DRAFTING A CLOUD COMPUTING CONTRACT

University of Oslo

Faculty of Law

Candidate number: 8024

Submission deadline: 1 December 2011

Word count: 17.924 (Max. 18.000)

25.11.2011

Table of contents

1 Introduction

1.1 Background

According to the US National Institute of Standards and Technology (NIST), Cloud computing is "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service-provider interaction*."[1] Cloud computing services are delivered by cloud providers who use resources such as: networks, servers, storage and applications which are available inside the internet (cloud). The special characteristic of cloud computing is the ability to deliver IT resources without depending on the particular Information Technology (IT) components in the physical world. Therefore the on-site installations of IT hardware and software no longer become the basic requirement to offer the services. Application of this method means that rather than installing and maintaining data/software on a defined network or desktop computer, the data/application is hosted on a number of computers in the cloud and available on demand.[2] From the commercial view point, utilizing the cloud will allow companies to take advantage of the best and latest technology since they will not have to disassemble and rebuild their entire IT infrastructure in order to upgrade.[3]

Before cloud computing was introduced, all the typical known services utilizing the cloud were already offered but through a separate model of business such as hosting contracts, outsourcing contracts and also license contracts. Cloud providers who offer data storage services are similar to data storage services in outsourcing contracts. The difference lies in the fact that cloud service will keep data in the cloud instead of being maintained in a server in the physical world. Therefore, concepts and even

---

[1] Peter Mell & Timothye Grance. "The NIST Definition of Cloud Computing: Recommendations of the NIST". US Department of Commerce. (September 2011) Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Last accessed 12 September 2012. Page 1

[2] See: David Navetta. "Legal Implications of Cloud Computing (The Basics and Framing the Issues)", available at http://www.llrx.com/features/cloudcomputing.htm. Last accessed 12 September 2012.

[3] Ibid

technological approaches behind "cloud computing" can thus not be considered a novelty as such and in particular data centers already employ methods to maintain scalability and reliability to ensure availability of their hosted data.[4]

A standard contract through click-warp method, in which a user will accept the terms and conditions offered by the third party by clicking the box provided for such purpose, is a chosen method in delivering a cloud contract to the customer. Moreover, depending on the type of services the cloud provider might offer, cloud computing contracts can also be considered a replication of one of the regular IT contracts. To sum it up, services in the cloud computing might be considered as resembling all the regular IT models of businesses.

1.2 Problem Statement

Utilizing the cloud will mean that it is difficult to determine the location of the data since they are kept inside the cloud and thus the data will flow between different data centers (location independence). In cloud computing all data is pooled together and stored randomly on a stack of servers and also all clients' accounts share the same servers (multi-tenant).[5] A simple question on what happens with data inside the cloud would trigger so many other questions such as the exact location of such data; which is important to determine the jurisdiction. Other questions focus on the security of the whole cloud architecture and customers' data or content, or questions on issue of data integrity, data disclosure, data confidentially, data protection policies, and also interoperability between the cloud providers.

Cloud providers offer their services to customers through a standard-form contract elaborated in the Terms and Conditions. Therefore reviewing the Terms and Conditions of cloud service will show a general pattern of the cloud provider approaches to address all the mentioned above issues. Subsequently, such patterns will be useful to identify the legal problems associated with cloud computing technology. Finally, identification

---

[4] Expert Group Report for Commission of the European Communities. "The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010". Available at http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf, Last accessed 12 September 2011. Page 5

[5] Cecile Christensen. "Cloud computing: what is it?" The Nordic IT Law Conference 2010. Available at http://www.it-retsforum.dk/uploads/media/Cloud_Computing_What_Is_It_by_Cecilie_Christensen.pdf, Last accessed 12 September 2011. Page 8

of these problems will be helpful to draft cloud contracts which are compatible with prevailing laws.

1.3 Objective

Based on the problem statement mentioned above, this thesis has three objectives:

- To explain the technological aspects of cloud computing and identifying the specific legal issues associated with such technology.
- To survey cloud providers' terms and conditions in market practice as an attempt to find a general pattern of cloud providers policy in addressing those legal issues.
- To elaborate the main legal considerations on drafting cloud computing contracts which are compatible with the prevailing laws.

1.4 Legal Questions

- What are the impacts of cloud computing technology towards the application of the existing laws?
- How are the cloud providers - through their terms and conditions - addressing specific legal issues associated with cloud computing technology?
- What are the legal considerations on drafting cloud computing contracts which are compatible with prevailing law? This concern is also equivalent to the question on whether the current practice is able to sufficiently address the overall legal impacts of cloud computing.

1.5 Previous Studies

A number of books and articles have been published on the cloud computing issues. Most of them discuss cloud computing from technological or legal points of view. There is a lack of literature that specifically identifies, reviews and also drafts a cloud computing contract based on the existing legal frameworks. Those previous studies will be used in this thesis insofar they can provide general foundations for this research.

1.6 Thesis Structure

The structure of this research will be divided as follows:

Chapter I Introduction

This chapter will serve as a brief introduction of the current issues of cloud computing from technological and legal points of view.

Chapter II Cloud contract and its legal implications

This chapter will firstly serve as the background to better understand the technological nature of cloud computing. Secondly, this chapter will also identify legal issues associated with such technology. The examination of the legal issues on this chapter will be conducted from the customer's (Consumers, Small Medium Enterprises/SMEs and Corporate) point of view. Therefore this thesis will not specifically base on the business to business (B2B) or business to consumer (B2C) analysis. This thesis also only focuses on the paid service model in the cloud computing. Finally, the last part of this chapter will be dedicated to elaborate on the nature of cloud computing contract as a form of standard-form contract.

Chapter III Elaboration on types of cloud contract documents and the survey of cloud computing terms and conditions.

Firstly this chapter will explain on all documents in cloud computing contracts known as the Terms and Conditions. Secondly this chapter will survey a range of cloud Terms and Conditions as offered by cloud providers to consumers. Since one particular clause in cloud contract can be a really heavy and broad topic, it is worth to note that this section does not seek to make a detailed review on the specific issue of one particular legal problem in cloud contract.

Chapter IV Drafting a cloud computing contract

Based on the findings from the previous chapter, this chapter firstly tries to elaborate on the main legal consideration on drafting a cloud computing contract based on the existing law. The approach in this chapter is similar to the previous chapter in which no detailed review on the particular subject will be made. Secondly, this chapter will discuss the aspect of contract negotiation in cloud computing contracts.

Chapter V Conclusion

This chapter will take into consideration what have been discussed in this thesis and provides some final remarks.

1.7 Methodology

The research will be conducted using traditional legal methods, i.e. focusing primarily on laws, regulations, *travaux preparatoires,* case law and other sources. The research will rely on the related normative framework on the regional or international law applied on the European level which directly or indirectly regulates cloud computing. Normative frameworks applicable in the digital environment such as the Data Protection Directive will also become important reference when analyzing legal issues. The Expert Group Report for Commission of the European Communities such as on The Future of Cloud Computing will be useful in the analysis.[6]

2 Cloud Computing Technology and Its Legal Implications

2.1 Service Models

There are three service models in cloud computing:

- Infrastructure as a Service (IaaS) stands for the capability to provide the consumer with a provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.[7]
- Platform as a Service (PaaS) stands for the capability provided to the consumer who can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[8]
- Software as a Service (SaaS) stands for the capability provided to the consumer who uses the provider's applications running on a cloud infrastructure.[9]

2.2 Deployments Models

According to NIST, there are four deployment models in cloud computing:[10]

---

[6] See: Expert Group Report. Supra note 4
[7] Peter Mell, Supra note 1. Page 3
[8] Ibid. pp.2-3
[9] Ibid. Page 2
[10] Ibid. Page 3

- *Private cloud*. The cloud infrastructure is provisioned for exclusive use by a single organization comprising of multiple consumers (e.g., business units).
- *Community cloud*. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- *Public cloud*. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or a combination of them.
- *Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2.3 Cloud Computing Characteristics

The most basic architecture of cloud computing technology lies in the front-end and the back-end principles. The front-end represents part of computing that is available to the cloud users. The back-end is the cloud (internet) which is comprised of infinite computing resources.

According to the Expert Group Report for Commission of the European Communities; cloud computing characteristics can be described as follows:[11]

- *Virtualisation* which refers to the capability to hide the technological complexity of the infrastructure (including management, configuration etc.) from the consumers and enables enhanced flexibility (through aggregation, routing and translation). Virtualisation can make it easier for the user to develop new applications, it aslo reduces the overhead for controlling the system.
- *Elasticity* is an essential feature of cloud systems and circumscribes the capability of the underlying infrastructure to adapt to changing, potentially non-functional requirements, for example amount and size of data supported by an application, number of concurrent users etc.

[11] Expert Group Report released broad cloud computing characteristics. For the purpose of this thesis, we will only describe the most relevant characteristics. For the complete characteristics, see: Expert Group Report. Supra Note 4. pp.12-15

- *Reliability* denotes the capability to ensure constant operation of the system without disruption, i.e. no loss of data, no code reset during execution etc.
- *Agility and Adaptability* refers to the capability of instant and precise reaction to changes according to the requests, resources and environmental conditions. This feature is present when the systems are required to respond to different resources, different quality or different routes. This feature strongly is connected to elastic capabilities.
- *Availability* of services and data is an essential capability of cloud systems and lies in the ability to introduce redundancy for services and data so failures can be masked transparently.
- *Location independence*: services can be accessed independent of the physical location of the user and the resource.
- *Multi-tenancy* the location of code and / or data is principally unknown and the same resource may be assigned to multiple users (potentially at the same time).

2.4 Legal Implications of Cloud Computing Technology

One important legal issue arising from the cloud computing technology is related to defining the controller and processor under the light of Data Protection Directive (DPD).[12] The DPD defines the controller as the party who determines the purposes and means of the processing of personal data.[13] Hence, processor means a party which processes personal data on behalf of the controller.[14] Applying such definitions in cloud computing service is quite challenging. For instance, a cloud customer who collects personal data in the service makes him a controller, and concomitantly the SaaS provider becomes the processor. However, in providing its service, the SaaS provider uses infrastructure made available by the IaaS provider. Under the DPD, an IaaS provider will be considered as a sub-processor since it is involved in processing the personal data.[15] Yet, the IaaS provider could offer cloud service without necessarily knowing the nature of the data their customers intend to process using their

[12] 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
[13] Ibid. Article 2 (d)
[14] Ibid. Article 2 (e)
[15] Ibid. Article 2 (f)

infrastructure.[16] Moreover, such providers generally can't control the form in which their customers choose to upload the data.[17] In this case, it is seems insufficient to consider the IaaS provider also responsible for the personal data.

Data integrity is also an important legal issue in cloud computing. Since cloud computing is a relatively new technology, there is a reasonable concern from customers on the issue of data integrity when using a cloud service. In cloud computing, the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.[18] This means that such computing resources will be shared by more than one user. A particular concern in this case is how the provider can ensure that the customer data is fully segregated and not co-mingled or accessible by others.[19]

Cloud computing is relatively a new business model and this fact has made security one of the biggest concerns for customers entering a cloud contract. There is a need to determine the level of data encryption for it to be considered adequately safe. To this end, the question of what audit controls are in place to ensure that the strong encryption has not been compromised and is used in the correct way with only the client knowing the keys become really important.[20]

The next issue of cloud security is the ownership of data in cloud computing. There are two important data issues here: firstly, data or content uploaded by the customer to the cloud, secondly, data emanating from relationships between the provider and customer in cloud service. Since the data that is uploaded to the cloud will be stored inside the provider infrastructure, the first concern is the ownership of such data or the content and

---

[16] Kuan Hon. "Data Protection: The Law and You." Available at: http://blogs.computerworlduk.com/cloud-vision/2011/04/data-protection-the-law-and-you-1/index.htm. Last accessed 26 October 2011
[17] Ibid
[18] Peter Mell. Supra note 1. Page 2
[19] Henry Wolfe. "Cloud Computing: The Emperor's New Clothes of IT." Informing Science Institute. University of Otago, New Zealand (2011). Available at: http://www.informingscience.org/proceedings/InSITE2011/InSITE11p599-608Wolfe281.pdf. Last accessed 9 October 2011. Page 602
[20] Ibid

applications in the cloud. As a result of activities between the user and provider, information of various types such as the amount of usage and traffic patterns information can be generated by the provider.[21] The ownership of such information becomes the second concern.

There is also a concern in determining the jurisdiction and applicable law in cloud computing contract in the absence of choice of law/forum. To illustrate, when a company processes data in the UK, stores it on a server in Ireland but sends it via France – as it may have a subsidiary there – it is not yet clear which country's law would prevail in a legal dispute if the party does not choose the jurisdiction for the cloud contract.[22]

There is also another concern on data portability issues which closely related to data interoperability. This becomes an important issue when a customer wants to move or use his data in another cloud service. It is worth to note that typical problem of PaaS is vendor lock-in,[23] in which the application created on the PaaS level cannot be moved to another cloud host. Applications developed in one PaaS provider will be unique since it was built with cloud resources that are available in the cloud platform of that provider. It is pertinent to note that data portability is not a legal issue that challenges the application of existing laws, but it is important in the light of achieving a single market agenda in EU.

