TILBURG UNIVERSITY

CLOUD COMPUTING AND THE REGULATORY FRAMEWORK FOR TELECOMMUNICATIONS AND INFORMATION SOCIETY SERVICES

VALENTINA PAVEL BURLOIU

MASTER THESIS

Coordinated by Kees Stuurman

ANR 351001

Law and Technology

February 2012

Table of Contents

LIST OF ABBREVIATIONS

API	Application Programming Interfaces
BCR	Binding Corporate Rules
CAPEX	Capital expenditure
DAE	Digital Agenda for Europe
DMCA	Digital Millennium Copyright Act
EC	European Community
ECJ	European Court of Justice
ECPA	Electronic Communications Privacy Act
ECS	Electronic Communications Service
EC Treaty	European Community Treaty
FCC	Federal Communication Commission
GATS	General Agreements on Trade in Services
IaaS	Infrastructure as a Service
IAPes	Internet Access Providers
IEC	International Engineering Consortium
IP	Internet Protocol
ISP	Internet Service Provider
ISS	Information Society Service
IT	Information Technology
NIST	US National Institute for Standards and Technology
NRA	National Regulatory Authority
OPEX	Operational expenditure
ONP	Open Network Provisions

PaaS	Platform as a Service
PTT	Postal Telegraph and Telephone service
SaaS	Software as a Service
SLA	Service Level Agreement
SME	Small and medium enterprise
SNS	Social Networking Sites
TEN	Trans-European Networks
WP	Working Party
WTO	World Trade Organization
USA	United States of America
USC	US Stored Communications Act
USO	Universal Service Obligation
VoIP	Voice over Internet Protocol

INTRODUCTION

In the context of the Lisbon agenda for growth and jobs, research and innovation are at the core of the Europe 2020 strategy. As part of this strategy, the ambitious Digital Agenda of the European Union underlines the impact of cloud computing both under the fifth pillar[1] but also as an important element for the European Single Market.[2] Therefore, it has been acknowledged that innovative and convergent technologies such as cloud computing "shake-up" the market and allow asking as to whether the trend should be approached from a regulatory perspective. [3]

Recent debates[4] prove that while there is no doubt about the benefits of cloud computing, serious legal issues impinging cloud emergence - such as security, privacy and liability - still remain to be considered. Factually, the aim of the Digital Agenda is to build a pan-European cloud enabling both industries and governments to benefit from this technology[5]. Policy-wise, the context from which European law choose to address the digital environment, which encompasses matters of privacy, electronic communication and electronic commerce, is that of separate legal regimes.[6] Indeed, in the absence of an "explicit regulation on a pan-European level"[7] for information technology services, the legal regimes mentioned above are a focal point for discussing the effects regulation has on cloud computing development.

As it has been stated by Microsoft's vice president for EU affairs, John Vassallo "[cloud computing] is as big as moving to PCs in the 70s. It will change the economics of doing business, it will change the economics of running governments, it will create a productivity

---

[1] The fifth pillar addresses research and innovation.

[2] European Commission, Directorate General for Information Society and Media, *Digital Agenda for Europe Annual Progress Report* (22 December 2011) 4 <http://ec.europa.eu/information_society/digital-agenda/documents/dae_annual_report_2011.pdf>

[3] Jasper P. Sluijs and others, *'Cloud Computing in the EU Policy Sphere'* (2011) TILEC Discussion Paper No 2011-036, 2 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909877> accessed 25 January 2012

[4] Trans-European Research and Education Networking Association (TERENA), TF-Storage conference (27 May 2011) <http://www.terena.org/news/fullstory.php?news_id=2903> accessed 18 December 2011

[5] Microsoft Europe, Microsoft Online Knowledge Center: Could Knowledge Center <http://www.microsoft.eu/cloud-computing/cloudknowledgecentre.aspx> accessed 18 December 2011

[6] Pierre Larouche, *'Communications Convergence and Public Service Broadcasting'* (2001) 4ff <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=832444> accessed 2 February 2012

[7] Jasper Sluijs and others, 'Cloud Computing in the EU Policy Sphere', 13

game that can be measured, some say, between 15 to 25 percent. That is a big leap"[8]. Therefore, considering the impact it will have at consumer, governmental and industrial level, it is imperative to start considering cloud computing as the instigator[9] for a broad reassessment of information policy-making process.[10] As a matter of fact, the European Commission, alerted by the potential economical benefits of cloud computing, is interested in removing the "unnecessary obstacles" for the adoption of cloud services.[11] Furthermore, the Commission intends to resolve stringent issues such as security and privacy in order to facilitate an "uninterrupted expansion and innovation of cloud computing"[12].

Keeping all of this in mind, the general purpose of this paper represents an engagement towards understanding the current issues arising from the intersection of cloud computing and regulatory provisions dealing with security, privacy and liability. More specifically, while the nature of cloud computing involves a direct and straightforward connection to electronic commerce, the question still pounders whether cloud providers are subject to the application of electronic communications regulation. Therefore, this paper is going to explore the circumstances in which the telecommunications framework is coming into play for dealing with relationships created in the cloud environment. Consequently, this research tries to identify the interplay between cloud providers and telecommunication providers and see whether cloud services have an electronic communications component that could trigger the application of telecommunications regulations. Alongside, given the relevance security, privacy and liability issues have for the IT sector and consequently also for cloud computing, we will analyze the inherent provisions springing from both the sector-specific regulations on telecommunications and from the electronic commerce regime.

To complete this task, this dissertation will necessarily start with an introduction to the cloud environment. Therefore, the first chapter presents the various proposed definitions of cloud computing, its actors and deployment models. Furthermore, the applications, benefits and the essential characteristics of cloud computing are also highlighted.

Following the first chapter, a brief chronological overview of the telecommunications regulations is presented. Thus, the second chapter helps the reader get acquainted with the parameters that the research question is addressing. To be more exact, because of the potential

---

[8] Jesse Verstraete, *'Cloud computing critical to Digital Agenda's success'*, Deutsche Welle radio interview by Teri Schulz (8 September 2010) <http://www.microsoft.eu/digital-policy/posts/cloud-computing-critical-to-digital-agendas-success.aspx> accessed 18 December 2011

[9] Paul T. Jaeger and others, *'Cloud Computing and Information Policy: Computing in a Policy Cloud?'*, 280

[10] Ibid., 282

[11] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, Meeting Note (16 November 2011) 2 <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/hearingreport-telecomsv2.pdf> accessed 19 January 2012

[12] Ibid.

application of electronic communications provisions to cloud providers, the telecommunications framework presentation is destined to familiarize the reader with the evolution of the different stages of this field.

The third chapter aims at clarifying whether under the current legislation we can indeed speak of a juxtaposing classification between the cloud and the telecommunications sphere, meaning if generally cloud services are or should be addressed by electronic communications regulation. The analysis begins by constructing a parallel between electronic communications services and information society services. In this respect, both the definitions of electronic communications services and information society services are examined to see whether they contain sufficient elements to address cloud specificities. Aside from the legal interpretation of these definitions, a comprehensive guide to describing cloud elements will serve as a basis for drawing the final conclusions related to the possibility of an overlap between the cloud, electronic communications and information society services. Furthermore, on a level which is distinct from the main purpose of this thesis, the findings of the research have been enriched with remarks relevant for considering the cloud strategy and possible regulatory approaches. We need to point out that the inevitable considerations about policy-wise approaches had as main contributing factors the lack of a consistent legislative approach and the generous margin of appreciation regarding the applicable framework for cloud.

The forth chapter highlights some of the legal issues the recent debates have been focusing on. Therefore, security, privacy and liability issues falling from both the telecommunications framework but also from the electronic commerce perspective will be analyzed and their impact on cloud computing will be assessed.

Finally, the paper ends with a comprehensive set of conclusions that demonstrate the impact the above mentioned set of regulations have on cloud computing at a European level. Additionally, on a more general note, the fifth chapter will also contain conclusions in terms of provoking reassessment of existing legal regimes and regulatory harmonization.

METHODOLOGY

This dissertation is based on the findings of a qualitative study as the aim is to understand the cloud paradigm, contextualize the phenomenon, interpret the regulatory framework of telecommunications and information society services and observe the implications of all of the above. Therefore, this author performed a desk study consisting of the consultation with both primary and secondary sources. To accomplish this, legislation, case law and policy papers were used as primary sources. Furthermore, scholarly literature was consulted and interpreted as a secondary sources. This author would like to add that the sources used were not limited to strictly scholastic materials. Given the multidisciplinary approach of the research, the materials or opinions consulted also originate from business representatives and field technicians.

