have difficulty getting</td></tr>
</table>

<table>
<tr><td colspan="2">customer data back.</td></tr>
<tr><td>Question 6.</td><td>Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?</td></tr>
<tr><td colspan="2">Answer 6. Technically, obviously there are no reasons why any type of data can't be stored in the cloud. Sectors too obviously. Candidate5 believes once you are with a reputable vendor, there are proper security safeguards in place etc., the data is encrypted to a recognised standard, no reason why any type of data cannot be stored in the cloud.</td></tr>
<tr><td>Question 7.</td><td>Jurisdiction seems to be an issue with data protection, what are your thoughts on this.</td></tr>
<tr><td colspan="2">Question 7. As mentioned earlier, vendors like Colt are offering up front the possibility to choose where you would like to put your data, and they and others offer an EEA only service, so some of the jurisdictional issues are being addressed. There are however a lot of mixed messages in the market place though, for example Billy Hawkes might come along and say it's fine once your data is in the E.U., but then each jurisdiction within Europe have adopted the European directive slightly differently. A lot of people are talking about using Germany as the place for storing data as it is seen as the lowest common denominator in terms of data protection law, France on the other hand is a jurisdiction where it is supposedly very difficult to get data out of, once it is has been transferred to a data center there, so jurisdiction is still not totally straight forward. It is difficult sometimes to find a conclusive answer regarding this area.</td></tr>
<tr><td>Question 8.</td><td>What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?</td></tr>
<tr><td colspan="2">Answer 8. Again this is in part down to a maturity thing, the technological maturity of the business and the cloud vendor. For a generic service like gmail and dropbox, others where 10Gbs of storage space is going to made available at $9.99 a month, there is never going to be any come back, it's a case of you get what you pay for. In these types of offerings the vendors have no capability to understand your business, they are giving you an off-the-shelf 100 dollar a month service, if they lose your data or the service is down for a day or 2, then it's your tough luck unfortunately. Amazon will abdicate everything, go with a crowd like Nirvanix or Colt (who offer Enterprise class clouds), and then you can completely tailor the level of service you get, whether particular storage of processing power is ring fenced for you. These vendors will even take some responsibility if something goes wrong! all this will come at a premium cost though.</td></tr>
<tr><td>Question 9.</td><td>Do you thing Cloud has contributed to an increase in Intellectual Property Violations.</td></tr>
<tr><td colspan="2">Answer 9. Candidate5 wasn't aware that cloud had made IP issues any greater, but from his perspective cloud had presented some issues in regard to his intellectual property, ownership of clients; Candidate5 cited the example where his company will re-sell a cloud service, then the client will put their information in the cloud, what's to stop the cloud vendor accessing that information and contacting the client directly, in that situation who now owns the client?, so this is a worry.</td></tr>
<tr><td>Question 10.</td><td>If Irish government in the morning said they were putting a particular department's data in the cloud, what would you think?, would it depend on the dept. in Question?</td></tr>
<tr><td colspan="2">Answer 10. Candidate5 said this is down to one thing and one thing only, who is the cloud vendor! If it's some cloud vendors, where their cloud service is held together with string he'd be really scared, if it's a more reputable vendor who he is familiar with then there is no problem.</td></tr>
<tr><td>Question 11.</td><td>What are the main technical issues with cloud implementations? Have you seen any issues with things such as vendor lock-in? Getting data back out if a provider goes bust?</td></tr>
</table>

Answer 11. The main technical issues are really related to that whole maturity thing I talked about earlier, some people hear cloud and want to be on board, but they don't have the need for it, or the business model or processes in place to take advantage of it. Candidate5 has seen issues with vendor lock-in; Azure is notoriously difficult to get your data back from. There doesn't seem to be any agreed standard or policy for retrieving data from a cloud vendor, Candidate5 hasn't seen one. There is also an issue where the cloud vendor you have signed up to has other layers of the service contracted to third parties, if a third party is ultimately holding the data and your vendor goes bust, how do you get your data back? For some of these reasons Candidate5 has seen the focus shift back to private cloud.

On vendor lock-in, large vendors (particularly PaaS ones) are able to offer huge storage space at knock down prices, economies of scale etc., so this is driving smaller vendors out of business, there is more likelihood of vendor lock-in if there are limited numbers of vendors in the market place.

Question 12. Have you heard of this Geolocation technology, do you think it could help allay client's fears if they had definitive knowledge of the whereabouts of their data?