The explanation above indicates that to some extent, the emergence of cloud computing technology has posed a challenge on the application of existing laws that has a bearing on cloud computing technology. Based on this fact, there is a need to review how these issues developed in cloud market practice. An assessment of cloud contracts, in which the provider governs their relationship with customers and certainly regulates all the above mentioned legal issues, will be required. Since what cloud service offers is

---

[21] Ibid. Page 604
[22] Marco Giunta. "Cloud Computing: An Opportunity and a Legal Maze." Available at: http://marcogiunta.com/tech/cloud-computing-an-opportunity-and-a-legal-maze/. Last accessed 10 September 2011.
[23] See generally: Mary Brandel. "The Trouble with Cloud: Vendor Lock-in." Available at: http://www.cio.com/article/488478/The_Trouble_with_Cloud_Vendor_Lock_in. Last accessed 25 September 2011.

presented in a standard-form contracting, it is necessary to firstly elaborate all the legal aspects of a standard-form contract.

2.5 Cloud Contract as Standard-form Contract

The provision of cloud services shall obviously be regulated by a contract, or a group of contracts, that will govern the specific 'position' of each party in the relationship, i.e. the duties, liabilities, remedies, etc.[24] Such contracts surely have to rely on fast-to-contract approaches which enable costumers to conclude the contract immediately.[25] Cloud agreements, therefore, are rarely negotiable, with most providers requiring a would-be subscriber to adopt their standard agreement.[26]

Electronic contracting that utilizes a standard-form contract presents the form on a take-it-or-leave-it basis. Therefore, non-negotiability becomes the most significant feature and leaves no room for the consumer to review or negotiate such contract. Costumers who try to read electronic boilerplates must struggle to understand pages filled with legal jargon that would be difficult for an experienced attorney to decipher.[27] Moreover, a party that writes standard terms drafts them in such a way as to resolve all possible issues in its favor.[28] Combined with the principle of take-it-or-leave-it, this would give an opportunity for the web site owners to create terms that not only minimize companies' legal obligations, but also shift their potential liability.[29]

The common method to assent in cloud contract is click-warp contracting.[30] As a method, click-wrap contracting is meant as a reference to the contracting model where

---

[24] Davide Parrilli. "Legal Issues in Grid and Cloud Computing." In: Grid and Cloud Computing: A Business Perspective on Technology and Applications (K. StanoevskaSlabeva). Berlin (Springer-Verlag) 2010. Page 98

[25] Simon Hodgett. "Cloud Computing Contracting and the Spectrum of Risk." Thirteenth Annual Canadian IT Association Conference. (2009) Available at: http://www.it-can.ca/direct/membersonly/2009conf/cloud_computing_hodgett.pdf. Last accessed 7 October 2011. Page 12

[26] Neil Brown. "Thames Valley Group Meeting Report: Cloud Computing Contracts." The IT Law Community. (2011) Available at: http://www.scl.org/site.aspx?i=ne19148. Last accessed 7 October 2011

[27] Robert Hillman. "Standard-Form Contracting in the Electronic Age." 77 N.Y.U. L. Rev. 429. 2002. Page 479

[28] James Maxeniner. "Standard Terms Contracting in the Global Electronic Age: European Alternatives", 28 Yale J. Int'l L. 109 (2003) Page 7

[29] Llewellyn Joseph Gibbons. "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace." Cornell J.L. & Pub. (2007). Page 475

[30] There are two other methods in electronic contracting: shrink-wrapped and browse-wrap method.

users express their agreement on terms offered by a business by clicking on the button of “I accept”, “Yes”, “I agree”.[31] Click-wrap agreement is the answer to the requirement of fast-to-contract approaches and also enabling the business to conclude the contract immediately.

Although standard-form contracts seem suspect and fail to satisfy contract law's notions of bargained-for exchange, courts and theorists generally consider enforcement of such terms appropriate.[32] Appropriate in this term means that such standard contracts must fulfill all requirements imposed by the existing laws namely: the content, incorporation of the terms and the information duties requirements.

2.5.1 Content Requirements

The required basic rules here are that terms are to be presented in plain and intelligible language.[33] Contracts must be drafted in such way to prevent the imposition of the unfair terms which are likely depriving the consumer right(s).[34] A good example of this requirement is the EU Unfair Term Directive which sets an indicative and non exhaustive list of unfair terms.[35] Another issue that needs to take into account is from the private international law perspective, in which a standard contract must provide a choice of court clause[36] and also choice of law clause.[37]

In Shrink-wrapped method, items such as software are sold in cellophane shrink-wrap with a visible notice stating the license agreement is enclosed. The shrink-wrap agreement becomes effective when the consumer tears open the shrink-wrapped package.
Browse-wrap, on the other hand, stands for a method of assenting into an electronic contract in which the internet users will find a hyperlink in the front page of the web which linking the user to the place where the web owner put the terms and conditions. (William Condon. 2004)

[31] Maryke Silalahi Nuth. “E-commerce Contracting: The Effective Formation of Online Contracts.” University of Oslo. (2011) Page 118

[32] Robert Hillman. Supra note 27. Page 437

[33] Article 5 of Council Directive 93/13/EEC on Unfair Terms on Consumer Contract

[34] Maryke. Supra note 31. Page 198

[35] Article 3 of Unfair Terms on Consumer Contract

[36] Council Regulation (EC) No 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Brussels I)

[37] Regulation (EC) No.593/2008 on the Law Applicable to Contractual Obligations (Rome I)

2.5.2 Incorporation of Terms

Incorporation of terms refers to the requirements in which a standard term is deemed to have been accepted by the other party and thus forming part of the contract.[38] In some member states of the EU, the incorporation terms are reflected in the "red hand" rules. The application of "red hand rules" implies that the more unreasonable a clause is, the greater the notice which must be given of it.[39] And if one condition in a set of printed conditions is particularly onerous or unusual, the party seeking to enforce it must show that that particular condition was fairly brought to the attention of the other party.[40]

In the US, prohibition of surprising clauses is addressed using an approach known as unconscionability doctrine.[41] If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.[42]

In Canada, the approach taken is using the "reasonable expectation" doctrine.[43] When applied, the doctrine of reasonable expectations thus creates an affirmative duty on the part of the business to point out and explain reasonably unexpected terms even if they clearly were stated in the contract.[44] This doctrine allows courts to overturn express contract language if the term contradicts the consumer's reasonable expectations.[45]

---

[38] Emily Weitzenboeck. "Electronic contracting: Recognition and Validity of Electronic Contract." Lecture Notes on E-Commerce Class of ICT Programme of University of Oslo. (2011) Page 15
[39] J Spurling Ltd v Bradshaw [1956] 1 WLR 461.
[40] Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1989] QB 433
[41] Codified in Section 2-302 of the Uniform Commercial Code.
[42] See generally: Robert Hillman. "The Richness of Contract Law: An Analysis and Critique of Contemporary Theories of Contract Law." 129-43 (1997). Page 25
[43] First appeared in the case of Wigle v. Allstate Ins. Co. of Canada (1984), 49 O.R. (2d) 101.
[44] Robert Hillman. Supra note 27. Page 460
[45] Ibid. Page 456

2.5.3 The Information Duties

This requirement obliges the seller or supplier to provide certain information in e-commerce transactions. The purpose of such obligation is to ensure the protection of the client; e.g. identification of the seller/service provider and also for consumer protection. On the EU level, based on the Distance Selling Directive (DSD), it is mandatory for the seller or supplier to provide the consumer with certain information such as: the identity of the supplier, his address, the main characteristics of the goods or services and the price of the goods or services including all taxes.[46] Detailed requirement in rendering such information is elaborated further in the DSD by stating "*…that the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions …*"[47]

3 GAZING INTO THE CLOUD: A SURVEY OF THE TERMS AND CONDITIONS IN CLOUD CONTRACT

This chapter will firstly explain the different types of cloud contracts offered in the cloud computing service. Secondly this chapter will review the current practice on how the provider governs their relationship with the customers in cloud contracts. We will focus the review on the cloud contract clauses which portray the legal implications described in section 2.3 of this thesis. This review will illustrate not only the level of legal compliance of cloud providers must abide by, but also the level of maturity of the cloud service market. More importantly; this review will illustrate how the cloud provider deals with legal issues associated with cloud computing technology.

To serve such purpose, 17 different cloud providers will be surveyed in order to present a clear and comprehensive view on cloud contracts (Annex A). The result of such survey will be combined with academic studies on the topic. Research initiated by the Centre for Commercial law Studies of Queen Mary University of London; surveyed 31

[46] Article 4 of DSD of Directive 97/7/EC on the Protection of Consumers in Respect of Distance Contracts
[47] Article 4 (2) of DSD

cloud computing contracts from 27 different providers is the example of academic study that will be useful to complete this chapter.[48]

3.1 Types of the Cloud Contracts

A standard-term contract in cloud service refers to a document or set of documents which governs the legal relationships between the user and cloud provider. Such standard-term contracts are commonly known as the Terms and Conditions (T&C). T&C documents usually come in a number of forms, from relatively short and simple, to lengthy and complex.[49] Some cloud providers will present their T&C in one integrated document or split it over several documents. The following are the cloud contract documents commonly offered by the cloud provider:

- Term of Service (ToS); usually serve as the most important document in electronic contracts as well as in cloud computing contracts. ToS describes different important provisions such as scope of cloud service, customer and provider obligations, Intellectual Property Rights (IPR), clauses related to data or content in the cloud service, applicable law and jurisdictions to the contract and termination of contract.
- Service Level Agreements (SAL); which describe specified level of service, support options, a guaranteed level of system performance as relating to downtime or uptime, in addition to a specified level of customer support and for what fee.[50]
- Acceptable Use Policy (AUP); this document details the permissible and also the prohibited uses of service. This document establishes an acceptable use of cloud services based on the cloud provider discretions using culture of ethical and lawful behavior perspective.
- Privacy Policy; this document generally governs handling of personal information. Rules and principles of data privacy as demonstrated in DPD are some of the main concerns of this document. Privacy policy also deals with the provider's responses to specific issues such as the collection of personal information or links to third party websites.

---

[48] Simon Bradshaw, Christopher Millard, and Ian Walden. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." Centre for Commercial Law Studies. London (2010). Available at http://ssrn.com/abstract=1662374. Last accessed 8 October 2011.
[49] Ibid Page 14
[50] Definition of Service Level Agreement. Available at: http://www.webopedia.com/TERM/S/Service_Level_Agreement.html. Last accessed 7 October 2011

3.2 A Survey of the Terms and Conditions of Cloud Contract

In this section we will survey, analyze and compare T&Cs taken from cloud service providers either on the IaaS, PaaS or SaaS level. At the same time one must take into consideration that the likeliness of a T&C will change rapidly following the most suitable market practice or legal compliance, it is important to note that this survey is made based on the T&C publicly available in the beginning of November 2011.

3.2.1 Customer Obligations

This relates to the provisions that spread throughout T&C documents and govern general obligations of the customer in relation with the utilization of the cloud service. Such obligations will vary from one cloud service provider to another and depend on the models of service offered (IaaS, PaaS or SaaS).

One type of obligation commonly found on this topic; is the existence of clauses that prohibit the customer from interfering with the back-end architecture of a cloud service. A good example is Rackspace, which prohibits the user to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without expressed authorization of the owner of the system or network.[51] This obligation reflects user limitation such as in SaaS or PaaS in which the user does not manage or control the underlying cloud infrastructure including network, servers, operating systems and storage.[52]

Another type of customer obligation is the set of obligations as stipulated in the AUP document. As explained before, the AUP document consists of a list of the permissible and impermissible acts for a customer when using the cloud service. An example of an obligation mentioned in AUP is the provision of bulk commercial e-mail or spam. According to the Electronic Communication Directive, the use of e-mail for direct marketing is only allowed to recipients who have given their prior consent.[53] In

---

[51] Article 1.1 of AUP. Rackspace. Available at: http://www.rackspace.ae/uploads/involve/user_all/64_Acceptableusepolicy.pdf. Last accessed 10 November 2011, Compare: Article 4.2.1 of Customer Agreement. Amazon Web Service. Available at: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html. Last accessed 10 November 2011

[52] Peter Mell, Supra note 1. pp.2-3

[53] Article 13 of the Directive 2002/58 on Privacy and Electronic Communications

compliance with this regulation, a cloud provider will stipulate that the user of their service must obtain the provider's advance approval for any bulk commercial e-mail other than for market research purposes.[54]

There is also an obligation regarding third party access to cloud service. In market practice, most of the T&C hold the customer responsible for the third party access to the service even if such access occurred because of manipulation or hacking.[55] It is also common for a T&C require customer to take reasonable security measures such as using encryptions. A good example of this would be T&C of Amazon Web Services (Amazon AWS) which states: "*...you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your content and applications.*"[56]

In some cases, cloud contracts also stipulate that customers will be responsible for any of the third party actions in the cloud service. An example of this practice is GoGrid that states: "*third party violations of the AUP using customer's Service, including any IP addresses, points of access to the Internet, systems, software, or equipment assigned to customer … will be considered violations by customer.*"[57]

3.2.2 Terms Related to Cloud Service Provider

A majority of the cloud service providers, as we will see in this section, set a standard-form contract which in nature will limit or resolve their inherent liabilities. Such attempts will be hidden in the number of clauses in the ToS as well as other T&C documents such as Privacy Policy and AUP. The following clauses are taken from different cloud T&C in which the provider disclaimed responsibilities in regards to the front-end architecture of the cloud:

- Flexiant: "*do not guarantee that the Website will be compatible with your PC or other hardware and equipment used to access the internet and/or the Website.*"[58]

---

[54] Article 3 of AUP. Rackspace. Supra Note 51
[55] This topic will be discussed in the section 3.2.3.2 on Data Integrity
[56] Article 7.2 of Customer Agreement. Amazon AWS. Supra note 51
[57] Article 4 of ToS. Gogrid. Available at: http://www.gogrid.com/legal/terms-service.php. Last accessed 10 November 2011
[58] Article 2.1 of ToS. Flexiant. Available at :http://www.flexiant.com/products/flexiscale/terms/. Last accessed 10 November 2011

- Joyent: "*does not warrant that …. (i) joyent services will meet your requirements.*"[59]
- Gogrid "*will have no liability whatsoever … from… mistakes, omissions, interruptions, deletions of files, errors, defects, delays in operation, or other failures of performance of the service, including without limitation accidental disconnection.…*"[60]

Most cloud providers also present arbitrary clauses in connection with service availability. A cloud provider reserves broad rights to "*at any time to modify, suspend, or discontinue providing the Service or any part thereof in its sole discretion with or without notice*."[61] Amazon promotes AWS as a reliable cloud computing option, but its service level agreement states that "*AWS reserves the right to refuse service, terminate accounts, remove or edit content in its sole discretion.*"[62] Similarly, Apple iWork Public Beta claims to reserve the right to modify, suspend or stop the Service (or any part thereof), either temporarily or permanently, at any time or from time to time, with or without prior notice.[63]

Cloud providers also consistently maintain that the users are entirely responsible for the security issue when using the service especially the security of access to service and any data contained within. See the following examples:

- Amazon: "*You expressly agree that your use of this site is at your sole risk.*"[64]

  "*If you use the AWS Site, you are responsible for maintaining the confidentiality of your AWS account and password and for restricting access to your computer, and you agree to accept*

[59] Article 9 of ToS. Joyentcloud. Available at: http://www.joyentcloud.com/about/policies/terms-of-service/. Last accessed 11 November 2011
[60] Article 8 (c) vii of ToS. Gogrid. Supra note 57
[61] Electronic Privacy Information Center. Cloud Computing. Available at: http://epic.org/privacy/cloudcomputing/. Last accessed 11 October 2011
[62] Ibid
[63] Article 2 of ToS. Apple iWork Public Beta. Available at: http://www.apple.com/legal/iworkcom/en/terms.html. Last accessed 12 November 2011
[64] Clause of "Disclaimer of Warranties and Limitation of Liability" of ToS. Amazon AWS. Available at: http://aws.amazon.com/terms/. Last accessed 11 November 2011

responsibility for all activities that occur under your account or password."[65]

- Gogrid: "*Customer will employ reasonable security precautions in its use of the Service, including … encryption of social security numbers, medical records, and information of similar sensitivity belonging to Customer or to its customers or users.*[66]

It is worth noting that some providers are taking different approaches to the security matter of cloud service. Dropbox, a file hosting and backup via SaaS, albeit on its website rather than in its T&C, states: "*Dropbox treats the security of your data very seriously. Everything you store on Dropbox is encrypted both in transmission and storage. Nobody can access your files unless you choose to share them yourself.*"[67]

Cloud providers also commonly deny the quality of the service and any related matters in delivering the service. An example of this is would be Gogrid which states "… *not responsible for the accuracy, completeness, and usefulness of the service.*"[68] Microsoft, in a slightly different approach states that "*Microsoft … make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose.*"[69]

Disclaimers regarding third party services or products for various reasons are also commonly found in T&C. Such disclaimers even exist in situations where the customer needs the third party's applications to access or use the cloud service. The example is Gogrid, that states: "… *not responsible or liable for third party products and services even if the third party products and services are related to the service or to customer's ability to receive or exploit the service.*"[70] This is consistent with the Gogrid T&C

---

[65] Clause on "Your Account" of ToS. Ibid
[66] Article 7 (b) of ToS. Gogrid. Supra note 57
[67] Simon Bradshaw. Supra note 48. Page 30
[68] Article 8 (c) viii of ToS. Gogrid. Supra note 57
[69] Clause on "Notice Specific to Documents Available on the Web Site" of ToS. Microsoft. Available at: http://www.microsoft.com/About/Legal/EN/US/IntellectualProperty/Copyright/default.aspx#EPC. Last accessed 10 November 2011.
[70] Article 1 (c) ii of ToS. Gogrid. Supra note 57

clause on Private and Confidential Information which states: "*GoGrid is not responsible for use or misuse of data by any third party*".[71]

The last issue related to the providers is regarding the variation of terms. Many providers claim to be able to amend their contracts unilaterally, simply by posting an updated version on the web.[72] Some of the providers will provide written notice when they are about to make an alteration to the terms. This approach is exercised by the cloud providers that offer services such as Google App,[73] or Dropbox.[74] In Elastichost, the customer's refusal to contract alterations will lead to the termination of the contract.[75] Furthermore, this clause does not mention what will happen with the customer's data if the termination occurred for such reason.

Some other websites, such as Flexiant, require the customer to monitor published T&C for unilateral changes.[76] Some providers simply state that they may vary their T&C, with no further notice on whether the customer will be notified of this or what constitutes acceptance of the change.[77] The examples of this would be UKFast[78] and Amazon AWS.[79]

3.2.3 Terms Related to Data

Terms related to customer data is one of the most controversial issues in cloud computing contract. Concerns about data range from the issue on how the provider will handle their customers' data, how they will assure the integrity of such data, where is the exact location of the data, the level of confidentiality and conditions to disclose such data to third party, and also what the policy on data preservation when the cloud

---

[71] Article 7 (a) of ToS. Ibid
[72] Simon Bradshaw, Christopher Millard, and Ian Walden. "The Terms They Are A-Changin'... watching Cloud Contracts Take Shape. The Center for Technology Innovation." Issue in Technology Innovation. (2011). Page 2
[73] Article 9.3 of Google Apps for Business Agreement. Google. Available at: http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html. Last accessed 12 November 2011
[74] Clause on "Modification" of ToS . Dropbox. Available at: https://www.dropbox.com/terms. Last accessed 12 November 2011
[75] Clause on "Suspension and Termination" of ToS. Elastichost. Available at: http://www.elastichosts.com/cloud-hosting/terms-of-service. Last accessed 12 November 2011
[76] Simon Bradshaw. Supra note 48. Page 42
[77] Ibid. Page 21
[78] Clause on "Corporate Profile" of T&Cs. UK Fast Cloud Service. Available at: http://www.ukfast.co.uk/terms.html. Last accessed 13 November 2011
[79] Article 2 of Customer Agreement. Amazon AWS. Supra note 51

contract relationship comes to an end. In market practice, it is not surprising that cloud providers respond to this issue in various ways and most of them disclaim any liability on customer data.

3.2.3.1 Ownership over Data

The first concern of the customer regarding this issue is who will own data or content uploaded by the customer to the cloud. Contrary to public concerns regarding the provider's claim to data possession,[80] most of cloud providers generally respect the customer ownership over data or content in the cloud. Most of the cloud T&C, such as Google,[81] Rackspace,[82] or Apple[83] do not show that providers have any intention on claiming ownership of data or content in the cloud. Generally, T&C state that the cloud provider "*does not claim ownership of the materials and/or content you submit or make available on the Service*."[84] Common provisions on ownership over customer data usually go as far as stating that both provider and customer retain all rights, title and interest in and to our respective trade secrets, inventions, copyrights and other intellectual property. Intellectual property developed by providers during the performance of the service(s) will belong to provider unless there is a customer interest in such intellectual property."[85]

Nonetheless, some providers also take a different approach by imposing a license by which the customer authorizes the provider to copy such data and republish it for the purpose of providing the service.[86] Microsoft mentions a purpose in connection with the operation of their Internet businesses,[87] while Facebook even goes further by stating

---

[80] See generally: Paul T. Jaeger, Jimmy Lin & Justin M. Grimes. "Cloud Computing and Information Policy: Computing in a Policy Cloud?". Journal of Information Technology & Politics, 5:3, 269-283. (2008) Available at: http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479. Last accessed 13 November 2011. See also: Simon Hodgett. Supra note 25
[81] Article 7, Google App Agreement. Google. Supra note 73
[82] Article 25 of General Terms. Rackspace. Available at: http://www.rackspace.co.uk/legal/general-terms/. Last accessed: 13 November 2011
[83] Article 7 of ToS. Apple iWork Public Beta. Supra note 63
[84] Ibid
[85] Article 25 of General Terms. Rackspace. Supra note 82
[86] Simon Bradshaw. Supra note 48. Page 43
[87] Clause on "Materials Provided to Microsoft" of ToS. Microsoft. Supra note 69

they are allowed to use any IP content that the user publicly posted on or in connection with Facebook. [88]

Another issue in the ownership of data is copyright infringements in the cloud service. Some providers facilitate the owner's copyright interests against the third party claims or infringements over the data or content. The example in this case is Google, in that it will assist the customer in defending its copyright when there is a claim from the third party.[89] In a different approach, Amazon AWS provides the customer with possibility to submit a complaint over the infringement of copyright by the third party.[90] In this complaint mechanism, Amazon AWS only collects facts of the infringements and does not mention anything about the possible legal remedies for the case.[91]

The ownership of various types of information emanating from the interaction of the user in the cloud service is another important issue. The amount of usage and traffic patterns information can be generated by the provider with justifiable reason that the information is needed to manage the cloud resources and performance on offer.[92] Microsoft Azure uses this approach and states: "*You also grant Microsoft the right to track and record usage patterns, trends, and other statistical data related to your use of the Services for Microsoft's internal use*."[93] It is not so clear how this type of provision will affect the customer's rights in a broad sense, but providers will surely benefit if they use such information for marketing campaigns.

3.2.3.2 Data Integrity

In relation to data integrity, most of the providers claim that they have no liability in relation to the loss of data or access to data. An example of this practice is ElasticHosts that states: "*We do not make any representations, warranties or guarantees regarding data retention, data integrity, service security or service suitability for any purpose*."[94] Furthermore, a provider can also claim not to be responsible for any use or misuse of

---

[88] Article 2.1 of "Statement of Rights and Responsibilities". Facebook. Available at: http://www.facebook.com/terms.php. Last accessed 12 November 2011
[89] Article 11 (5) b of Google App Agreement. Google. Supra note 73
[90] Clause on "Copyright Complaint" of ToS. Amazon AWS. Supra note 64
[91] Clause on "Notice and Procedure for Making Claims of Copyright Infringement". Ibid
[92] Henry Wolfe. Supra note 19. Page 604
[93] Simon Bradshaw. Supra note 48. Page 43
[94] Clause on "Services and Responsibilities". Elastic Host. Supra note 75

data by a third party. Another example is Gogrid which states that they are: "*…not responsible for use or misuse of data by any third party, including without limitation providers of Third Party Products and Services, the operator of any website linked to GoGrid's website, or any GoGrid customer, even if GoGrid hosts such customer's Website.*" [95]

Many cloud T&C also hold customers solely responsible for data security.[96] It is not rare to see clauses in which the customer is asked to provide a data encryption system on their own initiative.[97] In some cases, the cloud providers also request the customer to regularly maintain backups of their data as the providers make no data arrangements for the customer.[98] This practice indicates that cloud providers ignore the fact that a breach of security or loss of data can cause financial loss to the business as well as damage its reputation and the confidence of its customers.[99]

On the other hand, some providers actually take a different approach and to some extent provide a guarantee on data integrity. Salesforce.com states that it: "*shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of the customer data*."[100] CA 3Tera AppLogic also follows this approach by stating: "*The Company agrees to use best efforts and commercially reasonable best practices when deploying services related to data integrity…*".[101]

3.2.3.3 Data Location

While the customer can control some aspects of security and data integrity, such as maintaining independent back-ups and using data encryption, many aspects of data in a

---

[95] Article 7 (a) of ToS. Gogrid. Supra note 57
[96] See: Article 7 (2) of Customer Agreement. Amazon. Supra note 52; and clause on "Iwork.com Account" of ToS. Apple. Supra note 64
[97] See: Ibid. Amazon or Clause on "Account Security" of ToS. Dropbox. Supra note 75
[98] See: Article 6 of ToS. Joyentcloud. Supra note 60; or Article 4 of ToS. Apple iWork Public Beta. Supra note 64; Clause on "Your Responsibilities" of ToS. ElasticHosts. Supra note 76
[99] Mark Vincent, Nick Hart and Kate Morton. "Cloud Computing Contracts White Paper: A Survey of Terms and Conditions." Truman Hoyle Lawyers. (2011) Available at: http://www.ficpi.org.au/articles/White_Paper_June2011.pdf. Last accessed 13 October 2011. Page 10
[100] See: article 4 (2) of Master Subscription Agreement. Salesforce. Available at: http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf. Last accessed 14 November 2011
[101] Article 10 of ToS. 3Tera. Available at: http://www.3tera.com/Terms/index.php. Last accessed 14 November 2011

cloud based environment are out of the customer's control (or even knowledge).[102] The location of data is one of the aspects that is not controlled by the customer. As well as location, the international nature of the cloud raises questions about the extent to which data is protected in transit, be it between the customer and provider or within the providers own infrastructure.[103] Cloud practice shows that T&C generally do not stipulate data location in the contract. Rackspace only go as far as to inform the customer by stating: "*we are constantly upgrading our data centre facilities and in order for you to benefit from this, you agree that we may relocate your servers within our data centres…*".[104] Microsoft even takes a broader approach by stating: "*Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country…*".[105]

The location of customer data is likely to be a key concern for some customers, who will be mindful about the restrictions, for example, applying to the export of certain types of data from the U.S, or the export of "personal data" from the EEA.[106] Amazon AWS is one of the few providers that mention data location in their cloud service. Amazon AWS offers a number of "regional zones" in which a customer may be assured the data will remain. Amazon Web Services offers the option of restricting data storage to one of certain regions including the E.U. (specifically Ireland), U.S. Standard and U.S. West (Northern California).[107] However, the terms and conditions for Amazon Web Services do not contain any term that specifically warrants that data will be kept in a particular location.[108] A customer is asked to select a data region during the sign-up process instead of it being incorporated into the customer's contract with Amazon.[109]

A good example of a cloud contract which states the exact data location is the City of Los Angeles' Google Apps Contract which states: "*Google agrees to store and process*

---

[102] Mark Vincent. Supra note 99. Page 10
[103] Simon Bradshaw. Supra note 48. Page 28
[104] Article 20 of General Terms. Rackspace. Supra note 82
[105] Clause on "Use of Your Personal Information" of Privacy Statement. Microsoft. Available at: http://privacy.microsoft.com/en-us/fullnotice.mspx. Last accessed 13 November 2011
[106] Simon Bradshaw. Supra note 72. Page 5
[107] See: Amazon. FAQs "Where is my data stored." Available at: http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored. Last accessed 15 October 2011
[108] Simon Bradshaw. Supra note 72. Page 5
[109] Ibid

Customer's email and Google Message Discovery (GMD) data only in the continental United States. As soon as it shall become commercially feasible, Google shall store and process all other Customer Data, from any other Google Apps applications, only in the continental United States..."[110] It is seems Google provide such arrangement because they are dealing with a government agent which likely possess a bigger bargaining power compared to regular consumers or SMEs.