Additionally, the research was based on participatory observation since not only has this author closely followed the past developments in the field of cloud computing, but also actively took part in discussions with different experts, industry representatives, academia and legal practitioners, and attended a conference in Brussels entitled "Cloud Law or Legal Cloud?".

Given the novelty of the debates surrounding cloud computing and the current limited scale of usage in Europe, this research is going to be based on available expert and technical reports issued by organizations such as ETSI and NIST, workgroup conclusions and findings, conference notes and summaries of discussions, memos, articles and theoretical analyses.

This author would like to underline the importance of the research area by expressing the fact that the most recent studies[13] and debates[14] have been related to whether the current European regulatory regime is suitable for responding to the challenges of cloud computing. Therefore, the paper touches upon the major arguments under discussion and presents different points of view. At the same time, this research adds value to the current findings by presenting and analyzing new approaches in relation to the cloud model which consist in themselves the fundamentals of dealing with cloud computing and legal practice.

Therefore, since it has been consistently pointed out that the European policy is not yet ready to accommodate cloud concerns,[15] the central aim of the paper is to classify the knowledge we have today related to cloud computing and see the connection between the further emergence of the cloud and European regulation. Given the "disconnect in legal scope"[16], this research is

---

[13] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*

[14] Cloud Computing Hearing with Telecommunication and Web Hosting Industry

[15] Among others, Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 4

[16] Among others, Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 4

valuable and relevant since it provides new insight into the cloud computing matter by addressing the correlations that can be made in relation to the telecommunications framework and obligations that spring from this sphere.

The theoretical perspective from which this topic is approached resides within the European telecommunications framework and several connected European directives such as Directive 2002/58/EC and Directive 2000/31/EC. Therefore, the telecommunications regulations and the electronic commerce directive are used as main sources in order to provide an understanding of the core concepts.

For conducting this research, this author first thoroughly documented the specifics of cloud computing. In this respect, a considerable amount of technical reports have been consulted. Priority has been given to the documents issued by authoritative bodies such as ETSI, ENISA, NIST and RAND. Furthermore, available expert opinions and working group conclusions and findings, conference notes, memos and summaries of discussions and personal communications have been used in order to present a panoramic view of the subject. Additionally, online journal databases have been permanently searched for articles and books to complement the theoretical analysis.

The construction of the second chapter mainly relied on inspecting the chronological succession of regulations in the telecommunications sector. The third chapter interprets relevant legal texts and makes use of comparative article analysis to illustrate the different approaches to the topic. The forth chapter illustrates a descriptive research of legal obligations and evaluates these provisions in relation to their application to cloud computing. Furthermore, through the use of case studies, additional highlights are presented to complement the regulatory analysis.

However, we encountered two major difficulties in resource processing. The first one was related to the novelty of the topic in question. Intimately connected to this is the lack of an established and reliable common ground understanding of the meaning of the model, which adds to the challenges. Second, the speed with which new opinions and studies connected to the topic have been released represented another significant challenge of this research. This author would refer the reader to the list of used materials which were released no later than 2009 and as early as January 2012.

Furthermore, this author also needs to point out the identified limitations of this thesis. To begin with, the authors' limited technical understanding might have constituted either an obstacle in thoroughly analyzing specific facets of the cloud model or it could have represented the source of confusion in relation to observations based on information with technical particularities. As mentioned above, the speed at which new sources, findings and legislative pieces were released inevitably had an impact on this paper. Finally, the infantile stage of development of cloud computing might have also represented an obstacle for performing a complete and accurate analysis of its relation to European regulation.

Accordingly, the selected methodology is intended to guide us towards revealing the answer to our central question, namely in what circumstances is the telecommunication framework coming into play for dealing with the relationships created in a cloud environment.

Cloud computing has generated new types of relationships and specific actors are aggregated within its environment. For the purpose of our research, the distinction between a cloud provider and a cloud carrier, as it will be presented in the first chapter, is of significant importance for our analysis. Moreover, due to the rapid yet normal interposition of the cloud service delivery model into more and more fields and business sectors, a problematic issue would be that the legal regime that applies to cloud-based relationships is different from one sector to another. In this context, it has been raised under discussion whether the telecommunications regulations present sufficient elements that could potentially trigger their application to cloud.

Therefore, this research will focus on investigating when telecommunications regulations apply to the cloud environment. More specifically, it will identify the interposition between cloud providers and telecommunication providers. In this respect, specific definition related elements will be searched in order to see if the application of the telecommunications regulation could be triggered in relation to cloud providers. After this, a discussion will follow about the particularities of the telecommunications regime and information society rules in relation to security, privacy and liability matters which impact cloud providers.

CHAPTER ONE - Definition of terms and concepts

Although the ideas behind cloud computing are not new, the confluence of these ideas in a model where information can be accessed from a multitude of devices and regardless of location represents a major transformation of computing.[17] As a matter of fact it has been pointed out that cloud computing is basically an "evolution and repackaging of existing technologies and standards"[18]. Moreover, it has to be specified that the unique nature of cloud computing derives from the fact that it encompasses aspects of computer, information, and telecommunications issues.[19]

In order to understand the cloud environment, this chapter will first present the definition of terms and concepts. Second, the relationship between the actors in the cloud will be described. Afterwards, the cloud characteristics, applications and benefits will be illustrated in order to give a better overview of the paradigm. A special subsection will be addressed to the opportunities of cloud computing for Europe first because of the importance allocated to this subject by the European Commission but also because Europe, as a union, has better chances of taking the adequate measures in response to the public policy problems raised by cloud computing.

1. Definition of terms and concepts

Since a globally accepted official definition has not been established yet, the following section will present the definitions and concepts that we consider relevant for understanding the cloud environment.

Maximizing the vastness of available sources, we will begin by presenting the definition of cloud computing from a series of angles. Therefore, the perspective of academia, industry and authoritative government sources will be used in order to shape the edges of the cloud paradigm.

Important to note is that in September 2011, the US National Institute for Standards and Technology (NIST) issued a special release document regarding the definition of cloud computing which states that

---

[17] Sean R. Marston and others, *'Cloud Computing: The Business Perspective'* (2011) 51 (1) Decision Support Systems, 177 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1413545> accessed 18 December 2011

[18] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 6

[19] Paul T. Jaeger and others, *'Cloud Computing and Information Policy: Computing in a Policy Cloud'*, 278

> "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[20].

This definition has the status of an official definition in the US, whereas in Europe there is no universally accepted one. However, most practitioners[21] and organizations adopted the above as a working definition.

In Europe, the Expert Group Report advising the European Commission on matters of opportunities related to cloud computing resume to present a very broad definition of cloud. Therefore, they define the term cloud as

> "an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)"[22].

This document is more focused on describing the types of clouds and their characteristics rather than to provide a version of an official definition.

Furthermore, representative sources from the business sector such as Gartner revised their definition of cloud computing once they identified possibilities of improving the way cloud computing should be looked at. In Gartner's current view, cloud computing is "a style of Computing where scalable and elastic IT capabilities are provided as a service to multiple customers using Internet technologies"[23].

With regard to the practitioner's and academia's perspective, the most illustrative source is Vaquero et. all. The authors embarked on a collection and analysis of proposed definitions and made the recommendation for clouds to be seen as "a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services)"[24]

---

[20] Peter Mell and Timothy Grance, Recommendations of the National Institute of Standards and Technology, *'The NIST Definition of Cloud Computing'* (2011) National Institute of Standards and Technology, Special Publication 800-145, 2 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> accessed 18 December 2011

[21] Yet, there are still authors who addressed critique to this definition. In this sense, Sluijs and others have underlined the fact that the definition does not incorporate the multitude of cloud applications and services. See Sluijs and others, *'Cloud computing and EU policy'*, 7

[22] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, Public version 1.0, 8 <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf> accessed 7 January 2012

[23] Daryl Plummer, *'Experts Define Cloud Computing: Can we get a Little Definition in our definitions'* (Gartner Blog Network, 27 January 2009) <http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/> accessed 7 January 2012

[24] Luis M. Vaquero and others, *'A Break in the Clouds: Towards a Cloud Definition'* (2009) 39 (1) ACM SIGCOMM Computer Communication Review, 51 <http://delivery.acm.org/10.1145/1500000/1496100/p50-

which can be customized to any scale and therefore permit their ideal utilization. The authors further describe that the available resources are being offered via "a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs"[25]. The authors sum up that the highlights the definition proposes in relation to cloud computing characterization are "scalability, pay-per-use utility model and virtualization"[26]. This definition is worth mentioning not only because of the fact that it was proposed after a thorough analysis of the most suitable available definitions but also because the author started to develop it by referring to the major features of a similar paradigm formally introduced, the grid.[27]

Additionally, Vaquero et. all expresses two important forewarns. First, he observes that the general confusion about the cloud paradigm has given raise to the assumption that it includes just about "any solution that allows the outsourcing of all kinds of hosting and computing resources"[28]. Second, he points out a confusion that has to be avoided, namely to separate between cloud computing and grid computing. The reason for this confusion is that clouds and grids share certain fundamental aspects such as diminished computing costs and additional elasticity and reliability through intermediaries operating hardware.[29] Identifying the same confusion, the European Expert Group Report also highlights the importance of a clear separation of these terms.[30] Furthermore, the same report mentions that the expansion of repackaging offerings as cloud services (without actually changing the provided capabilities) is another factor that contributed to the general confusion regarding interrelated aspects of cloud computing.[31]

Moreover, Armbrust et. all establishes a delimitation when it comes to the dimension and composition of cloud computing. The authors state that cloud computing is the sum of

---

vaquero.pdf?ip=137.56.104.226&acc=ACTIVE%20SERVICE&CFID=77016447&CFTOKEN=22393273&__acm__=1325934879_54ca9a9465d480d5f9e920bf64c38d12> accessed 7 January 2012

[25] Ibid.