Answer 12. Candidate5 has heard a lot about geolocation. Advised me to look at the Intel site, as Intel are doing a lot of work in this area, building geolocation technology into their chips. Another crowd to look at who do similar things is a crowd called packetmotion. Intel are building this into the chips, so the operating system and applications running on the OS have access to the geotag information, then cloud technology, vmware, whatever, can access this information, and depending on how the system is set up can decide not to function if the information coming from the chip doesn't match where it's supposed to be running.

This is maybe 12 months away, but it is coming.

On the website/integrated framework/guide for users. Candidate5 said that there is a vested interest in this whole area being a little opaque. He said he is familiar with come cost models available on the web, but wasn't aware of legal ones, he said it will be tricky to make this information generic. Candidate5 comes from a SAP background, where SAP offered the business the panacea of a generic suite of applications, capable of fitting into any organisation's business model. But then when people adopted SAP, they wanted it all changed and modified. The same is true for cloud, every organisation will want it tailored to work with their organisation a little differently, so not sure about offering generic guidelines, particularly from a legal perspective? Perhaps a knowledgebase would be good, to dispel some of the peculiar dynamics of cloud.

Question 13. Should my focus be directed in another area/should I be doing anything different?

Answer 13. Candidate5 suggested looking at the whole area of data leakage, or PCI DSS (The Payment Card Industry Data Security Standard), where there is work going on involving trawling through reams of an organisation's data and making sure it is where it is meant to be.

Also data access points for cloud will be big in the future, you can access cloud from so many devices, so controlling the whole authentication and authorisation to access particular sets and types of data will be big; who, on what device, from where. I.e. maybe look at the geo-tag information of the accessing device, if it is outside a preconfigured list, don't let it access the data? that kind of thing might be worth a look.

Question 14. Where should I be looking at for more information?

Answer 14. VMware website is good, particularly for IaaS, look at a crowd called the cloud foundry (http://www.cloudfoundry.com/); they are doing good stuff on PaaS. Nirvanix have some good stuff on Infrastructure.

Interview No.	6
Date	30-APR-2012

<table>
<tr><td>Institution</td><td>IT Infrastructure and Services Company, Dublin</td></tr>
<tr><td>Individual</td><td>Candidate6, Operations Director</td></tr>
<tr><td>Comments</td><td>I explained that most of the questions would have a legal slant, and that if Candidate6 didn’t have a view or have knowledge of a certain legal issue that was fine, explained that I just wanted to have some impression of what legal issues (if any) technical experts believed existed within the legal landscape of cloud. Candidate6 was very happy to review any artefact I send her, can call/email her too if I have further questions.</td></tr>
<tr><td>Question 1.</td><td>I have read many definitions of what cloud computing is, what in your opinion defines cloud computing, and indeed makes it any different to grid computing/storing data on rented server space?</td></tr>
<tr><td colspan="2">Answer 1. Candidate6 believes that cloud computing is an offering that allows users and companies to pay for raw resource and software services as they use them. It is particularly well suited to companies that have a peak of requirement during a particular time of the year such as bookmakers etc who need spikes of resource during high profile race festivals etc. She believes cloud has gained momentum as a concept and technology offering due to the widespread adoption by users in their private lives. Users are using cloud offerings like gmail etc in their everyday lives so are pushing IT groups to provide that kind of flexibility and agility in the company environment. Cloud is seen as allowing companies to just pay as they go for resource used giving it the perception of being cheaper than renting and is seen as being less complex than the idea of grid computing. Companies are also enthused by the idea of getting back to their core business instead of taking on the running of complex IT environments that have little to do with their real business.</td></tr>
<tr><td>Question 2.</td><td>How do you think the whole concept of cloud computing is being considered by Irish businesses, are they excited about it, do they want to get on board, are they cautious? If cautious – Why?</td></tr>
<tr><td colspan="2">Answer 2. Candidate6 believes that almost all businesses are talking about cloud but few have a real understanding of what is involved in truly being ready to take their core applications into the cloud and equally few would consider putting their core applications into the cloud due to the perceived risk in areas like data protection, secure backups and communications costs. Many businesses are currently engaging consulting firms to prepare “cloud readiness” studies for two reasons, firstly to show they can “tick the box” that they have looked at cloud as everyone else is and secondly to get an understanding of what really is involved in adopting cloud technologies and gaining a view of any potential cost savings or other advantages of adopting the technology.
Many companies are interested about cloud and what it can offer them at the business level as the perception is that cloud will allow businesses the agility that they want and a speed to deployment of new applications but there is a lot of scepticism within the IT departments. She has seen a few companies aggressively implement “private clouds” where they became the cloud provider internally to their business. This middle ground has proved a good compromise as the IT groups don’t feel under threat and the business gets the agility they crave. Implementing a private cloud changes the dynamic between IT and the rest of the business as the business gets used to the concept of paying for the resource they use and IT becomes a revenue generator as opposed to a cost drain. The adoption of private clouds means that companies feel like they are getting some of the benefits of the cloud while not taking on the risk they perceive they would encounter by using the public cloud.
For smaller departmental needs she has seen individuals in the businesses subscribing to specific cloud services like Sharepoint for individual projects without the knowledge of either the rest of the business or the IT department, this is a risk that companies fear as it means that sensitive company information is being stored out in the cloud without due diligence taking place on the offering or provider to ensure that the information is being stored and protected to the level required.</td></tr>
<tr><td>Question 3.</td><td>I have identified some legal issues associated with cloud computing, before I talk about them, can you please let me know if you are aware of any?</td></tr>
<tr><td colspan="2">Answer 3. Candidate6 indicated that stories such as wikileaks and the ability of the US government to go</td></tr>
</table>