Closely related to data location is the matter of data protection. Data protection is relevant when customer data is flowing through different jurisdictions. To comply with data protection law, some providers regulate the transfer of personal data to third countries in the T&C.[111] One example is Rackspace that stipulates "*each party agrees to comply with the respective obligations under the Data Protection Act 1998 as applicable to personal data*".[112] Rackspace define their roles when they become a controller or become processor in the light of Data Protection Directive.[113] Rackspace agrees to not provide access to personal data to any subcontractor or affiliate outside of the EEA unless that person meets the requirements of such Directive:[114]

(i) *is located in a country for which the European Commission has made a positive finding of adequacy,*

(ii) *is located in the United States and has certified to the United States Department of Commerce that it adheres to the Safe Harbour framework,*

(iii) *has signed the standard contractual model clauses for the transfer of personal data.*

3.2.3.4 Data Disclosure

In general, there are two conditions in which the provider will disclose data or content to the third party. Some providers assure that data disclosure will only take place based on court orders, whereas others state that they will do so based on business interests.

---

[110] Thomas J. Trappler. "If it's in the Cloud, Get It on Paper: Cloud Computing Contract Issues." Educause Quarterly. Volume 33, Number 2. (2010). Available at: http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532. Last accessed 11 October 2011.
[111] Article 25 of DPD
[112] Article 19 of General Terms. Rackspace. Supra note 82
[113] Article 9 (1) & (2). Ibid
[114] Article 9 (1) Ibid

Elastichost,[115] Flexiant,[116] and Google App,[117] stipulate that data disclosure will be based on court or administrative orders and simply as a measure of compliance with applicable law. A different approach is taken by Microsoft which states "we may also disclose personal information as part of a corporate transaction such as a merger or sale of assets."[118]

Most of the providers do not mention procedures of disclosing data on the basis of court or administrative orders. A cloud study from Centre for Commercial Law Studies found that only Salesforce provides a notification when disclosing data to the third party. T&C for Salesforce provide that the customer will be given advance notice of a requested disclosure, unless such notice is prohibited, and that Salesforce will assist the customer in opposing such orders.[119] On the other hand, Microsoft states: "… *will not disclose your personal information outside of Microsoft and its controlled subsidiaries and affiliates without your consent.*"[120]

It also commonly found that cloud providers do not mention anything about data disclosure in their T&C. Examples of providers that adopt this practice are Iron Mountain,[121] Joyent,[122] or 3Tera.[123] This practice is consistent with the provider's policy in which they hold no duty of confidentiality regarding customer data.[124]

3.2.3.5 Data Preservation

Data preservation covers issues of customer access to the data upon the termination of contract. Cloud providers address this issue utilizing different approaches. Some providers assert that customer's data will be deleted as soon as the relationship between

---

[115] Clause on "Privacy Policy" of ToS. Elastichost. Supranote 75
[116] Clause on "How do we use this information?" of Privacy Policy. Flexiant. Available at: http://www.flexiant.com/about/privacy/. Last accessed 13 November 2011
[117] Article 6 of Google App Agreement. Google. Supra note 73
[118] Clause on "Sharing Your Personal Information" of Privacy Statement. Microsoft. Supra note 105
[119] Simon Bradshaw. Supra note 48. Page 26
[120] Op. Cit Microsoft.
[121] See generally: Client-Software License Agreement. Iron Mountain. Available at: http://ironmountain.com/legal/livevaultc.asp. Last accessed 13 November 2011
[122] See generally: ToS of Joyentcloud. Supra note 59
[123] See generally: ToS of 3Tera. Supra note 101
[124] Simon Bradshaw. Supra note 48. Page 27

customer and provider ends.[125] For providers such as Joyent, Apple and ElasticHosts, the customers are requested to backup their data and thus will not have access to data that is stored on the service after the termination.[126] Some other providers such as 3Tera do not mention anything about what will happen with customer data after the termination. Such conduct surely looks ironic since 3Tera previously have stated that it will use best efforts and commercially reasonable best practices when deploying services related to data integrity, backup, security, and retention.[127]

On the other hand, some providers assert that they will normally preserve customer data for a set period of time following the end of a service contract.[128] Amazon assure that they will not take any action to intentionally erase any of customer data for a period of thirty (30) days after the effective date of termination.[129] Google is not really clear with the time period as they state: "*after a commercially reasonable period of time, Google will delete Customer Data …*"[130] The same case also happens in Facebook that states: "*When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).*"[131]

3.2.4 Applicable Law and Jurisdiction

In the practice, often the choice of law and choice of forum are specified as the place where the service provider has its principal of business or main office. A study from Queen Mary University of London found that around half of the 31 cloud providers choose the law of a particular US state commonly California, but also include Massachusetts, Washington, Utah and Texas.[132]

Some other providers make the choice of law and forum based on the strong presence in a jurisdiction.[133] Salesforce is a good example of this case. In its T&C, Salesforce states

---

[125] Ibid. Page 23
[126] See Supra note 98
[127] Article 10 of ToS. 3Tera. Supra note 101
[128] Simon Bradshaw. Supra note 48. pp.23-25
[129] Article 3.7.2 of Customer Agreement. Amazon. Supra note 51
[130] Article 10.4 of Google App Agreement. Google. Supra note 73
[131] Article 2 2 of Statement of Rights and Responsibilities. Facebook. Supranote 88
[132] Simon Bradshaw. Supra note 48. Page 17
[133] Mark Vincent. Supra note 99. Page 5

that "*any lawsuit arising out of or in connection with this Agreement, and which courts can adjudicate any such lawsuit, depend on where you are domiciled*".[134] At first glance, it looks like this provision implies that Salesforce determine the applicable law and jurisdiction based on the location of the customer. But then Salesforce creates "different zones" of governing law and the courts based on its branch office. So example, if the customer that is residing in Japan made a cloud contract with Salesforce, the governing law and jurisdiction will be in Tokyo.[135] This is due to the fact that Salesforce has a Japanese affiliate called Kabushiki Kaisha.[136] This means a customer who resides in Thailand must travel to Japan if they want to challenge the cloud contract in front of a court.

3.2.5 Contract Termination

Most of the cloud providers (for example Apple,[137] Adrive,[138] Dropbox,[139] Microsoft,[140] etc) claim the right to terminate or suspend for a period of time all or part of services at anytime, with or without cause, and with or without notice. In providers such as Elastichost[141] and Akamai,[142] the termination can only take place when the customer, among others, submits false or misleading information to the provider, or violates Acceptable Use Policy, provision of the Terms of Service or any applicable laws.

There are two important issues for the customer following the end of the relationship with their provider; namely data deletion and data portability. Data deletion is related to the issue whether the provider will assure that data will be deleted from the cloud after the termination stage. As has been discussed earlier in this chapter, some providers choose to preserve customer data for some time, while others choose to delete it immediately. If the provider mentions data deletion in their T&C, they tend to

---

[134] Article 13 (1) of Master Subscription Agreement. Salesforce. Supra note 100
[135] Ibid
[136] Ibid
[137] Article 8 of ToS. Apple iWork Public Beta. Supra note 63
[138] Article 18 of ToS. Adrive. Available at: http://www.adrive.com/terms. Last accessed 13 November 2011
[139] Clause on "Termination" of ToS. Dropbox. Supra note 74
[140] Clause on "Use of Services" of ToS. Microsoft. Supra note 69
[141] Clause on "Termination and Suspension" of ToS. Elastichosts. Supra note 75
[142] Article 6.3 of T&Cs. Akamai. Available at: http://www.akamai.com/dl/akamai/Akamai_Terms_Conditions_2009.pdf. Last accessed 13 November 2011

incorporate it into the termination clause instead of the warranty. Hence there is not a hundred percent guarantee that data will be completely deleted from the cloud.

Moreover, most of the T&C does not mention data portability if customers choose to end the relationship because they want to switch providers. Providers such as Dropbox can only go as far as to ensure the retaining of customer data when the contract is terminated.[143] Whereas Salesforce states that it: "*…will make available for customer to download a file of data in comma separated value (.csv) format ….*"[144] Nevertheless, Salesforce does not explain any further whether such data will be compatible for reuse with another provider.

4 DRAFTING A CLOUD COMPUTING CONTRACT

4.1 Relevant Issues to Address on the Cloud Computing Contract

This section will analyze all the findings presented in previous chapter from the customer's point of view. The approach taken for analysis will be based on legal principles and frameworks that have a bearing on the cloud computing technology. Since most of the terms in cloud computing contract deals with data issues, the analysis on this section will be heavily influenced by data protection regime in the EU.

The purpose of this section is to find whether the clauses commonly presented in the cloud T&C are compatible with the prevailing laws. Subsequently, such purpose will lead to finding whether the existing laws are adequate to address the legal issues associated with cloud computing technology. Therefore, this section does not intend to draft an ideal cloud contract word for word, but rather to provide a legal consideration in drafting fair and reasonable terms in cloud contracts from a customer's point of view.

[143] See: Clause on "Termination" of ToS. Dropbox. Supra note 74
[144] Article 12.5 of Master Subscription Agreement. Salesforce. Supra note 100

4.1.1 Data Security

In terms of technology, cloud computing service is unique and different from the rest of the conventional IT business models. In cloud computing, data flows freely instead of being attached to certain datacenters in physical world. This implies the fact that only cloud providers understand the pattern of data movement within the cloud. The *virtualisation* characteristic in cloud computing technology has created a system where only providers understand the back-end architecture of the cloud. Therefore, cloud providers should also be responsible for the security of the back-end architecture. To this end, the cloud provider must take steps in securing their own cloud service and subsequently the customer's data security by employing appropriate security measures.

The protection regime for personal data in data protection law can serve as a good guide for protection of customer data in cloud computing service. In connection with personal data in cloud computing, many data protection authorities require that each cloud provider must - like any traditional data center – have functioning security architecture and associated management.[145] On their own initiative, providers such as Microsoft have already initiated a project which attempts to strike a balance between security, efficiency and functionality of cloud computing.[146]

Under the DPD, a controller must implement appropriate technical and organizational measures when processing personal data.[147] Applying this rule to cloud computing, will also require the establishment of a notification mechanism for the customer in the case of data security breaches.[148] There is also a need to ensure that such security measures are adequate and properly maintained from time to time. For this purpose, an independent security audit for cloud computing service will be required.

---

[145] See for example the guidelines published by The German Data Protection Authority. Orientierungshilfe – Cloud Computing. (2011) Available at: http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf. Last accessed 30 September 2011

[146] See Microsoft Research. Cloud Cryptography. Available at: http://research.microsoft.com/en-us/projects/cryptocloud/. Last accessed 25 October 2011.

[147] Article 17 of DPD

[148] See European Network and Information Security Agency (ENISA). Cloud Computing Benefits, Risks and Recommendations for Information Security. (2009), Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. Last accessed 18 October 2011. Page 6

Nevertheless, it is seems impossible for a cloud provider to allow a third party to audit their cloud architecture security. One of the reasons for this practice is the protection of trade secrets of the cloud service. None of the cloud T&C ever mention third party involvement in regular security audits. This implies that the creation of standardized security measures in cloud service is out of the cloud contract scope. Therefore, the most reasonable way to solve this problem is by creating a specific provision in which the cloud providers are obligated to provide adequate security measures. After all, fulfilling the role of providing security measures is an obligation which is enshrined in various disciplines of laws.[149]

Providing security as a means of compliance to existing law can be observed from the Google Gmail case. In 2009, EPIC filed a complaint to the US Federal Trade Commission, urging an investigation into Google's cloud computing services to determine the adequacy of privacy and security safeguards.[150] Due to this complaint, Google subsequently established HTTPS by default for their Gmail service.