[26] Ibid.

[27] Luis M. Vaquero and others, *'A Break in the Clouds: Towards a Cloud Definition'*, 54

[28] Ibid., 50

[29] Ibid., 51

[30] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, 5

[31] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, 6

Software as a Service (SaaS) and utility computing and that it does not include small or medium sized data centers, even if these turn to virtualization for management purposes[32].

In search for a reference document that would balance the visions expressed by practice, industry and scholars, we indicate RAND Europe's technical report[33] as a valuable working tool because it presents cloud computing terms and concepts in a manner clearer for layman. However useful this document might be, we acknowledge at the same time that NIST's definition and presentation of types, deployment models and characteristics provide a more comprehensive description of the paradigm.

Interestingly, RAND Europe has also considered defining cloud computing from the perspective of an information technology (IT). From this point of view, they suggest seeing cloud computing as

> "a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centers, tablet computers, notebooks, wall computers, handhelds, sensors, monitors, etc."[34]

We have seen so far the multitude of perspectives from which cloud computing can be approached. However, perhaps it is more useful to present the elements required in any cloud environment rather than stop at only one definition.

Therefore, the essential characteristics our main reference source - NIST - identifies are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[35] The following section, which individually describes the cloud's characteristics, accentuates how easy and "at hand" this model can be for consumer usage.

First of all, **on demand self-service** means that a consumer can one-sidedly allocate computing capabilities, thus eliminating the interaction with each service provider in relation to server time, network storage and others.[36] Second, **broad network access**, encompasses the network's capabilities that are facilitated by access through a multitude of devices such as

---

[32] Michael Armbrust and others, *'Above the Clouds: A Berkeley View of Cloud Computing'* (10 February 2009) Technical Report No. UCB/EECS-2009-28, 4-6 <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf> accessed 7 January 2012

[33] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'* (Technical Report, 2011) <http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR933.pdf> accessed 7 January 2012

[34] Carl Hewitt, *'ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing'* (2008) 12 (5) IEEE Internet Computing, 96–99 as quoted by RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'* (Technical Report, 2011) 17

[35] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing'*, 2

[36] Ibid.

mobile phones, tablets, laptops or workstations.[37] Third, **resource pooling** is a term that describes the fact that through the use of a multi-tenant design which can be dynamically customized, the provider's computing resources are shared in order to respond to numerous consumers' demand.[38] Moreover, it implies location abstraction, meaning that the consumer, as a general rule, is neither involved in the control nor knowledgeable about the location of the provided resources.[39] However, the delimitation of location is possible at the upper level of abstraction, for instance the country, state or datacenter.[40] Examples of such resources include storage, processing, memory and network bandwidth.[41] Another notable characteristic is the **rapid elasticity** which point to the fact that the consumer perceives the available capabilities as infinite and provisioned irrespective of size and period of time.[42] Therefore, the essential component is the fact that it can promptly respond to diminishing or increasing the provisioning of resources in exact proportion with the demand.[43]

Last, **measured service** refers to the fact that cloud models mechanically manipulate and adjust resources use through a measuring system applicable to the category of service such as storage, processing, bandwidth or active user accounts.[44] Therefore, the system presents has a transparent mechanism for both parties for tracking resource usage.[45]

Described with slight differences[46], there are generally three cloud systems: software, platform and infrastructure. Because it gives a more complete overview over the capabilities each model provides[47], NIST's definition will be used as a reference for presenting the service models.

Therefore, in the following, each deployment model will be described accompanied by examples of the respective service.

---

[37] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing'*, 2

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] For example, RAND Europe also talks about Hardware as a Service (HaaS) while NIST incorporates the description of HaaS in Infrastructure of a Service (Iaas).

[47] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 2

First, **Software as a Service (SaaS)** enables the consumer to make use of the provider's applications that were build on a cloud platform.[48] The ways in which the applications can be typically accessed are via a web browser or a program interface.[49] In this scenario, the consumer does not administer or manipulate manage the implicit cloud infrastructure (which includes network, servers, operating systems, storage and individual application capabilities; however, as a possible exception, some configuration settings can be adjusted by the consumer).[50] Examples of SaaS include Google Docs, Salesforce CRM, SAP Business by Design.

Second, **Platform as a Service (PaaS)** means that the consumer's capability to turn to effective use, on the cloud platform, the consumer-created applications which were generated using various elements and tools necessary for application delivered by the provider.[51] As in the case for Saas, the consumer does not have control of the cloud infrastructure, however he administers the created applications and its configuration preferences.[52] A few examples are Force.com, Google App Engine, Windows Azure.

The third deployment model is **Infrastructure as a Service (IaaS).** This refers to provisioning processing, storage, networks and other essential computer resources which allow the consumer to make effective use and run any type of random software such as operating systems or applications.[53] Whereas the consumer is enabled to exercise control over the operating systems, storage and utilized applications, as well as partial control of some networking components (such as host firewalls), he is not in a position to manipulate the underlying cloud platform.[54] Known practical applications are Amazon S3, SQL Azure, Amazon EC2, Zimory, Elastichots.

Additionally some authors speak of EaaS/XaaS, the abbreviation of everything as a service, which means a combination of SaaS, IaaS and Paas.[55]

---

[48] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 2

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Ibid., 3

[53] Ibid.

[54] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 2

[55] Andrew Joint and Edwin Baker, *'Knowing the past to understand the present – issues in the contracting for cloud based services'* (2011) 27 (4) Computer Law & Security Review, 409 <http://www.sciencedirect.com/science/article/pii/S0267364911000689 > accessed 7 January 2012

Important to note is that the European Expert Group Report stresses the fact that while this division can be seen as a "usage pattern" for cloud systems based on Grids and Web services, they have nevertheless the potential to develop these models to a larger extent.[56]

An additional aspect to be mentioned is that while cloud providers usually focus on providing one type of functionality, simultaneously offering multiple types of functionalities is not a confinement.[57] Moreover, one type of functionality can be developed with the help of other layers. In other words, SaaS can be developed on PaaS and delivered through IaaS. As an example, we can mention Twitter which uses Infrastructure as a Service from Amazon in order to deliver its product - Software as a Service - to customers. Additionally, also customers can interrelate cloud services offered by distinct providers. Therefore, they can joggle with cloud services so that the main service to be supported by a secondary one.[58]

In conclusion, it is important to be aware of the fact that the cloud service that the customer uses can be functioning on several layers of the cloud model[59], hence it implies the "increased sophistication of cloud use increasing layering of providers"[60]. Implicitly, there are also instances where the cloud service is provisioned without the customer being aware of the interposition of different cloud providers since a client's interest resides only with the finite product and not the backstage details. As a result, only to mention a glimpse of the new challenges, there are serious confrontations regarding the processing of personal data in the cloud.[61]

Furthermore, as we will see below, clouds may be hosted and employed in different ways. The four deployment models are private, community, public and hybrid. However, we have to keep in mind RAND Europe's remark that due to the "immature and exploratory nature"[62] of cloud computing deployments, we have to be aware of the fact that its service models may

---

[56] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, 10

[57] Ibid., 9

[58] Examples in this sense may be related to monitoring (such as Nimsoft) and online pricing systems (such as Zuora is offering for Windows Azure customers). For information about ZuoRA see <http://blogs.msdn.com/b/windowsazure/archive/2010/11/11/real-world-windows-azure-interview-with-jeff-yoshimura-head-of-product-marketing-zuora.aspx>

[59] SNVLabs <http://blog.svnlabs.com/saas-built-using-a-paas-google-app-engine-and-using-iaas-amazon-ec2/> accessed 7 January 2012

[60] W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1'* (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011, 7 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577> accessed 7 January 2012

[61] For further analysis see chapter four.