<table>
<tr><td colspan="2">to the cloud provider and demand access to the data and also the incident of customers of Amazon having no recourse on the provider even though the cloud service was offline for a period of time were the only real life experiences that she was aware of. She did have concerns over cloud contracts as her impression was that there was no recourse by the customer if the cloud service was offline for any period of time other than a maximum reimbursement of the fee paid by the customer for the service. If a customer is running their core business from the cloud then this could be catastrophic if the service was offline for a period of time. That is a huge risk in cloud adoption for core applications. Another perceived issue candidate6 had was if a company moved from one cloud provider to another she was not confident that the company's data would be properly removed and deleted from the first provider.</td></tr>
<tr><td>Question 4.</td><td>Do you think cloud vendors are violating the DPD principles?</td></tr>
<tr><td colspan="2">Answer 4. Candidate6 believes it is entirely down to the maturity of the cloud provider. Many companies will assume that all cloud providers adhere to a very high standard and provide all their services under a best practice, but in reality that is not always the case and in most cases even cloud offerings are only as good as the people who implement them. Vendors may not be aware that they are violating the DPD principles but it can just be down to a simple mistake in implementation of a company's environment that would cause it to be in breach of the DPD principles.</td></tr>
<tr><td>Question 5.</td><td>Do you believe cloud clients are aware of the DPD, and if their data is being managed in accordance with the DPD principles?</td></tr>
<tr><td colspan="2">Answer 5. It depends on whom you are talking to within the organisation. In most cases the business owner is aware of the DPD but IT may be less so. This also becomes especially tricky in the cases where departments are taking on cloud contracts for a specific service as mentioned earlier such as sharepoint. These are the incidents where DPD principles are not always considered.</td></tr>
<tr><td>Question 6.</td><td>Have you a view on whether all data types can be stored/should be stored in a cloud environment? I.e. do you believe some data types are not suitable for the cloud?</td></tr>
<tr><td colspan="2">Answer 6. Candidate6 is not aware of any particular data type but she would doubt that certain applications are candidates to go into the cloud i.e. Some intensive financial or insurance applications which are written for bespoke or specific technology platforms such as IBM iSeries or mainframes would need such a large amount of the application to be rewritten to make it portable to general cloud platforms that it would not make sense to consider them for migration to cloud.</td></tr>
<tr><td>Question 7.</td><td>Jurisdiction seems to be an issue with data protection, what are your thoughts on this.</td></tr>
<tr><td colspan="2">Question 7. Very few cloud providers if any seem to offer the option of keeping the data on island in Ireland so inevitably jurisdiction becomes an immediate issue when adopting cloud because as a minimum a company needs to consider the implication of the data going to an EU country. It is a complicated issue as each country even within the EU seems to have different laws surrounding how data is handled. It makes cloud adoption complicated as it is no longer a business decision or an IT decision, suddenly businesses need to have legal input of which many have no in house expertise so it's seen as a very costly and unknown element of a solution and can be a big barrier to considering cloud.</td></tr>
<tr><td>Question 8.</td><td>What do you think of these terms (abdication of liability)?, are clients willing to accept these and why are these terms so different to other IT contracts for services, such as signing up to an ISP, whose TOCs you would believe are not so onerous on clients ? Where is the fair play, can clients pay more up front so the vendor assumes more liability?</td></tr>
<tr><td colspan="2">Answer 8. It depends on the type of cloud adopted by the enterprise. With public cloud the terms of conditions are what they are and you accept that and pay the low rate that goes with that. If you want specific terms or increased liability ownership by the cloud vendor then you need to go with a more bespoke cloud offering but this inevitably will come with increased cost. The cloud offering that offers private users to put up their private photo collection will not necessarily be the correct cloud offering for a financial company to store their customer information on, they are entirely two different sets of</td></tr>
</table>