The customer also has an obligation in regards to security issues of cloud computing service. The front-end architecture of cloud computing, which operate outside the control of cloud providers, become the sole responsibility of the users.[151] To this end, customers must employ an Identity and Access Management System that deals with the authentication such as IDs, passwords, PINs, machine-readable passports, as well as biometrics.[152] In short, the customer must also be responsible for the security of the cloud computing service by using an Identity Management System.[153]

---

[149] For example in the consumer case:
- Implementation of appropriate technical and organizational measures to protect personal data as in article 17 DPD
- General human rights instruments on right to privacy which directly connected to data protection, and
- In directly, also connected to Unfair Terms Directive when a provider excluding its liability and causing a detrimental effect to consumer. See: Annex 1 (q) of Unfair Terms Directive

[150] See: EPIC Org. Cloud computing news. 7 February 2011. Available at: http://epic.org/privacy/cloudcomputing/. Last accessed 27 October 2011.
[151] See generally: Orientierungshilfe. Supra note 145
[152] ENISA. Supra note 148. Page 67
[153] Ibid

The cloud provider needs to set forth expressly in the cloud contract a provision in which a customer's must employ security measures when accessing or using the cloud service. Such a provision will provide a clear division of responsibilities regarding the security measures for both parties in the cloud service. This effort will make it easier to determine which party is responsible if there is any security breach such as unlawful access by a third party in the cloud service.

4.1.2 Terms Related to Cloud Service Provider

Cloud providers often disclaim liability in relation to service availability. Such denials are enshrined in contract clauses which relate to the performance of service from the provider's side. The answer to this problem lies within the characteristic of the cloud computing technology itself. Reliability is one of the core features of cloud computing technology. Reliability denotes the capability to ensure constant operation of the system without disruption, i.e. no loss of data, no code reset during execution etc.[154] If that characteristic is an inherent part of cloud computing technology, and not just serves as cloud service marketing campaign, then it should not be so difficult for cloud provider to give a guarantee of the service availability, as it is already become an inherent characteristic of cloud technology.

Thus, having an obligation to secure data and combined with the guarantee for the service availability, will certainly make providers present more reasonable terms regarding their responsibilities in the cloud contract. Controversial T&C provisions which relate to the denial of service availability will likely diminish since a clause on disclaimer will only be limited to justified events as elaborated in the force majeure clause. With the clear role in security and data availability, providers will design a clause of limitation of liability solely to the loss that cannot be addressed through reasonable efforts. It is worth noting that, following discussions with the UK Office of Fair Trading, Apple agreed in the late 2009 to revise the T&C for its iTunes music service, in particular for terms that sought to exclude liability for faulty services.[155]

---

[154] Expert Group Report. Supra Note 4. Page 13
[155] Simon Bradshaw. Supra note 48. Page 33

Attempts to resolve liability arising from electronic contracts is not something new and emerged only after the cloud computing service. Many cloud providers have a background in hosting and internet service provision, where an arms-length relationship with customers, reinforced by broad contractual disclaimers, is commonplace.[156] Moreover, many cloud providers are based in the United States, and therefore operate within a legal culture that tends to have a more laissez-faire approach to, for example, exclusion and limitation of liabilities, than is typically the case in Europe.[157]

In practice, a cloud provider can promote and justify that data monitoring is needed to ensure the quality of cloud service. This is contradictory with another clauses in the cloud contract in which they disclaim any warranties/guarantees for the service quality. Another common problem found in cloud practice is the existence of contract clauses in which the providers claim the right to amend the contract unilaterally and also a disclaimer for third party services or products.

Despite of these broad disclaimers, other cloud providers are taking different approaches and are able to present a T&C with many of its clauses that are not detrimental to its customer. Some providers are able to ensure that variation to terms will only happen with the customer's consent. Some providers are also able to ensure the quality of cloud service. This fact indicates that the ongoing detrimental practice in cloud service has no technological justifications. To this end, the common problem in which cloud providers sought to resolve their liability do emerged from the architecture of cloud computing technology. It is emerges because the providers choose to present a T&C in such a manner at the first place.

The existences of unfair terms in cloud T&C can surely be challenged using existing laws. For a consumer, in some U.S. states, in E.U. countries and in various other jurisdictions; the validity of such terms may be challenged under consumer protection laws.[158] For customers who are a SMEs or corporations there are no legal frameworks dedicated specially to ensure the inapplicability of detrimental terms as in the consumer

[156] Simon Bradshaw. Supra note 72. Page 10
[157] Ibid
[158] Simon Bradshaw. Supra note 72. Page 2

case. However, referring to enforceability of a standard-form contract as we already discussed in the chapter II, a cloud customer from the US, for example, can use the doctrine of unconscionability to challenge the validity of some terms of the T&C.

Furthermore, cloud providers must also employ notification procedures for important events that are affecting legal interests of customers. Such notification must be set forth expressly as one of the contract clauses and is available in the event of security breach, data breach, data disclosure or contract termination.

In the case of a data breach, a notification must not only inform the customer about the accident, but must also elaborate all measures that have been taken to prevent or to address the breaches, the potential impacts of the breach on the customer's interests and also advise on possible remedies. Good example of notification of data breaches can be observed from the Sony PlayStation case (August 2011) when personal information of millions of users was stolen from the Playstation Network (PSN) and Sony Online Entertainment (SOE) system.[159]

4.1.3 Terms Related to Data

4.1.3.1 Ownership over data

Cloud providers generally respect and in some cases also protect the ownership of data or content of the customer available in the cloud service. This fact indicates that legal frameworks on intellectual property law such as Berne convention (related to the rightful owner data or content uploaded or in the cloud),[160] Database Directive (related to protection of database as in data storage service of SaaS level),[161] Computer Software Directive (related to protection of software develop in the PaaS level),[162] are still applicable in the cloud computing case.

---

[159] BBC News. Sony's PlayStation Hack Apology. 27 April 2011. Available at: http://www.bbc.co.uk/news/technology-13206004. Last accessed 26 October 2011

[160] Article 2 of Berne Convention for the Protection of Literary and Artistic Works

[161] Article 3 of the Directive 96/9/EC on the Legal Protection of Databases, which stipulates copyright remains an appropriate form of exclusive right for authors who have created databases.

[162] Article 1 (3) of Directive 2009/24/EC on the Legal Protection of Computer Programs, which requires a computer program to be the author's "own intellectual creation" to qualify for protection by copyright.

One exception in this area is Facebook, which does not mention anything about the purpose and condition when they are use IP content of the customer. It is worth noting that currently Facebook is facing a class action litigation in the US court concerning Facebook "Beacon" program which is designed to allow users to share information with selected friends about actions taken on affiliated, third-party Web sites.[163] Plaintiffs claimed inadequate notice or choice about how Facebook and its affiliates collected information about Web-browsing activity before publication on Facebook.[164]

Another issue that needs to be addressed is the issue of the ownership of various types of information emanating from the interaction of the user in the cloud service. According to Chris Reef; "*information generated by the provider for its own internal purposes, such as billing or management of its Cloud, will belong to the provider*".[165] He stated that the providers need to give special attention to the principle of equity when gathering such information.[166] Such principles require the provider - who gathered or received the information in confidence - not to take unfair advantage. If the provider does not inform the customer that their information will be used in such way, that failure amounts to unfair conduct in the context of the confidential relationship.[167] If the information gathering also involves customer's data that is protected by copyright, they will need a license from the customer to copy such data.[168] Using this approach, information gathering by providers can be justified only when there is a clear purpose, does not serve as a means to take unfair advantage and respects copyrighted works that belong to customer.

---

[163] McCall v. Facebook, Inc., No. 10-16380 (9th Cir. filed June 23, 2010). In Mark H. Wittow (2011)
[164] Mark H. Wittow. Cloud Computing: Recent Cases and Anticipating New Types of Claims. The Computer and Internet Lawyer Vol 28 No.I (2011). Available at: http://www.klgates.com/files/Publication/5d61b5e9-ad6f-4d6a-985c-30cb6b84dae2/Presentation/PublicationAttachment/42137be3-c03c-4c58-a527-31d872b78ec5/Wittow_CloudComputing_Jan2011.pdf. Last accessed 29 October 2011. Page 6
[165] Chris Reed. Information 'Ownership' in the Cloud (March 2, 2010). Queen Mary School of Law Legal Studies Research Paper No. 45/2010. Available at SSRN: http://ssrn.com/abstract=1562461. Last accessed 20 October 2011. Page 17
[166] Ibid. Page 18
[167] Ibid
[168] Ibid. Page 19

A recent case on copyright infringement in cloud computing is Cartoon Network v. CSC Holdings, Inc.[169] This case attempted to solve whether momentary data stream can be constituted as a copy in the sense of copyright protection. Cartoon Network sought for a judgment on whether Cablevision's cloud-based remote storage digital video recorder system, more commonly known as an "RS-DVR", violated their respective copyrights.[170] The court reasoned that the data which contained the copyrighted programs, and which was moved to "buffers" to allow customers to record the program on the RS-DVR, only remained in the buffers for a very short period of time and was automatically overwritten as soon as it was processed. As such; the data was not "fixed" as is required to qualify as a "copy" under the Copyright Act.[171]

4.1.3.2 Data Integrity and Data Availability

Data integrity is closely connected to data availability and they both become the most important elements in the provision of cloud computing services. Diminish the quality level of data integrity and data availability can cause fatal effects to cloud customer. An example of this case is Amazon EC2 which had a service outage on April 2011 and became the worst case in cloud computing history.[172]

In current market practice, most of the cloud providers attempt to resolve any liability regarding data integrity and availability. This practice seems contradictory with the cloud architecture that enables them to provide ample opportunities to design systems to withstand failures.[173] One of the main the characteristics of cloud computing is the ability to introduce redundancy for services and data so failures can be masked transparently.[174] This characteristic implies that a rejection to ensure data integrity and availability will also means a rejection to the capability of cloud computing technology itself.

---

[169] Decision 536 F.3d 121 (2008). United States Court of Appeals for the Second Circuit.
[170] Fernando Pinguelo & Bradford Muller. Avoid the Rainy Day: Survey of U.S. Cloud Computing Caselaw. (2011) Boston College Intellectual Property & Technology Forum. Available at: http://bciptf.org/wp-content/uploads/2011/07/1-AVOID-THE-RAINY-DAY.pdf. Last accessed 20 October 2011. Page 3
[171] Ibid
[172] For detail of the case, see: Thorsten. Amazon EC2 Outage: Summary and Lessons Learned. Available at: http://blog.rightscale.com/2011/04/25/amazon-ec2-outage-summary-and-lessons-learned/. Last accessed 26 October 2011
[173] Ibid
[174] Expert Group Report. Supra note 4. Page 14

Data Protection law provides a good approach on how to maintain data integrity and data availability. Duty of integrity implies that cloud provider must be able to implement appropriate technical and organizational measures to protect customer data against accidental or unlawful destruction or accidental loss.[175] Duty of availability implies that cloud provider must be able to ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed and that all operations can be eventually reinstituted in a timely and organized manner.[176]

Data integrity and data availability must become an integral responsibility of the cloud provider and should be set forth expressly in the warranty clause of the cloud contract. Limitation of liability to data integrity and data availability must be limited only to events where cloud providers already gave their "best commercial effort" and solely on the grounds of the events that are set forth in force majeure clause such as denial of service attacks, equipment outages, and natural disasters.

4.1.3.3 Data Disclosure

Data disclosure is permissible only when it is based on the justified grounds such as court or administrative order and compliance with applicable law.[177] The cloud provider must dedicate a specific clause that elaborates in detail procedures and conditions for data disclosure. Such clause must ensure that the customer will receive a notification in each request for data disclosure by a third party. To date, only Salesforce provides the customer with advanced notification for a requested disclosure.

In the US, mere notification does not mean the provider can disclose data to the court. In this case, the customer must also give his direct consent for data disclosure. In

---

[175] See article 17 of DPD

[176] Wayne Jansen & Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (2011). Available at: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf. Last accessed 26 October 2011. Page 37

[177] In the US, data disclosure is based on Electronic Communications Privacy Act of 1986 (ECPA). Particularly on the § 2702 of Voluntary Disclosure of Customer Communications or Records.