[62] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*, xi

change in the future.[63] Furthermore, as Joint and Baker observe, even inside the industry there are particular problems that add up to the degree of uncertainty and inconsistency. The authors point out the fact that on one hand, the jargon that has been created around cloud services leads to a general state of confusion for potential end users and, on the other hand, the separate opinions within the industry contribute to uncertainty and unreliability towards the product[64].

Therefore, the premature stage of cloud computing might represent an impediment for a complete and accurate analysis of its relation to European regulation.[65] Consequently, we can also ask whether its further development will change in any way its relation to the regulatory framework.

For describing the four deployment models, we will also point to the NIST's document because we consider it the most appropriate description of ways in which computing can be used.[66]

First, **private cloud** refers to the situation in which the cloud infrastructure is provisioned for the discretion of a sole organization.[67] The ownership and administration of the infrastructure can be in the power of the organization, a third party or it can be managed by both of them.[68] The infrastructure may be located on premises or irrespective of it.[69] An example of a private cloud is eBAy.

In the case of a **community cloud**, the infrastructure is provisioned for the use of an only and specific community of consumers "sharing the same missions, security requirements, policy and compliance considerations".[70] The exercise of management and operational control over the respective infrastructure can be performed by one or several organizations in the community, a third party or by a combination of them.[71] With respect to the physical

---

[63] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*, 18

[64] Andrew Joint and Edwin Baker, *'Knowing the past to understand the present – issues in the contracting for cloud based services'*, 407

[65] Jasper Sluijs and others, *'Cloud Computing in the EU policy'*, 7

[66] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 3

[67] Ibid.

[68] Ibid.

[69] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 3

[70] Ibid.

[71] Ibid.

existence of the infrastructure, this may be either on or off the premises.[72] Community clouds are still a project for the future, but Zimory and RightScale present reasons for their actual development.[73]

Public cloud means that the infrastructure is provisioned for the use of the general public.[74] In this case a business, academic, or government organization, or some combination of them may be the owner of the infrastructure, as well as the one managing and operating it. Public clouds are located on the premises of the cloud provider.[75] Some examples of public clouds are Amazon, Google Apps, and Windows Azure.

The **hybrid cloud** consists of two or more distinct cloud infrastructures such as private, community or public.[76] While they remain unique entities, they are at the same time connected by "a standardized or proprietary technology that enables data and application portability (e.g.: cloud bursting for load balancing between clouds)"[77]. There are not many hybrid clouds in current use, but there are some initiatives taken by IBM and Juniper to introduce the fundamental technologies for building them.[78]

2. Relationships in the cloud

There are different divisions regarding the actors in the cloud, but as for the other sections in this chapter we will make use of NIST's interpretation.

NIST identifies five actors: the cloud consumer, the cloud provider, the cloud auditor, the cloud broker and the cloud carrier.[79]

---

[72] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 3

[73] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010',* 11

[74] Peter Mell and Timothy Grance, *'The NIST Definition of Cloud Computing',* 3

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges',* 11

[79] Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'* (2011) Special Publication 500-291, 16 <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024> accessed 7 January 2012

The **cloud consumer** can be either a person or an organization that while maintaining a business relationship with a cloud provider, he also uses the service offered by the provider.[80] The consumer's range of options can be from the mere use of applications or services for process operations, to the development, management and deployment of application created on a cloud platform and as far as installing and administrating services for IT infrastructure related proceedings.[81]

Like the cloud consumer, the **cloud provider** can be either a person or an organization, but it can also be an entity granting the availability of services to cloud consumers.[82] A cloud provider has the triple role of "building the requested software/platform/infrastructure services, managing the technical infrastructure required for providing the services, provisioning the services at agreed-upon service levels, and protecting the security and privacy of the services".[83]

Therefore, a cloud provider deals with "installing, managing, maintaining and supporting the software application on a cloud infrastructure" when delivering SaaS, with "provisioning and managing cloud infrastructure and middleware for the platform consumers and providing development, deployment and administration tools to platform consumers" as PaaS but also with "providing and managing the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers" as far as IaaS is concerned.[84]

The **cloud auditor** carries out independent estimation of the "cloud services, information system operations, performance and security of a cloud implementation"[85]. Moreover security controls, privacy impacts and performance of the provided services are also being evaluated.[86]

A **cloud broker** is an entity that generally provides services targeting service intermediation, service aggregation, and service arbitrage.[87] The cloud broker "manages the use, performance

---

[80] Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'*, 16

[81] As illustrated in table 2 "Consumer activities" of Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'*, 18

[82] Ibid., 19

[83] Ibid.

[84] As illustrated in table 2 "Provider activities" of Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'*, 18

[85] Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'*, 24

[86] Ibid.

[87] Ibid., 25

and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers".[88]

A **cloud carrier** has the role on an intermediary because by providing "connectivity and transport" of cloud services it makes the link between cloud consumers and cloud providers possible.[89] The access a cloud carrier provides is possible via the use of network, telecommunication, and other such types of access devices.[90] For instance computers, laptops, mobile phones, mobile Internet devices make it possible for a consumer to receive cloud services.[91] Cloud services are usually provisioned by network and telecommunications operators or by a transport agent.[92] A transport agent can be "a business organization that provides physical transport of storage media such as high-capacity hard drives".[93] Additionally, it is worth mentioning that service level agreements (SLAs) are going to be established between cloud carriers and cloud providers.[94] This type of agreements reflects the general terms and conditions regarding the service level offered to cloud consumers.[95] To this end, the cloud carrier may be requested to assure "dedicated and encrypted connections between cloud consumers and cloud providers".[96]

Focusing even more on the link that has to be put in place so that the end-user becomes able to consume cloud services, we would like to make additional specifications that this link runs over an IP network and can be anything from DSL to mobile such as GPRS and 3G to wireless.[97] Moreover, in any of the used architectures, users have to enjoy the same quality and "feel".[98] Furthermore, it is important to keep in mind the fact that a cloud carrier does not necessarily have to be a cloud provider as well. In fact, third parties usually operate this link.[99] Therefore, the conclusion is that the relationship created between cloud providers and

---

[88] Michael Hogan and others, National Institute of Standards and Technology, *'Cloud Computing Standards Roadmap – Version 1.0'*, 25

[89] Ibid.

[90] Ibid.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Ibid.

[95] Ibid.

[96] Ibid.

[97] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 8

[98] Ibid., 10

[99] Ibid., 9

internet service providers (ISPs) is the one actually responsible for enabling the provider to "branch out of the cloud"[100] and reach the customer.

To sum up, the access provisioning scenarios are either cloud providers that operate the link themselves hence bearing a double role of cloud service provider and internet service provider or a cloud provider that entered into an agreement with an ISP in order to deliver the services. Complicating things even further, it can happen that the customer be accessible by a "succession of ISPs" in the eventuality of data portability".[101] However, an important aspect to be considered is that while clouds have a global reach, ISPs have the disadvantage that they are physically connected to a certain jurisdiction.[102]

3. Cloud characteristics, applications and benefits

One of the key elements of cloud computing is the shift from viewing software and computer power as products, to purchasing them as services on an as-needed basis.[103] The most popular characteristics of cloud computing are related to the economics of this model – cost reduction and resource efficient allocation being thus among the strongest factors that currently lead to new business models.

Apart from cost reduction, cloud computing allows organizations to focus time and resources on substantial tasks operations[104]. Therefore, the degree of flexibility, be it for sourcing purposes, for testing new services or for performing secondary business applications represent important assets as well.[105]

For mere end consumers, the possibility to access their data from any internet location allows to remain productive.[106] Another advantage is that it facilitates sharing and permits

---

[100] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 10

[101] Ibid., 17

[102] Ibid., 18

[103] Christopher S. Yoo, *'Cloud Computing: Architectural and Policy Implications'* (2011) Technology Policy Institute, 4 <http://www.techpolicyinstitute.org/files/yoo%20architectural_and_policy_implications.pdf accessed 7 January 2012

[104] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*, 19

[105] Ibid.

[106] Christopher S. Yoo, *'Cloud Computing: Architectural and Policy Implications'*, 11

collaboration among multiple users.[107] Moreover, while it allows for vast storage space, the re-provisioning of the cloud infrastructure is identified as an opportunity with regards to availability and resilience.[108]

Therefore, the economics of scale and the removal of on-site infrastructure deployment and management are some of the major benefits of cloud computing.[109] Other benefits worth mentioning are the reduction of capital investments, of software updating and licensing costs and reallocation of staff and other resources.[110]

Despite RAND Europe's warning that these benefits have been only asserted in market literature, it is important to see that public institutions such as the City of Los Angeles, the Danish National IT Agency and a EU Member State eHealth Provider adopted the cloud model[111].