<table>
<tr><td colspan="2">requirements so they would not require the same solution, so companies should remember that cost should only be one consideration when choosing a cloud provider.</td></tr>
<tr><td>Question 9.</td><td>Do you thing Cloud has contributed to an increase in Intellectual Property Violations.</td></tr>
<tr><td colspan="2">Answer 9. It hasn’t been one of the biggest consideration of her company or her company’s customers as the environments where cloud solutions are being adopted tend to be standard applications, if they were involved in more deployments where software and application development was taking place in the cloud it might be more of a consideration in those cases in relation to ownership of the IP developed. In general data security so that cloud providers did not have access to any customer information is always a consideration.</td></tr>
<tr><td>Question 10.</td><td>If Irish government in the morning said they were putting a particular department’s data in the cloud, what would you think?, would it depend on the dept. in Question?</td></tr>
<tr><td colspan="2">Answer 10. Candidate6 would still have reservations about core applications being put in a public cloud irrespective of which department they belong to, She would have no problem with general less critical applications being put into the cloud as long as the decision criteria when selecting the cloud vender was not based on price but instead of the level of service being delivered to the department.</td></tr>
<tr><td>Question 11.</td><td>What are the main technical issues with cloud implementations? Have you seen any issues with things such as vendor lock-in? Getting data back out if a provider goes bust?</td></tr>
<tr><td colspan="2">Answer 11. The main issues identified by Candidate6 were firstly companies understanding the communication requirements for any non web based application they want hosted by a cloud provider (and the resulting costs!), and secondly the risk associated with any future migrations between cloud providers for applications/data or with trying to get an application/data back out of the cloud to host in house again. The maturity of the cloud providers has not been tested to know if those migrations will be achievable or whether customers will find themselves completely locked in once they adopt a cloud offering. She would also question whether any of the cloud vendors would be in a position to successfully migrate any non Microsoft/Linux OS based application into the cloud.</td></tr>
<tr><td>Question 12.</td><td>Have you heard of this Geolocation technology, do you think it could help allay client’s fears if they had definitive knowledge of the whereabouts of their data?</td></tr>
<tr><td colspan="2">Answer 12. Candidate6 had heard of this technology. She told me to look at work Intel and VMware were doing, particularly at a product called Intel TXT (Trusted Execution Technology). Apparently Intel have done work building geolocation technology into their chips, on top of this they have a stack that can talk to the hypervisor layer (the VMware layer), and you can configure Intel TXT to only launch the VMware components if the geolocation information coming from the chip match the geolocation information in a preconfigured registry.</td></tr>
<tr><td>Question 13.</td><td>Should my focus be directed in another area/should I be doing anything different?</td></tr>
<tr><td colspan="2">Answer 13. Candidate6 mentioned there are tonnes of areas in relation to cloud that I could look at but wondered how much time I had!, She mentioned IBM are doing a lot of work with the cloud and green IT, Six Sigma. Advised to check out their websites for more information, if I wanted to stick with the geolocation stuff definitely look at the Intel TXT stuff... She also noted that the Intel TXT was a promising solution for Intel based applications, but wasn’t sure if the same could be said for mainframe, e.g. not sure if IBM are doing anything similar with their chips and the AIX OS.</td></tr>
<tr><td>Question 14.</td><td>Where should I be looking at for more information?</td></tr>
<tr><td colspan="2">Answer 14. IBM, VMware, Cisco, Intel and Microsoft are the main vendors that Candidate6 gets her information from, advised to look at their websites for white papers, online demos etc.</td></tr>
</table>