Suzlon Energy Ltd v. Microsoft Corporation,[178] the court decided that Hotmail service (cloud based email provider) was not allowed to disclose the customer's data even if it is based on court order - provided that that customer did not give his direct consent in the first place. Moreover, the Court held that the protections of the Electronic Communications Privacy Act (ECPA) against unrestricted disclosure of emails by an electronic communication service provider apply to non-U.S. nationals as well as to U.S. citizens.[179] The same approach has been taken by the US District Court of Northern District of California when deciding the case of Suzlon Energy Ltd v. Google Inc.'s.[180]

Providers such as Microsoft choose to disclose customer data on the grounds of operation of internet businesses. In disclosing customer data for the purpose of business, the provider has to ensure that it will not cause a detrimental effect to confidential data. Thus, particular attention must be given to types of data which have been stated clearly by the customer as intellectual property works. One of the most relevant issues in this regard would be trade secrets. In this case, the provider must ensure that the protection given to customer must be at the minimum threshold as set forth by article 39 (2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights.[181]

To date, there are no specific procedures and conditions of data disclosure in cloud service that must be followed by the cloud providers. The DPD address some issues on data disclosures but such provisions are only applicable to personal data and not to all

[178] No. 10-35793. D.C. No. 2:10-cv-0170-MJP. The Ninth Circuit Court of Appeals of the US.
[179] K&L Gates. Cloud Computing Case Clarifies Applicability of US Privacy Law to Non-U.S. Nationals. (2010) Available at: http://www.tmtlawwatch.com/2011/10/articles/cloud-computing-case-clarifies-applicability-of-us-privacy-law-to-nonus-nationals/. Last accessed 29 October 2011.
[180] See the decision on: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2010mc80034/224153/31/0.pdf
[181] Protection must be given to information which:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and
(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

the data that is available in the cloud service.[182] Therefore, the potential customer of the cloud provider should carefully analyze the confidentiality/non-disclosure clause to determine whether the cloud provider offers sufficient guarantees to protect the customer's secret information and know how it will circulate in the cloud.[183]

4.1.3.4 Data Location

Cloud practice indicates the possibility of offering cloud service in which the customer's data will be attached to a particular location. One can argue that setting data location in cloud service will be expensive. The $7.2 million contract of Google App. with Los Angeles city administration can be use to support this argument.[184] Furthermore, one can also argue that Los Angeles city administration is a governmental body and therefore has a strong bargaining position in contract negotiation. Regardless of such arguments, this contract implies that setting up a data location in cloud service is possible. There is no evidence that setting data location in cloud service deprives the *Elasticity* characteristic of cloud computing.[185]

Amazon EC2 is offered with the ability to place data in multiple locations in separate geographic areas or countries. By setting up Availability Zones, Amazon are able to: "*… set data in the locations that are engineered to be insulated from failures in other Availability Zones and also providing inexpensive, low latency network connectivity to other Availability Zones in the same region.*"[186] According to Amazon, by launching instances in separate Availability Zones, customer will be able to protect their applications from failure within a single location.[187] Amazon EC2 is currently available in six regions: US East (Northern Virginia), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), and AWS GovCloud.[188]

---

[182] See article 16 of the DPD
[183] ENISA. Supra note 148. Page 108
[184] C.Net. News. LA Approves $7.2 Million Google Apps deal. 27 October 2009. Available at: http://news.cnet.com/8301-27080_3-10384433-245.html. Last accessed 20 October 2011
[185] Compare: Bob Warfield. Gartner: The Cloud is Not a Contract.12 January 2011. Available at: http://www.enterpriseirregulars.com/31367/gartner-the-cloud-is-not-a-contract/. Last accessed 28 October 2011
[186] Amazon Web Service. Amazon Elastic Compute Cloud (Amazon EC2). Available at: http://aws.amazon.com/ec2/. Last accessed 20 October 2011.
[187] Ibid
[188] Ibid

Unlike Google App., Amazon does not provide the setting of data location only for government agents or based on negotiation. Their offers are available to regular customers and also come with a reasonable service price. Using the logic from the Amazon EC2 Availability Zones, and presuming that providing data location is not so expensive, then why do not the other providers follow this approach? Not necessarily to fulfill any legal principles, setting up a data location is arguably helpful to prevent single location failure such as promoted by Amazon.

It is worth noting that the German Data protection Authority recently issued a guidance paper on cloud computing which calls on the cloud provider to have "*transparent, detailed and unambiguous contractual provisions regarding the processing of data in the cloud, in particular regarding the location of data processing and notification about possible changes to the locations where cloud data may be processed*".[189]

4.1.4 Data Protection Issues

From all the relevant legal implications associated with cloud computing technology, the greatest implications lie in the field of data protection law. The following are a few of the data protection law issues associated with cloud computing.

4.1.4.1 Contract Alteration and the Essence of Controlling under DPD

In a PaaS contract scenario, a customer who collects personal data would be a controller according to the DPD. As a controller, they will determine the purposes and means of the processing of personal data.[190] The DPD describes broad definitions, principles and measures for controllers to comply with when acting as a controller.[191] A cloud provider, on the other hand, would be a processor since they are processing such personal data on behalf of the customer/controller.[192]

---

[189] Privacy and Information Law Blog. German DPAs Issue Resolution and Guidance Paper on Cloud Computing and Compliance with Data Protection Law. Hunton & Williams LLP. (2011). Available at: http://www.huntonprivacyblog.com/2011/10/articles/german-dpas-issue-resolution-and-guidance-paper-on-cloud-computing-and-compliance-with-data-protection-law/. Last accessed 26 October 2011
[190] Article 2 (d) of DPD
[191] Article 6, 7, 8, 9 , 10 & 11 of DPD
[192] Article 2 (e) of DPD

Provisions on collecting customer data are generally mentioned in ToS and Privacy Policy. When a cloud provider claims a right to amend the T&C on their own discretion, the exercising of controlling function of the personal data by the controller will be diminished. In this scenario, cloud provider is the only party who determines the overall aspect of the cloud contract including the provisions that have a bearing on personal data. This practice is against the provision of the DPD in which a processor may solely act on the instructions of the controller.[193]

On the other hand, even if the cloud contract is negotiated, the customer/controller must always determine the course of provisions regarding the protection of end-user personal data. They have a duty to ensure that the whole policy of the cloud provider will be compatible to support their role as the controller under the meaning of DPD. On the basis of this interest, the approach adopted by Rackspace which stipulates that each party agrees to comply with the respective obligations under the Data Protection Act 1998, does not seem detailed enough to draw a conclusion that customer has full control over the course of processing personal data.

The right of providers to unilaterally change the contract terms has made some data protection authorities choose not to recommend cloud computing as solution for processing personal data. This is appeared in the Danish Data Protection Agency's opinions for the Odense Municipality's case.[194] In this case, Odense Municipality wanted to use Google Apps online office suite to process the personal data of their students. The Danish Data Protection Agency's viewed that Google App. can unilaterally change the agreement terms and therefore, Odense Municipality, in reality, has no control of how the data will be processed.[195]

4.1.4.2 Data Location and Security Measures

The DPD states that controllers must "… *choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures*

[193] Ibid
[194] The Danish Data Protection Agency. Processing of Sensitive Personal Data in a Cloud Solution. J.no. 2010-52-0138. (2011). Available at: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/. Last accessed 26 October 2011
[195] Section 5.3.1. The Act on Processing of Personal Data's Requirements on Instructions and Processor Agreement. Ibid

governing the processing to be carried out, and must ensure compliance with those measures."[196] In the conventional IT business models, the technology allows the abstraction of the location of personal data which is processed by the processor on behalf of the controller. This is different with cloud computing, because here; personal data will flow freely between datacenters and subsequently, data can be located in multiple jurisdictions. As a consequence, the customer/controller will be required to monitor the compliance of technical security measures in each of data centers.[197]

Even if cloud providers are able to ensure the compliance to DPD rules on trans-border data flows and enlist one of the companies in the Safe Harbor Agreement,[198] it is still difficult to see that customer/controller is able to assess the level of encryption employed by the provider during the transfer of data between datacenters.[199] Moreover, it is also difficult to see that customer will have effective means to ensure the adequate protection of personal data in data centers located on another continent.[200]

4.1.4.3 Data Encryption for Personal Data

Personal data means any information relating to an identified or identifiable natural person.[201] When a customer/controller chooses to secure the personal data with a strong encryption system before uploading to the provider site, it will make the likeliness of identification of personal data become less identifiable to the provider. The customer/controller who uploads encrypted data into the SaaS will also presumably have the access for decrypting such data. Therefore, information that is secured with a strong encryption will be outside the cloud provider's knowledge. The provider might further secure such data through another layer of encryption. In this case, such data will be treated in the same manner as any other customer's data in the cloud service.

The problem arises when a customer encrypts and also decrypts a personal data inside the cloud by utilizing encryption resources provided by the cloud provider. If

---

[196] Article 17 (2) of DPD
[197] See also Section 5.3.1. The Act on Processing of Personal Data's Requirements on Instructions and Processor Agreement. Op. Cit. The Danish Data Protection Agency.
[198] Article 25 (1) and (2) of DPD
[199] Section 7.2. Transmission and Login. The Danish Data Protection Agency. Supra note 194.
[200] Ibid
[201] Article 2 (a) of DPD

decryption occurs on the cloud provider's servers, theoretically it could access the decrypted data and identify data subjects.[202] Thus, data - even if not "personal data" - while in encrypted form in the cloud, could become "personal data" when decrypted for use in a cloud application.[203] It seems unsatisfactory that the cloud provider's status should vary with the strength of encryption or anonymisation techniques used by its customer, of which it may have no knowledge or control.[204]

4.1.4.4 Defining the Cloud Provider Roles under DPD

Customers who use cloud service from a SaaS provider for processing personal data will become a controller. The SaaS provider in this case will become the processor. In providing their service, the SaaS provider/processor will utilize a cloud service from PaaS or IaaS providers. Defining the limit of liability of PaaS or IaaS providers in this case would be really important since it will also determine whether they should be held accountable for the processing of personal data that is located within their infrastructure. With the possible layers of providers and sub-providers in cloud computing, it's often unclear which party determines (and to what extent) the "means" of processing personal data in the cloud.[205]

IaaS or PaaS providers are generally not aware or have actual knowledge of information contained in their customers' data that is processed using their cloud platform. A recent study from Queen Mary University suggest that: "Just as web hosts lose their defenses on acquiring the appropriate knowledge and control, infrastructure providers should not be treated as "processors" of any personal data processed using their services, unless and until they gain sufficient knowledge and control (access)."[206] To this end, since the nature of service offered on the IaaS or PaaS level are similar to providing a regular hosting service, it is seems more suitable to determine their roles by using the E-

---

[202] Kuan Hon. Supra note 16
[203] Ibid
[204] Kuan Hon, Christopher Millard and Ian Walden. "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing Part 2." Queen Mary School of Law Legal Studies Research Paper No. 77/2011. Available at SSRN: http://ssrn.com/abstract=1794130. Last accessed 26 October 2011. Page 18
[205] Kuan Hon. "Who's responsible for personal data in cloud computing?" On Computerblog UK, 23 May 2011. Available at: http://blogs.computerworlduk.com/cloud-vision/2011/05/whos-responsible-for-personal-data-in-cloud-computing/index.htm. Last accessed 26 October 2011
[206] Ibid

commerce Directive. Therefore, instead of applying the DPD, it is more appropriate to consider the limits of their liability based on *Mere Conduit* principles enshrined in article 14 of E-commerce Directive.[207]

The legal issues of data protection in cloud computing will not be solved by relying on market practice. Since all the problems mentioned above lie outside of the cloud contract scope, efforts by cloud providers that clearly state their compliance to DPD rules will still be useless. Considering this fact, it seems the existing laws regulating data protection in the EU are not enough to address relevant personal data issues of cloud computing.[208] Currently, the DPD is under revision and hopefully a newer version will be able to address those problems.[209]

4.1.5 Applicable Law and Jurisdiction

A survey on market practice indicated that cloud providers have always included the clauses of forum of choice and forum of law in the T&C.[210] Most cloud providers claim that the contracts are subject to the laws of the jurisdiction where they have their main place of business.[211] This provision will have different consequences for customer who is acting as consumer or as corporate entity.

For a consumer in the EU, this provision can be challenged under the consumer protection legal frameworks. Rome I regulates that the contract shall be governed by the law of the country where the consumer has his habitual residence,[212] provided that the

---

[207] Article 14 on Hosting read as follow:
Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[208] Article 29 Working Party recently released opinion on the concepts of "controller" and "processor" (Opinion 1/2010, adopted on 16 February 2010.) This opinion is an attempt to address the issue of cloud computing. According to Kuan Hon, this opinion useful to some extent but still leaves a grey area. See further study on Kuan Hon. Supra note 205. Page 11

[209] See European Commission webpage: http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

[210] See section 3.2.4 of this thesis

[211] For a view on the pattern of jurisdiction choice on cloud contract, see: Simon Bradshaw. Supra note 49. pp.17

[212] See Article 6 of Rome I

professional pursues his commercial or professional activities in that country,[213] or if the establishment is outside the EU,[214] directs such activities to that country or to several countries including that country.[215] Furthermore, based on the Brussels Regulation I, consumers may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.[216] Finally, based on the Unfair Terms Directive, a contract provision on applicable law and jurisdiction shall be regarded as unfair if,[217] it excludes or hinders the consumer's right to take legal action or exercise any other legal remedy.[218]

The provision of choice of law is greatly important for customer who is an SME or corporation. Under the regulation of Rome I which has international applicability,[219] a contract shall be governed by the law chosen by the parties.[220] The choice shall be made expressly and clearly demonstrated by the terms of the contract or the circumstances of the case.[221] Application of this rule in the cloud service will require the customer to surrender to the clause of choice of forum/law which is solely drafted by the cloud provider. In this case, it will be the law of the country where provider has its establishment. Therefore, customers will find themselves being expected to travel to a court in another state or even country to argue a claim under commercial law with which they may not be familiar.[222]

Cloud computing technology poses a serious problem in the case of the absence of choice of law in a cloud contract that is concluded within the EU. Applying Brussels I in this case means that cloud providers may be sued in the courts for the place of performance of the obligation in question,[223] and in the case of the provision of

---

[213] Ibid Article 6 (1) a of Rome I
[214] "The concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period." Case C-221/89 Factortame [1991] ECR I-3905 §20
[215] Article 6 (1) b of Rome I
[216] Article 16 (1) of Brussels I
[217] Article 3 (1) of Unfair Terms Directive
[218] Annex 1 (q) of Unfair Terms Directive
[219] Article 2 of Rome I
[220] Freedom of Choice. Article 3 of Rome I
[221] Ibid
[222] Simon Bradshaw. Supra note 72. Page 5
[223] Article 5 of Brussels I

services, the place in a Member State where, under the contract, the services were provided or should have been provided.[224]

In cloud computing contracts, adopting the place of performance refers to place where the service is performed by software operating automatically or where performance occurs on a server located in a jurisdiction different to that which the website is stored.[225] Applying the place of performance in the cloud contract will be difficult since both the cloud service and the server of the cloud provider are located in the cloud.