Interestingly, the European Expert Group Report made a distinction between three types of challenges related to cloud environments.[112] First, the *non-functional* challenges refer to the qualities or properties of the system such as elasticity, reliability, quality of service, agility, adaptability and availability.[113] Second, the *economic* considerations revolve mainly around cut reduction, pay per use, improved time to market, return of investment, turning CAPEX into OPEX and going "green".[114] Third, the identified *technological* challenges are virtualization, multi-tenancy, security, privacy and compliance, data management, APIs and/or programming enhancements, metering and development of tools.[115]

However, a complete list of applications and benefits of cloud computing is difficult to present due to the vastness of possible ways in which it can be used.

In conclusion, as the European Expert Group Report states,

---

[107] Christopher S. Yoo, *'Cloud Computing: Architectural and Policy Implications'*, 11

[108] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*, 7

[109] Ibid., 18

[110] Ibid.

[111] Ibid.

[112] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, 12

[113] Ibid.

[114] Ibid.

[115] Ibid.

"cloud technologies and models have not yet reached their full potential and many of the capabilities associated with clouds are not yet developed and researched to a level that allows their exploitation to the full degree, respectively meeting all requirements under all potential circumstances of usage.

Many aspects are still in an experimental stage where the long-term impact on provisioning and usage is yet unknown. Furthermore, plenty of as still unforeseen challenges could arise from exploiting the cloud capabilities to their full potential, involving in particular aspects deriving from the large degree of scalability and heterogeneity of the underlying resources."[116]

4. Identified opportunities for Europe

The European Expert Group report identified, in tight connection with the telecommunication industry, the following opportunities for cloud computing in the near future.[117] First, since it is anticipated that telecommunications companies will deliver cloud offerings, accent should be put on the constant development of cloud infrastructures.[118] In this sense we consider necessary to mention that already more and more telecommunication companies such as Telefonica[119] and BT[120] are offering cloud computing services to users and businesses. Second, a business opportunity emerges for the telecommunications sector as well as for major IT and other companies which do not fully exploit their hardware resources.[121] Third, leveling up with the development of goods, services and capital, Europe has the opportunity

---

[116] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010',* 1

[117] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010',* 3

[118] Ibid., 3

[119] Telefonica, Public Consultation on Cloud Computing (30 August 2011) 2 <http://www.publicpolicy.telefonica.com/blogs/wp-content/uploads/2011/01/Respuesta_consulta_Cloud_Computing.pdf> accessed 7 January 2012 and Telefonica, *'Cloud Computing isn't just a buzzword'* (19 May 2011) <http://www.publicpolicy.telefonica.com/blogs/blog/2011/05/19/cloud-computing-isn%E2%80%99t-just-a-buzzword-2/> accessed 7 January 2012 and Anuradha Shukla, *'Sierra and Telefonica Announce New Cloud Computing Service'* (22 February 2010) <http://hosted-voip.tmcnet.com/feature/articles/76395-sierra-telefonica-announce-new-cloud-computing-service.htm> accessed 7 January 2012

[120] Lewis Dowling, *'BT says cloud gaming "just the start"'* (22 September 2011) <http://www.totaltele.com/view.aspx?ID=467896> accessed 7 January 2011 and Global Telecoms Business, *'BT offers Ribbit cloud phone service'* (3 November 2009) <http://www.globaltelecomsbusiness.com/Article/2330030/Sectors/25197/BT-offers-Ribbit-cloud-phone-service.html?Type=Channel&ArticleID=2330030&ID=25197> accessed 7 January 2012

[121] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010',* 3

to develop a "free market of IT services".[122] It is emphasized that the telecommunication industry is expected to "supplement" the basic ISP services with cloud offerings. Last, the consolidation of guidelines for helping businesses to easily accommodate the migration and efficient usage of clouds is also seen as an opportunity.[123]

It is important to highlight the analysis conducted by RAND Europe. The analysis lists several European policies that raise issues of cloud computing applicability or that present opportunities to improve the policies in order to obtain better objectives. Among the listed legislation, we would like to mention: the E-Commerce Directive 2000/31/EC which raised the issue of linking the applicable law to physical location, the ePrivacy Directive 2002/58/EC which leaves no possibility for breach notification rules to apply to cloud service providers and which also does not allow the fulfillment of communications secrecy obligations, and Data Retention Directive 2006/24/EC which raises the issue of applicability of data retention rules.[124] These provisions will be further addressed in chapter four.

Moreover, the European Expert Report made a recommendation in the same sense as RAND Europe, for EC together with Member States to set up the right regulatory framework to advance the adoption of cloud computing.[125]

Conclusion

RAND Europe's investigation concludes that the intricacy of issues associated with cloud computing is sufficient to justify the development of entirely new public policy approaches.[126] Furthermore, RAND Europe expresses the fact that only with the involvement of public policymakers at both the European and national level the economic benefits of cloud computing can be achieved while putting prize on European values at the same time.[127]

However, along the line of this paper we will also see other points of view and arguments in a sense that it is not entirely appropriate to intervene with a targeted legal regime addressing cloud computing.

---

[122] European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*, 3

[123] Ibid.

[124] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*, 8 and 86-93

[125] European Commission Expert Group Report, '*The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010*', 3

[126] Ibid., 15

[127] Ibid., 12

CHAPTER TWO - Overview of the telecommunications regulations

This chapter will first present an overview of the telecommunications regulation from the 1980s up to present days. Additionally, short remarks will be underlined regarding the factors that triggered the revision of the telecommunications regulation time and again. After pointing out the chronological stages, the last part of this chapter will present two major elements that are inherently related to the telecommunications framework. In this sense, the author will first briefly touch upon the net neutrality debate. Following this, the issue of convergence will be presented. Notwithstanding the complexity of these issues, although the analysis this chapter may be too narrow in relation to their inherent problematic, still this author considers it important to highlight their significance for cloud computing. Additionally, the final part of this chapter analyzes a very interesting position of professor's Kevin Werbach from University of Pennsylvania and makes use of the American model to make projections and assumptions of how it is best to tackle the wave of concerns cloud computing has brought about. Unavoidably, the remarks revolving around regulatory approaches were triggered by the intense debates and widespread uncertainty related to the regulatory provisions applicable to cloud. Nevertheless, these observations enhance our research with substantial insight.

Prior to the 1980s, the telecommunications sector was characterized, in the majority of cases, by a single operator owned or controlled by the state. However, this was contradictory with one of the fundamental principles of the European Community Treaty (EC Treaty), namely a single internal market.[128] Therefore, articles 31, 86 and 295 EC Treaty[129] together with the European Court of Justice (ECJ) case law[130] point out that the creation of monopolistic undertakings is in breach of the Treaty's provisions.[131] Additionally, globalization, the development of new technologies and the competitive challenge from the USA, UK[132] and Japan[133] triggered the process of liberalization for the telecommunication industry. As a consequence, in the 1990s the full liberalization procedure was initiated. In this sense, the

---

[128] Robert Klotz, The Liberalization of the EU Telecommunications Markets in Christian Koenig and others (eds), *EC Competition and Telecommunications Law* (Kluwer Law International 2009), ch 3, 53

[129] European Union, Consolidated versions of the Treaty on European Union and of the Treaty Establishing the European Community European Union 29.12.2003

[130] Case C-202/88, *France v. Commission*, [1991] ECR I-1223

[131] Robert Klotz, *EC Competition and Telecommunications Law*, ch 3, 55-56

[132] Peter Humphreys and Seamus Simpson, *'Globalization, the Competition State and the Rise of the "Regulatory" State in European Telecommunications'* (2008) 46 (4) JCMS, 851 <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5965.2008.00802.x/pdf> accessed 19 January 2012

[133] Robert Klotz, *EC Competition and Telecommunications Law*, ch 3, 56

Commission adopted seven European Community (EC) directives having as general purpose to eliminate the monopoly of the telecommunication infrastructures and services.[134] Moreover, with the aim to promote fair competition, the directives were supplemented with the Open Network Provisions (ONP) – an instrument favoring entrant operators on the market - and a regulation on unbundled local loop access.[135] Following this, in pursue of a "harmonized pro-competitive regulatory regime"[136], in 2002, 2007 and 2009 a sequence of policy reviews took place.