Therefore in case of cloud services, it is extremely difficult, if not impossible, to assess the place of provision of the services.[226] It is seems the existing law unable to properly address this issue. To this end, criteria for determining when cloud provider is to be considered 'established' in the EU should be clear, and harmonized across the EU.[227] In solving legal cases similar to this problem, the courts must be able to find a solution that makes sense from the technological and legal point of view.[228] In the long term, there is a strong need to ensure that cloud providers will always mention provision of applicable law and jurisdiction in the cloud contract.

4.1.6 Contract Termination

Not only claiming the right to terminate contracts in any given time, most of the cloud providers also do not provide a notification for termination events. Notification is important for customers in order to have adequate time to arrange their data. In cloud practice, termination policy in which the provider requests the customer to handle their own data interests in the event of termination, can still be justified as long the provider presents an advance notice to the customer and such notification must consist of information on the time period given to customer to arrange their data and also a reminder to save data for one last time before the termination.

---

[224] Article 5 1 (b) of Brussel I
[225] Anassutzi & Co. "Jurisdiction and Law Issues in Cloud Computing Agreements" Available at: http://www.anassutzi.com/articles/185-jurisdiction-and-law-issues-in-cloud-computing-agreements.html. Last accessed 12 September 2011
[226] Davide Parrilli. Supra note 24. pp.107-108
[227] Queen Mary University. "Cloud Legal Project Response to European Commission Cloud Computing Consultation" Available at: http://www.cloudlegal.ccls.qmul.ac.uk/Research/55027.html. Last accessed 26 October 2011.
[228] Davide Parrilli. Supra note 24. pp.107-108

In relation to data deletion after contract termination, current practice mirrors existing concerns about the difficulty in ensuring that sensitive data is purged from magnetic media.[229] None of the cloud providers guarantee that data will be deleted in a fashion that it is no longer possible to be read or recreated. In the case of Odense Municipality and Google App., the Danish Data Protection Agency view that it is impossible to assess whether the deletion of data media at Google Ireland Limited's and Google Inc.'s data centers is adequate.[230] In this case, the Agency finds it unclear whether the data is deleted in such a way that they cannot possibly be recreated from Google's servers.[231]

Regarding data interoperability, the practice indicates a lack of standard in relation to guaranteeing data portability if the customer wants to use another cloud service after contract termination. Supplying standard data import/export tools and interfaces would ease the fear of being held captive to a provider.[232] The EU identifies data interoperability as one of the most important issues in utilizing clouds for the benefit of single market agenda.[233]

Significant efforts have been taken to address the interoperability issue. In 2009, EuroCloud, backed by more than 30 leading cloud computing vendors, was established to promote the development of standards in cloud computing across the EU.[234] Industry professionals were coalesced to form several bodies like the Open Web Foundation (2008) that promotes the development and protection of open, non-proprietary specifications for web technologies.[235] The manifesto of Open Web Foundation states

---

[229] Simon Bradshaw. Supra note 48. Page 26
[230] Section 6.3 Deletion of Personal Data. The Danish Data Protection Agency. Supra note 196
[231] Ibid
[232] World Economic Forum. "Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation" (2010). Available at: World Economic Forum. Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation. Last accessed 16 November 2011. Page 17
[233] See the opinion of Neelie Kroes (Vice-President of the European Commission). European Cloud Computing Strategy Needs to Aim High. (2011). Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/199&format=HTML&aged=1&language=EN&guiLanguage=en. Last Accessed 26 October 2011
[234] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay & and Juheng Zhang. "Cloud Computing: The Business Perspective" (2009). Available at SSRN: http://ssrn.com/abstract=1413545. Last accessed 19 October 2011. Page 14
[235] Ibid

that cloud providers must not use their market position to lock customers into their particular platforms and limiting their choice of providers.[236] There are also initiatives from cloud providers to provide better interoperability for users when they want to move their data in and out of provider services.[237]

4.2 Contract Negotiation vs. Due Diligence

In the second chapter we discussed that cloud computing contracts are usually presented in a standard-form contract. A standard-form contract will be enforceable when it fulfills the requirements on content, incorporations of terms and information duties.[238] Contrary to this requirement, current practice indicates that cloud contracts are frequently presented in an unfair manner toward the customer. In the cloud contract, the customer must accept the terms even if the customer realizes that such terms are inconspicuous and deprive his reasonable right(s). Surely, customers can always leave by clicking "no" to the click-wrap contract and start looking for another cloud provider. Rejecting one cloud provider offer will open a possibility to choose another cloud provider. Therefore, as opposed to contract negotiation, a customer can always employ careful due diligence to find a suitable cloud provider. In this case, the customer must ensure that due diligence will not merely based on economic criteria but also based on the legal considerations and most importantly security aspects of the cloud service.

Risk mitigation is a step in due diligence that requires the customer to carefully select the cloud provider on the basis of its reputation, professionalism, or its technical skills.[239] The customer also needs to make a thorough assessment of the provisions of the cloud T&C and the legal consequences that it might entail. Finally, customers also need to consider the effectiveness of security systems by making a comparison between the cloud providers.

---

[236] The Open Cloud Manifesto. Draft 1.0.9. Available at: http://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf. Last accessed 18 October 2011.
[237] See: Google Data Liberation Front on http://www.dataliberation.org/. Last accessed 18 October 2011.
[238] See Section 2.5 of this thesis
[239] Balboni, Paolo, Data Protection and Data Security Issues Related to Cloud Computing in the EU (August 18, 2010). Tilburg Law School Research Paper No. 022/2010. Available at SSRN: http://ssrn.com/abstract=1661437. Last accessed 29 October 2011. Page 3

It is understandable that reading a cloud T&C is not an easy task and some customers might find it confusing, but a recent study found that customers actually spend their time reading the electronic contract terms presented to them.[240] The growing number of more aware costumer will play significant part in shaping the cloud computing into a better law-friendly technology.[241]

The market competition among the cloud providers will also shape cloud computing into a better practice. The intense drive to capture market share in the electronic world makes e-businesses highly sensitive to their reputations.[242] When the customer becomes more aware and use the provider's reputation, security and potential legal risks as a market differentiator, the provider will also be driven to improve the security practices and present a fair and just T&C.[243] In the end, the intense focus on reputation created by the e-business environment diminishes the likelihood that e-businesses will offer inefficient terms in their standard forms.[244]

5 CONCLUSION

Cloud computing technology has created impacts towards the application of the existing laws mainly in the field of data protection law and also in the field of jurisdictions and applicable law to the cloud contract. The previous chapter indicates that some provisions in data protection law are inapplicable in cloud computing cases since it has some new technological features that lie outside the scope of data protection law. The place of performance as the means to determine applicable law for contract in the absence of choice of law is also inadequate in its application in cloud computing contracts since the boundaries established by such laws does not fit with the

[240] See generally: Shmuel Becher & Esther Unger-Aviram. "The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction" DePaul Bus. & Comm. L.J. 199 (2010). Available at: https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=8+DePaul+Bus.+%26+Comm.+L.J.+199&srctype=smi&srcid=3B15&key=7b33ab519c475d164d0a5758cb666e74. Last Accessed: 26 October 2011
[241] Ibid
[242] Robert Hillman. Supra note 27. Page 42
[243] Compare: ENISA. Supra note 148. Page 8
[244] Robert Hillman. Supra note 27. Page 43

technological features of cloud computing. This implies that some fields of law that have a bearing on cloud computing need to be revised in order to adequately address legal issues associated with such technology.

The relative immaturity of the market for the cloud computing services is reflected in contracts that are currently in widespread use which include many clauses that appear to be inappropriate and or unenforceable and in some cases illegal.[245] Such practice does not have any relationship with the novelty of cloud computing technology, but mainly emerges because the cloud providers try to resolve the liability arising from the cloud contracts. To this end, the existing laws regulating contractual relationships in electronic contracts are still adequate to challenge such detrimental practice.

Due to the special characteristics of the cloud computing technology, there is a strong need to harmonize standard-form contracts in cloud service by setting up uniform rules regulating cloud practice. Policy makers should give attention to ensure that cloud providers are responsible in providing adequate security measures, as well as having a duty on data availability and integrity, and also providing a notification particularly in the matter of data breach, data disclosure and termination of contract. The most reasonable approach in setting up standards on cloud practice is passing a legislation such as adopted in data protection regime. An example of such legislation is the EU Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries.[246] The annex to this decision is dedicated to regulate standard contractual clauses that must be used in the contract for processors in third countries.

There are also subject matters that have great benefits to boost the customer's confidence for entering a contract but currently lie outside the scope of a standard-form contract. Such issues mainly include the need to ensure the business continuity of cloud

---

[245] Christopher Millard. "Cloud computing: Identifying and Managing Legal Risks" Google / Oxford Internet Institution. (2011). Available at: http://www.slideshare.net/CloudLegal/millard-cloud-computing-key-legal-and-regulatory-challenges-oiigoogle-lecture-brussels-feb-2011. Last accessed 31October 2011. Page 8

[246] Commission Decision No. 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries

providers or disaster planning in the cloud service, the need to audit or validate the security provided by the cloud service provider or the need to ensure interoperability between the cloud providers. Those measures have to be standardized throughout cloud computing contracts as it is almost impossible to rely on the solutions of the market practice or expect the cloud provider to incorporate such matters it in the cloud contract.

The creation of uniform contractual clauses applicable to cloud computing service will give benefits to all the parties involved in the cloud service. In the cloud provider's case, instead of being hostile against the providers, uniformity will serve as the way out from complicated problems in providing a cloud contract which is compatible with prevailing laws. In addition, the likelihood of encountering legal problems in front of court, brought to on the grounds of lack of applicability of the cloud contract, will also diminish. A standardized cloud contract will eventually drive the cloud providers to compete better in providing service to customers. At this stage, providers will only focus on issues of better marketing service and maintaining the customer. Customers will find themselves in a solid framework guaranteeing better protection when engaging in cloud contract. The customer will be able to choose the provider based on its service reliability and reputation and doing so without having to worry about entering a detrimental cloud contract. Finally, stable cloud computing market and standardized cloud practice will simplify and accelerate the cross border business activities and overall will help achieve a single market agenda.

In the latest development of cloud computing issues on the European level, the EU commission has held a public consultation on cloud computing which consists of all parties involved in cloud computing technology. This consultation is part of EU strategy to analyze and plan for future actions on cloud computing with the expected result to be announced in early 2012. There are three broad areas for the cloud strategy: the legal framework, technical and commercial fundamentals, as well as the market.[247] Addressing the issue of contractual relationships between the cloud provider and consumer in cloud computing service shall obviously become an integral part of the legal framework strategy.

[247] Neelie Kroes. Supra note 233

REFERENCE TABLE

International Conventions and European Union Directives

Agreement on Trade-Related Aspects of Intellectual Property Rights (1994) of World Trade Organization (WTO). Adopted on April 15, 1994 at Marrakesh. Entry into Force on January 1, 1995.

Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886.

Council Regulation *(*EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters. Official Journal L 012, 16/01/2001 P. 0001 - 0023

Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts. Official Journal L 095, 21/04/1993 P. 0029 - 0034.

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. Official Journal L 281, 23/11/1995 P. 0031 - 0050

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases. OJ L 77, 27.3.1996, p. 20–28

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts. OJ L 144, 4.6.1997, p. 19–27

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Official Journal L 201, 31/07/2002 P. 0037 - 0047

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs. Official Journal L 111 , 05/05/2009 P. 0016 - 0022

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I**).** Official Journal L 177, 04/07/2008 P. 0006 - 0016

Others

Article 29 Working Party opinion on the concepts of "controller" and "processor" (Opinion 1/2010, adopted on 16 February 2010)

Commission Decision No. 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries

The Danish Data Protection Agency. Processing of sensitive personal data in a cloud solution. (2011). Available at: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/. Last accessed 26 October 2011.

The German Data Protection Authority. Orientierungshilfe – Cloud Computing. (2011) Available at: http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf. Last accessed 30 September 2011

The U.S. Electronic Communications Privacy Act of 1986 (ECPA)

The U.S. Uniform Commercial Code

Law Cases

Cartoon Network v. CSC Holdings, Inc. Decision 536 F.3d 121 (2008) United States Court of Appeals for the Second Circuit.

Factortame. Case C-221/89 [1991] ECR I-3905 §20

Google, Inc.'S v. Suzlon Energy Ltd. Case No. C 10-80034 JW (PVT). United States District Court. Northern District OF California. San Jose Division

Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1989] QB 433

J Spurling Ltd v Bradshaw [1956] 1 WLR 461

McCall v. Facebook, Inc., No. 10-16380 (9th Cir. filed June 23, 2010).