Before going into details regarding the focus of these reviews, in order to understand the scale of this phenomenon, two major facts need to be reminded. First, it is important to note that in 1990 there were only 12 countries in the world that had regulatory agencies functioning independently from telecommunication operators.[137] The regulatory agencies were not under the authority of the government ministries or postal, telegraph, and telephone services (PTTs), thus they enjoyed a certain level of autonomy. However, just 10 years after that, this number exploded to more than 96.[138] The second aspect worth mentioning is that during the revision process, certain international agreements adopted several of these reforms.[139] For example, the World Trade Organization (WTO) not only enshrines the basic trade rules that apply to telecommunications in the General Agreements on Trade in Services (GATS) but also includes an Annex on Telecommunications that guarantees for reasonable access to and use of public telecommunications.[140] More importantly, WTO also adopted a Reference Paper that sets out the basic definitions and principles on the regulatory framework for the basic telecommunications services.[141]

In brief, the 2002 review concentrated on assembling a regulatory outline. The regulatory structure included the framework directive and four specific directives: Access, Authorization, Universal Services and Privacy directives which serve the role of "promoting

---

[134] Robert Klotz, *EC Competition and Telecommunications Law,* ch 3, 57

[135] Ibid.

[136] Peter Humphreys and Seamus Simpson, *'Globalization, the Competition State and the Rise of the "Regulatory" State in European Telecommunications'*, 851

[137] Hank Itven and others, Telecommunications Regulation Handbook, *Module 1 - Overview of Telecommunications Regulations* (*Info*Dev Program of the World Bank 2000), 3 <http://rru.worldbank.org/Documents/Toolkits/telecom_mod1.pdf> accessed 19 January 2012

[138] Ibid.

[139] Ibid., 23

[140] See World Trade Organization, General Agreement on Trade in Services, available at

<http://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm> accessed 4 February 2012

[141] See World Trade Organization, Negotiating group on basic telecommunications, available at <http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm> accessed 4 February 2012

competition through maximizing consumer benefits, creating a harmonized enforcement practice and promoting the interests of EU citizens related to consumer and data protection and universal service".[142] Importantly, through the means of this type of regulation, new entry operators are awarded access to the networks and services of the already established operators.[143] Needless to say, this mechanism was designed to create effective competition as a main contributing factor to Europe's position as an important economical player. It is important to note that the Framework Directive does not cover the content of services delivered over electronic communications networks and services[144] and that it does not apply to telecommunications terminal equipment.[145]

Moreover, a regulation of roaming on public mobile telephone networks was adopted. Its aim was that consumers pay clear and low prices for roaming services when they are traveling across Europe.[146] However, despite the continuous efforts to complement the telecommunications framework, two major flaws were observed by the Commission and triggered another review in 2007. The first obstacle was the segmentation of the single market into national markets seen at an individual level and the second shortcoming was a certain lack of consistency observed in the application of the regulatory framework.[147]

Furthermore, consenting that telecommunications are at the backbone of a world-wide information society and that they represents the gateway to global economic activity, the "Telecoms Package" was amended in December 2009 by the two Directives "Better law-making" and the "Citizens' rights", as well as by a body of European regulators for electronic communications.[148] Recognizing the on-going sequence of changes, the revised EU rules

---

[142] See article 8 (2), (4) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, hereinafter referred to as the "Framework Directive" and Robert Klotz, *EC Competition and Telecommunications Law*, ch 3, 89

[143] Robert Klotz, *EC Competition and Telecommunications Law*, ch 3, 89

[144] Recital 5 of the Framework Directive

[145] Recital 8 of the Framework Directive

[146] The roaming regulation was amended in 2009 and it was concentrated on lowering voice call roaming prices and adopting the "Euro SMS tariff". For additional information see Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/activities/roaming/regulation/archives/current_rules/index_en.htm> accessed 4 February 2012

[147] Christian Koenig and others (eds), *EC Competition and Telecommunications Law*, (Kluwer Law International 2009), foreword xxxiv

[148] European Commission, Summaries of EU legislation, Information Society <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm#amending act> accessed 19 January 2012

were related to offering a better protection to consumers[149], ensuring an open market, advocating financing directed at new communication infrastructures such as radio spectrum and wireless broadband services, and increasing the trustworthiness and safety of communication networks.[150]

As a side note, which is relevant to our discussion about cloud computing, we need to point out that the new power awarded to national regulators to impose, after consulting with the Commission, a certain quality of service for network transmission services[151], may represent either a valuable instrument that will enable cloud operations to function without distortions or negative impact on clients' activities or a cumbersome pressure if the duty will not be weighted and imposed appropriately.

Furthermore, the new regulation that establishes the Body of European Regulators for Electronic Communications (BEREC) has the function to assure concordant regulation across Europe and to consolidate the telecommunication industry market.[152] In this respect, BEREC will work closely with the National Regulatory Authorities (NRAs)[153] and the Commission as an attempt to dissolve the unconsolidated cooperation with the "European Regulators Group". Furthermore, BEREC will "assist, advise, and complement" the work of national telecommunications regulators when dealing with regulatory decisions of European relevance.[154] Thus, by establishing this body, a more "transparent and efficient approach" is to be achieved regarding regulatory matters substantially impacting the European market. Another important attribution for BEREC and the Commission is the power to oblige national

[149] The desire to strengthen consumer rights is translated by introducing enhanced rights with regards to access, information, quality of service, privacy and data protection.

[150] Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/policy/ecomm/eu-rules/index_en.htm>

[151] Article 22.2 of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.4.2002, hereinafter referred to as the "Universal Service Directive".

[152] Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/eu_consultation_procedures/index_en.htm>

[153] The term "national regulatory authority" is defined in article 2 lit. g) of the Framework Directive as the "body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives". Moreover, article 3 of the Framework Directive provides that the competent body appointed by Member States needs to be a distinct, independent entity from all organizations providing electronic communications networks, equipment or services.

[154] Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm>

regulators to renounce its envisioned regulation if the two bodies conclude that the remedy would hamper competition in the telecoms market sector.[155]

These new rules were to be transposed into the Member States' national laws by 25 May 2011. However, on the 24th of November 2011, 6 months after the deadline, the Commission has started the infringement procedure by addressing a "Letter of Formal Notice" to 16 Member States.[156]

As a closure to the telecommunication chronological evolution, we would like to remind the reader that, even putting aside any cloud policy investigations per se, the transformation of a single voice market to the "triple play" video, voice and data network architecture still forces a re-evaluation of our regulatory models and understandings. To support this statement, as Timothy Tardiff points out, the evolution implies a completely new competition architecture and industry construction.[157] In this sense, we can refer to the Malaysian government as a pioneer in adopting laws on convergence.[158] Moreover, in India there have been discussions about a Communications Convergence Bill but it is unclear whether the Government will decide to take steps to implement it.[159] Furthermore, as professor Yu-li Li shows, in Japan, Taiwan, Korea and Hong-Kong there are similar attempts towards adopting a "Comprehensive Legal Structure of Information and Communications".[160] Finally, to conclude, John Janowiak, Senior Director of the International Engineering Consortium (IEC) advises the traditional telecommunication operators to start "reinventing" themselves in order to maintain a competitive advantage in the 21st century IP-based network.[161] Therefore,

---

[155] For this remark together with a list of the main elements of the reform see Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm>

[156] European Commission, Press release, *'Digital Agenda: Commission presses 16 Member States to implement new EU telecoms rules'* (24 November 2011) IP/11/1429 <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1429&format=HTML&aged=0&language=EN&guiLanguage=en> accessed 7 January 2012

[157] Timothy Tardiff, *'Changes in industry structure and technological convergence: implications for competition policy and regulation in telecommunications'* (2007) 4 IEEP, 109 <http://www.springerlink.com/content/wg612681347lk809/fulltext.pdf> accessed 9 January 2012

[158] See Malaysian Communications and Multimedia Commission Act 1998 <http://www.skmm.gov.my/link_file/the_law/NewAct/Act%20589/Act%20589/a0589.htm> accessed 10 January 2012

[159] The ICT Regulation Toolkit, Practice Notice, *'India's Communications Convergence Bill'* (last updated 2 February 2012) <http://www.ictregulationtoolkit.org/en/PracticeNote.1222.html> accessed 10 January 2012

[160] Yu-li Liu, *'The Impact of Convergence on Telecommunications Law and Policy: A Comparison between Japan and Taiwan'* (2009) 1 <http://www.koryu.or.jp/08_03_03_01_middle.nsf/2c11a7a88aa171b449256798000a5805/417089fe85025d5c492577450035aa00/$FILE/liuyouli.pdf> accessed 10 January 2012

[161] John R. Janowiak, *'Convergence, the law and the future of the ICT sector'* (2005 North America) *<http://www.connect-world.com/~cwiml/index.php/magazine/global-ict/item/1070-convergence-the-law-and-the-future-of-the-ict-sector> accessed 10 January 2012*

consistent with the identified opportunities for Europe described in the first chapter, we can observe that telecommunications and cloud computing perform under the same spot light on the European stage.

Following the chronological transformations of the sector we will also consider relevant to touch upon two substantial aspects related to the telecommunications sector. However, we note the fact that the discussion related to them is not only far more complex and vast but also acrimonious and much more subtle than the scope of our research allows us to perform. Therefore, we will first briefly present the net neutrality debate followed by relevant issue springing from the issue of convergence.

Tightly connected to the reform and to the idea of Trans-European Networks (TEN) as catalyst of a single internal market, are the "net neutrality" and "net freedoms" guarantees. By promoting the open and neutral character of the internet, the new rules aim to offer the consumer a diversity of choice regarding providers[162], supported by facile switch of operators, more transparency[163] and more information regarding the conditions limiting access of services and applications and the service quality they should expect. Needless to point out the importance each of the above directions have on both traditional telecommunications aspects as well as cloud related activities since they set forth the guidelines for their operational activities. On a contrasting point of view, Lehr launches the hypothesis that along with the transformation of wired provider networks into convergence models, the regulatory focus on technology neutrality will become less significant.[164] Additionally, the same author explains why the availability of technical options represents both a challenge and a temptation in the view of policy regulation. Lehr first states that the challenge comes from the duty to acknowledge and grasp the technical differences leading to substantial policy and economic implications. Second, he shows that the temptation lays in the abstention to automatically disregard the differences between networks and services that due to technological innovation appear to function as substitutes because of their similar construction model and operation functions.[165] Therefore, by projecting his reasoning to the cloud example we can see that the model perfectly applies to the author's ideas. To complement this statement, the next chapter will further develop on the cloud comprising elements which point to the "regulatory temptation" mentioned above.

---

[162] Article 8.(4).(g) of the Framework Directive

[163] Article 21 of the Universal Service Directive

[164] William Lehr and John Chapin, *'On the convergence of wired and wireless access network architectures'* (2010) 22 Information Economics and Policy, 38 following on the idea initiated by Tim Wu <http://www.sciencedirect.com/science/article/pii/S0167624509000778> accessed 9 January 2012

[165] William Lehr and John Chapin, *'On the convergence of wired and wireless access network architectures'* (2010) 22 Information Economics and Policy, 40

In connection to the "study of implications of cloud computing on the design of telecommunications network"[166], a second relevant discussion issue is convergence.

Before going into details about this aspect, we would like to express one comparative idea which further stresses the significance of cloud computing and recognizes its value for the European Union. As a general remark, we can observe that the telecommunication sector is destined to recurrent regulatory revisions. Although dealing with problems at different levels, as a parallel, perhaps the challenge of a clear regulatory framework for the cloud model represents in present times what the lack of competitiveness due to state monopoly meant in the 1980s: an impediment towards having a variety of "diverse, sophisticated and affordable services".[167] Given the amplitude of the cloud phenomenon, we can perhaps speak of a second era of sort of "liberalization", in a sense that the same consequences are sought nowadays such as they were 30 years ago. In this respect, the Commission comes forward with a cloud computing plan and strategy for Europe.[168] We cannot identify differences between this new strategy and the goal enshrined at the inception of the liberalization process. Both are intended to contribute to the stabilization of a single internal market and both are used as tools to serve the economical objectives of the European market. However, as we have briefly touched upon in the past section, the major issue revolving the telecommunications sector at the moment lies with one of its intrinsic characteristics, convergence. Convergence reveals a number of regulatory challenges, however due to the complexity of the issue in question, only a limited number of problems can be fitted in this research. Moreover, a short note has to be considered related to the trends surrounding convergence. There have been identified two trends of convergence; the first one represents the convergence between telecommunications and ICT and the second one presupposes the convergences of telecommunications and media, thus content related services.[169] Moreover, as Jones identifies, we can speak about three levels of convergence, namely in relation to the infrastructure, in relation to the content and at end user terminals.[170] Therefore, because of the multitude of services and industries that are now

---

[166] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 6

[167] Peter Humphreys and Seamus Simpson, *'Globalization, the Competition State and the Rise of the "Regulatory" State in European Telecommunications'*, 851

[168] On 27th of January 2011, Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes publicly announced the initiation of a EU-wide cloud computing strategy. See European Commission, *'Towards a European Cloud Computing Strategy'* (27 January 2011) SPEECH/11/50 <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50> accessed 7 January 2012. For reference to the Digital Agenda see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>

[169] For a detailed overview see Antonio Alabau and Luis Guijarro, *'The Electronic Communications Policy of the European Union'* (2011) Editorial Universitat Politecnica de Valencia, available at <http://personales.upv.es/lguijar/book/AlabauGuijarro2011en.pdf>

[170] Andrew Jones, *'Convergence'* (2007) 12 (2) Information Security Technical Report, 70 <http://pdn.sciencedirect.com/science?_ob=MiamiImageURL&_cid=271961&_user=522558&_pii=S136341270700009X&_check=y&_origin=article&_zone=toolbar&_coverDate=31-Dec-

colliding, the discussion related to cloud computing is not a simple one if we were to associate these services to telecommunications.

While still tackling with the discussion about convergence, we consider valuable to express some interesting points illustrated by Kevin Werbach in his recent article, The Network Utility[171]. The reason for focusing on this article is that the author gives another perspective on the regulatory challenges of cloud computing. In this respect, the idea expressed above – that the lack of a clear way to address the regulatory problem of cloud computing represents an impediment for having a rich palette of advanced and inexpensive services – earns itself another viewpoint. This new viewpoint is rooted in the past regulatory approach experience the United States Federal Communication Commission (FCC) had with computer utility. Given the interrelation of computer utility and cloud computing, we consider valuable to present Werbach's opinions. Therefore, the author makes an interesting comparison between the regulatory challenges that cloud computing gives raise today and the discussions revolving computer utility that took place in the 1960s. Interestingly, back in that period, the FCC decision not to intervene directly with the incumbent computer utility model led, as the author points out, to the culminant success of the IT sector.[172] In his opinion, the resemblance of issues and regulatory challenges between cloud computing and computer utility is a striking one. Therefore, it is appropriate to briefly mention this comparison not only because it leaves room for nowadays cloud computing possible regulatory approaches and previsions but also because we have to admit that Europe has a tradition to look to its American neighbors when it comes to making policy decisions. To support this statement, perhaps the most relevant example for our topic is precisely the shift to liberalizing the telecommunications sector[173]. Consequently, we can expect that the European arena will closely monitor and recourse to American decisions. Therefore, we find this article particularly relevant because, although seen through American eyes, it accurately illustrates the cycle of the cloud computing phenomenon. By a "normal development cycle", we mean the fact that cloud computing represents the normal evolution of the fundamental idea based

---

2007&view=c&originContentFamily=serial&wchp=dGLbVlS-zSkzk&md5=2bebfc28bd4b8684674b0547f3468538/1-s2.0-S136341270700009X-main.pdf> accessed 19 January 2012

[171] Werback Kevin, *'The Network Utility'* (2011) 60 Duke L. J. 1761-1840 <http://scholarship.law.duke.edu/dlj/vol60/iss8/3/> accessed 10 January 2012

[172] Ibid., 1762

[173] Another example launched by our American counterparts was the net neutrality debate. Also originating in USA was the issue of liability of online intermediaries which we will discuss in the forth chapter (see Charlotte Waelde and Lilian Edwards, *'Online Intermediaries and Liability for Copyright Infringement'* (2005) WIPO Workshop Keynote Paper Geneva, 4 < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159640> accessed 6 February 2012)

on computer utility and that it responds to nowadays economical and daily activity needs in the same way computer utility did in the 1960s.[174]

However, the FCC's decision not to intervene regarding computer utility leaves room for an interesting analysis given the fact that, although computer utility meant in 1960s a revolutionary change for the information technology sector, the approach of the regulatory body proved to be the most suitable and with a positive impact for the market. We find this decision very interesting because it is not often for a regulatory body to have the necessary wisdom, maturity and vision to restrain from using its power and to be capable of foreseeing what is best for market and societal needs. Consequently, we believe this is an important lesson for the current European debate regarding cloud computing.

As a result, Werbach's article brings about important questions. First of all, we cannot restrain from wondering what would have meant if the FCC addressed the convergence of computing and communication directly. How would it have been different and why would it not mean the same "spectacular success"[175] for the IT industry? To find the answer to these questions is beyond the scope of this paper but perhaps it is useful to specify the fact that the same author admits that the FCC's decision not to directly address both the issue of "computers as users of communications and computers as a form of communication"[176] led, on a long run, to disbelief and confusion.[177] Nowadays, a possible way to look at this phenomenon is as a second cycle of development[178], a cycle that is more accurately responding to economical and individual needs. Impressive figures come to back up this statement such as the economical previsions and the increasing number of corporate cloud users.[179] Therefore, to affirm that leaving the cloud computing model to develop itself and not intervene through regulation will not have the same beneficial results as non-state intervention had for computer utility would not be out of place. However, a 360-degree perspective must be taken into account when assessing this issue.