Suzlon Energy Ltd v. Microsoft Corporation. No. 10-35793. D.C. No. 2:10-cv-0170-MJP. The Ninth Circuit Court of Appeals of the US.

Wigle v. Allstate Ins. Co. of Canada (1984), 49 O.R. (2d) 101

Newspapers

BBC News. Sony's PlayStation Hack Apology. 27 April 2011. Available at: http://www.bbc.co.uk/news/technology-13206004. Last accessed 26 October 2011

Elinor Mills. LA approves $7.2 million Google Apps deal. C.Net. News. Available at: http://news.cnet.com/8301-27080_3-10384433-245.html. Last accessed 20 October 2011

EPIC Org. Cloud computing news. 7 February 2011. Available at: http://epic.org/privacy/cloudcomputing/. Last accessed 27 October 2011

Privacy and Information Law Blog. German DPAs Issue Resolution and Guidance Paper on Cloud Computing and Compliance with Data Protection Law. Hunton & Williams LLP. (October 2011). Available at: http://www.huntonprivacyblog.com/2011/10/articles/german-dpas-issue-resolution-and-guidance-paper-on-cloud-computing-and-compliance-with-data-protection-law/. Last accessed 26 October 2011

Articles

Anassutzi & Co. Jurisdiction and law issues in cloud computing agreements. Available at: http://www.anassutzi.com/articles/185-jurisdiction-and-law-issues-in-cloud-computing-agreements.html. Last accessed 12 September 2011

Anil Gupta & Parag Pande. A proposed Solution: Data Availability and Error Correction in Cloud Computing. International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (4) : 2011

Balboni, Paolo, Data Protection and Data Security Issues Related to Cloud Computing in the EU (August 18, 2010). Tilburg Law School Research Paper No. 022/2010. Available at SSRN: http://ssrn.com/abstract=1661437. Last accessed 29 October 2011

Bob Warfield. Gartner: The Cloud is Not a Contract. Available at: http://www.enterpriseirregulars.com/31367/gartner-the-cloud-is-not-a-contract/. Last accessed 28 October 2011

Chris Reed. Information 'Ownership' in the Cloud (March 2, 2010). Queen Mary School of Law Legal Studies Research Paper No. 45/2010. Available at SSRN: http://ssrn.com/abstract=1562461. Last accessed 20 October 2011

David Navetta. "Legal Implications of Cloud Computing", available at http://www.llrx.com/features/cloudcomputing.htm, last access 12 September 2012

Davide Parrilli. Legal Issues in Grid and Cloud Computing. In: Grid and Cloud Computing: A Business Perspective on Technology and Applications (K. StanoevskaSlabeva). Berlin (Springer-Verlag) 2010

European Network and Information Security Agency (ENISA). Cloud Computing Benefits, Risks and Recommendations For Information Security 5 (2009), Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment/at_download/fullReport. Last accessed 18 October 2011

Expert Group Report for Commission of the European Communities. "The Future of Cloud computing: Opportunities for European Cloud Computing Beyond 2010". Available at http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf, last accessed 12 September 2011

Fernando Pinguelo & Bradford Muller. Avoid the Rainy Day: Survey of U.S. Cloud Computing Caselaw. (2011) Boston College Intellectual Property & Technology Forum. Available at: http://bciptf.org/wp-content/uploads/2011/07/1-AVOID-THE-RAINY-DAY.pdf. Last accessed 20 October 2011

Henry Wolfe. Cloud Computing: The Emperor's New Clothes of IT. Informing Science Institute. University of Otago, New Zealand (2011). Available at: http://www.informingscience.org/proceedings/InSITE2011/InSITE11p599-608Wolfe281.pdf. Last accessed 9 October 2011

James Maxeniner. Standard Terms Contracting in the Global Electronic Age: European Alternatives, 28 Yale J. Int'l L. 109 (2003)

Jen Millea. Heading into the Cloud: Cloud Computing and Education. Available at: http://blogs.educationau.edu.au/jmillea/2009/06/23/heading-into-the-cloud-cloud-computing-and-education/. Last accessed 10 October 2011

K&L Gates. Cloud Computing Case Clarifies Applicability of US Privacy Law to Non-U.S. Nationals. Available at: http://www.tmtlawwatch.com/2011/10/articles/cloud-computing-case-clarifies-applicability-of-us-privacy-law-to-nonus-nationals/. Last accessed 29 October 2011

Kuan Hon. Data Protection: The Law and You. Available at: http://blogs.computerworlduk.com/cloud-vision/2011/04/data-protection-the-law-and-you-1/index.htm. Last accessed 26 October 2011

_____. Who's responsible for personal data in cloud computing? Available at: http://blogs.computerworlduk.com/cloud-vision/2011/05/whos-responsible-for-personal-data-in-cloud-computing/index.htm. Last accessed 26 October 2011

Kuan Hon, Christopher Millard and Ian Walden. Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing Part 2. Queen Mary School of Law Legal Studies Research Paper No. 77/2011. Available at SSRN: http://ssrn.com/abstract=1794130. Last accessed 26 October 2011

Llewellyn Joseph Gibbons. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. Cornell J.L. & Pub. (2007)

Marco Giunta. Cloud Computing: An Opportunity and a Legal Maze. Available at: http://marcogiunta.com/tech/cloud-computing-an-opportunity-and-a-legal-maze/. Last accessed 10 September 2011

Mary Brandel. The Trouble with Cloud: Vendor Lock-in. Available at: http://www.cio.com/article/488478/The_Trouble_with_Cloud_Vendor_Lock_in. Last accessed 25 September 2011

Mark Vincent, Nick Hart and Kate Morton. Cloud Computing Contracts White Paper: A Survey of Terms and Conditions. Truman Hoyle Lawyers. Available at: http://www.ficpi.org.au/articles/White_Paper_June2011.pdf. Last accessed 13 October 2011

Mark H. Wittow. Cloud Computing: Recent Cases and Anticipating New Types of Claims. The Computer and Internet Lawyer Vol 28 No.I (2011). Available at: http://www.klgates.com/files/Publication/5d61b5e9-ad6f-4d6a-985c-30cb6b84dae2/Presentation/PublicationAttachment/42137be3-c03c-4c58-a527-31d872b78ec5/Wittow_CloudComputing_Jan2011.pdf. Last accessed 29 October 2011

Neil Brown. Thames Valley Group Meeting Report: Cloud Computing Contracts. The IT Law Community. Available at http://www.scl.org/site.aspx?i=ne19148. Last accessed 7 October 2011

Paul T. Jaeger, Jimmy Lin & Justin M. Grimes. Legal and Quasi-Legal Issues in Cloud Computing Contracts and Cloud Computing and Information Policy: Computing in a Policy Cloud? Available at http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479. Last accessed 20 October 2011

Peter Mell & Timothye Grance. "The NIST Definition of Cloud Computing: Recommendations of the NIST". Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Last accessed 12 September 2011

Thorsten. Amazon EC2 Outage: Summary and Lessons Learned. Available at: http://blog.rightscale.com/2011/04/25/amazon-ec2-outage-summary-and-lessons-learned/. Last accessed 26 October 2011

Robert Hillman. The Richness of Contract Law: An Analysis and Critique of Contemporary Theories of Contract Law. 129-43 (1997)

_____. Standard-Form Contracting in the Electronic Age. 77 N.Y.U. L. Rev. 429 (2002)

Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay & and Juheng Zhang. Cloud Computing: The Business Perspective. (2009). Available at SSRN: http://ssrn.com/abstract=1413545. Last accessed 19 October 2011

Simon Bradshaw, Christopher Millard, and Ian Walden. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Centre for Commercial Law Studies. London (2010). Available at http://ssrn.com/abstract=1662374. Last accessed 8 October 2011

Simon Bradshaw, Christopher Millard, and Ian Walden. The Terms They Are A-Changin'... watching Cloud Contracts Take Shape. The Center for Technology Innovation. Issue in Technology Innovation. (2011)

Simon Hodgett. Cloud Computing Contracting and the Spectrum of Risk. Thirteenth Annual Canadian IT Association Conference (2009). Available at: http://www.it-can.ca/direct/membersonly/2009conf/cloud_computing_hodgett.pdf. Last accessed 13 October 2011

Shmuel Becher & Esther Unger-Aviram. The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction. DePaul Bus. & Comm. L.J. 199 (2010). Available at: https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=8+DePaul+Bus.+%26+Comm.+L.J.+199&srctype=smi&srcid=3B15&key=7b33ab519c475d164d0a5758cb666e74. Last Accessed: 26 October 2011

Thomas J. Trappler. If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues. Educause Quarterly. Volume 33, Number 2, 2010. Available at: http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532. Last accessed 11 October 2011

Wayne Jansen & Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (2011). Available at: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf. Last accessed 26 October 2011

William Condon. Electronic Assent to Online Contracts: Do Courts Consistently Enforce Clickwrap Agreements. 16 Regent U. L. Rev. 433 (2003-2004). Page 221. Available at: http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/regulr16&div=20&id=&page. Last accessed 6 October 2011

World Economic Forum. Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation. (2010)

PhD Dissertation

Maryke Silalahi Nuth. "E-commerce Contracting: The Effective Formation of Online Contracts." University of Oslo. (2011)

Websites

Electronic Privacy Information Center. Cloud Computing. Available at: http://epic.org/privacy/cloudcomputing/. Last accessed 11 October 2011

Google Data Liberation Front on http://www.dataliberation.org/. Last accessed 18 October 2011

Microsoft Research. Cloud Cryptography. Available at: http://research.microsoft.com/en-us/projects/cryptocloud/

The Open Cloud Manifesto. Draft 1.0.9. Available at: http://gevaperry.typepad.com/Open%20Cloud%20Manifesto%20v1.0.9.pdf. Last accessed 18 October 2011

Lecture Notes

Cecile Christensen. "Cloud computing: what is it?" The Nordic IT Law Conference 2010. Available at http://www.it-retsforum.dk/uploads/media/Cloud_Computing_What_Is_It_by_Cecilie_Christensen.pdf, last accessed 12 September 2011

Christopher Millard. Cloud computing: identifying and managing legal risks. Google / Oxford Internet Institution. (2011). Available at: http://www.slideshare.net/CloudLegal/millard-cloud-computing-key-legal-and-regulatory-challenges-oiigoogle-lecture-brussels-feb-2011. Last accessed 31October 2011

Definition of Service Level Agreement. Available at: http://www.webopedia.com/TERM/S/Service_Level_Agreement.html. Last accessed 7 October 2011

Emily Weitzenboeck. Electronic contracting: Recognition and Validity of Electronic Contract. Lecture Notes on E-Commerce Class of ICT Programme of University of Oslo. 2011

Others

Neelie Kroes (Vice-President of the European Commission). European Cloud Computing Strategy needs to aim high. (2011). Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/199&format=HTML&aged=1&language=EN&guiLanguage=en. Last Accessed 26 October 2011

Queen Mary University. Cloud Legal Project response to European Commission Cloud Computing Consultation. Available at: http://www.cloudlegal.ccls.qmul.ac.uk/Research/55027.html. Last accessed 26 October 2011.

"All material referred to in this assignment is listed in the reference list"

ANNEX A

CLOUD PROVIDERS COVERED BY SURVEY
(Conducted from 10th until 14th of November 2011)

Adrive
Term of Service available at: http://www.adrive.com/terms.

Akamai
Terms and Conditions available at:
http://www.akamai.com/dl/akamai/Akamai_Terms_Conditions_2009.pdf.

Amazon Web Service
- Customer Agreement available at: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html.
- Term of Service available at: http://aws.amazon.com/terms/.

Apple iWork Public Beta
Term of Service available at: http://www.apple.com/legal/iworkcom/en/terms.html.

Dropbox
Term of Service available at: https://www.dropbox.com/terms.

Elastichost
Term of Service available at: http://www.elastichosts.com/cloud-hosting/terms-of-service.

Facebook
Statement of Rights and Responsibilities available at:
http://www.facebook.com/terms.php.

Flexiant
- Term of Service available at: http://www.flexiant.com/products/flexiscale/terms/.
- Privacy Policy available at: http://www.flexiant.com/about/privacy/.

Gogrid
Term of Service available at: http://www.gogrid.com/legal/terms-service.php.

Google
Google Apps for Business Agreement available at: http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html.

Iron Mountain
Client-Software License Agreement available at: http://ironmountain.com/legal/livevaultc.asp.

Joyentcloud
Term of Service available at: http://www.joyentcloud.com/about/policies/terms-of-service/.

Microsoft
- Term of Service available at: http://www.microsoft.com/About/Legal/EN/US/IntellectualProperty/Copyright/default.aspx#EPC.
- Privacy Statement available at: http://privacy.microsoft.com/en-us/fullnotice.mspx.

Rackspace
- General Terms available at: http://www.rackspace.co.uk/legal/general-terms/.
- Acceptable Use Policy available at: http://www.rackspace.ae/uploads/involve/user_all/64_Acceptableusepolicy.pdf.

Salesforce
Master Subscription Agreement available at: http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf.

UK Fast Cloud Service
Terms and Conditions available at: http://www.ukfast.co.uk/terms.html.

3Tera
Term of Service available at: http://www.3tera.com/Terms/index.php.