---

[174] In this sense, as Walfredo Cirne from Google's infrastructure group in California, USA states in an interview, "cloud computing is really an evolutionary step on how we use computers". See Gordon Blair and others, *'Perspectives on cloud computing: interviews with five leading scientists from the cloud community'* (2011) J Internet Serv Appl <http://www.choreos.eu/bin/download/Download/UsefulResources/CHOReOS-InternetOfServices-Paper-June11.pdf> accessed 19 January 2012

[175] Werback Kevin, *'The network Utility'*, 1762

[176] Ibid., 1840

[177] Ibid., 1762, 1840

[178] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 2

[179] Forrester Research predicts a rise of the current 40.7 billion dollars global value market of cloud services to 241 billion dollars by 2020. See Kiril Kirilov, Cloud Tweaks, *'Cloud Computing Market Will Top $241 Billion in 2020'* (26 April 2011) <http://www.cloudtweaks.com/2011/04/cloud-computing-market-will-top-241-billion-in-2020/> accessed 10 January 2012

Additionally, although due to the limitation of this study we cannot extrapolate it too far, we would like to make reference to the Collingridge dilemma[180]. In this sense, it is appropriate to mention the dilemma that might exist at the moment regarding cloud computing. On this account, it appears that there are sector-specific rules that address to cloud related issues such as security, privacy and liability and therefore the patchwork of provisions might lead to significant inconsistencies.[181]

In addition to the already illustrated regulatory challenges, several reports and communications from the European Commission are an indication of the deficiencies in existing regulation, which currently leave the cloud model exposed and forced to grow on unstable grounds. In this respect, we can mention the recently released report [182] on the outcome of the public consultation of the third periodic review on Universal service in e-communications, the Communication on the open internet and net neutrality in Europe released on the 19th of April 2011 and the public consultation on personal data breach notifications under ePrivacy Directive which has ended on the 9th of November 2011.

Indisputably, the regulatory issue still revolves around the duality of networked computers relying on communications as their backbone and networked computers as utilities in themselves.[183] Needless to say, the convergence of technology and industry structure is no longer in an incipient phase. It has become the normality of present times, therefore many authors have argued that a clear and balanced position must be put forward.

Up until now, we have seen the parameters of the telecommunications and we have presented its sequential stages of revision. The reason behind presenting this chapter was to provide it as means to allow us to move forth inside the limits of our conducting research. Moreover, it proved to endow our study with the complexities of the possible approaches legislators may need to consider in the eventuality of a new cloud policy.

---

[180] The Collingridge dilemma means reflecting whether the legislator should intervene at an early stage of development of the technology in question or to postpone the intervention until a more mature stage of development. See David Collingridge, *The Social Control of Technology* (Pinter, 1980) as referred to by Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'* (2010) 33 European Law Review 2008, 881 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1645524> accessed 6 February 2012

[181] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 881

[182] See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Universal service in e-communications: report on the outcome of the public consultation and the third periodic review of the scope in accordance with Article 15 of Directive 2002/22/EC (23 November 2011) COM (2011) 795 final <http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/universal_service/comm_us_en.pdf> accessed 7 January 2012

[183] Werback Kevin, *'The network Utility'*

CHAPTER THREE - Parallel between cloud and telecommunications relationships

This chapter has as a primary goal to build a parallel between the relationships specific to the cloud model and those related to telecommunications. Whereas there is significant indication that information society provisions apply to cloud computing, this analysis is meant to shed light in respect of the possible applicability of telecommunications regulations to the cloud. Given the acknowledgment of this complexity, we will perform a definition analysis in an attempt to decipher the circumstances in which the telecommunications regulation will unavoidably apply to cloud providers. With this scope in mind, the investigations are based on the electronic communications and information society services definition provisions. Furthermore, we will also dissect the cloud elements in order to see if we can speak of an overlap between cloud and telecommunications.

As a preamble to the core analysis of this paper, this section first observes the developments which led some to assert the need for a substantial and immediate approach towards cloud computing. Having this in mind, we will highlight the regulatory trend in relation with the telecommunications sector and see how it relates to cloud computing. Furthermore, we will hypothesize along the approaches legislators could consider when discussing a cloud policy proposal and subsequently, some remarks will follow regarding the eligibility of the telecommunications framework for the "cloud strategy". Additionally, we will refer back to Werback's statement supporting a regulatory approach addressing convergent services to point out another reason why cloud could become the instigator of a major policy reassessment.

We will begin by reminding the technology sector-specific developments and their essential dependence on and interrelation with telecommunications. In this sense, we point out the fact that the rapid evolution of technology and the dynamic growth of data communications, broadband networks and internet-based services determine a constant change for communications technologies and services.[184] At the same time, as some authors have pointed out, convergence between telecommunications, media and information technology sectors urges significant regulatory attention. These two factors, combined with the fact that all transmission networks and services should be covered by a single regulatory framework[185] can point to the conclusion that the effects that the cloud model will have on economic activities will require a new policy strategy.[186] Continuing on the same line of thinking, we can also assume that, with the contingency of a new "cloud directive", it might be easier to

[184] Europe's Information Society Thematic Portal <http://ec.europa.eu/information_society/policy/ecomm/index_en.htm>

[185] Recital 5 of the Framework Directive

[186] RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'*

integrate the new piece of regulation to the "Telecom Package". Therefore, it may be easier to add up regulation in this manner rather than adopt a stand-alone product. As a supposition, we can launch the hypothesis that there is the need for a systematic movement of integrating the cloud computing model within legal boundaries because a linear approach would be neither sufficient and effective enough nor plausible for the cloud model to be seen as an individual sector.[187] Additionally, given the lack of a clear shape of the regulatory sphere applicable to cloud computing, this can serve as another reason why a linear approach would not be appropriate.

However, the telecom framework can prove to be of help. In fact, as a trend ever since liberalization, the convergence of communications and broadcasting technology forced the EU to reshape the regulatory boundaries to include all "electronic communications networks and services" in a new regulatory framework.[188] Linking back to Werbach's conclusion that dealing only with computers reliant on communications and leaving aside the issue of the convergence of the two industries leads to an unbalanced and undesirable situation characterized by general skepticism[189], we can easily admit this is not at all desired particularly because of the serious legal and economical implications. On the contrary, it is the appropriate time to intervene and channel these implications in foreseeable and controllable consequences. For this reason, the acknowledgement of the possible trajectories might prove to be useful for legislators. Therefore, the aim of this introduction was to analyze the possible regulatory approaches and to specify the possible arguments for a trajectory leaning towards cloud offerings ruled by telecommunications provisions.

Nevertheless, however useful it may be to preach for an integrated piece of regulation, the current relationships within and in conjunction with the telecommunication sphere need to be carefully examined so that consistent deductions can be later expressed.

Ideally, the telecommunications' sector expectations are directed towards avoiding their cloud offerings to be classed as telecommunication services.[190] One reason for this might be because cloud services resemble[191] hosting and outsourcing, thus they should be categorized as

---

[187] This statement is based on two arguments. First there will be no point in building a piece of regulation because cloud computing is not a new technology; instead the model is merely unraveling a series of loopholes in legislation. Second, the fact that convergent services *in general* would require more regulatory attention add up to concluding that a linear approach would not be appropriate.

[188] Europa, Gateway to the European Union <http://europa.eu/pol/infso/index_en.htm> accessed 7 January

[189] Werback Kevin, *'The network Utility'*, 1762

[190] E-mail from David Callahan, Deputy Head of Unit, Software & Service Architectures and Infrastructures, European Commission DG INFSO to author (22 November 2011)

[191] Andrew Joint and Edwin Baker, *'Knowing the past to understand the present – issues in the contracting for cloud based services'* (2011) 27 (4) Computer Law and Security Review, 411 <http://www.sciencedirect.com/science/article/pii/S0267364911000689> accessed 10 January 2012 and Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 6. However, in a recent European Commission

information society services. However, as we can notice in Joint and Baker's article[192], the contractual differences between cloud and outsourcing deals clearly show that the two cannot be aligned together because of fundamental differences[193]. Therefore, this argument is not solid enough to be the *sole* basis for eliminating the possibility of cataloguing cloud offerings as electronic communications services and consequently putting them alongside the information society services. Having this turn, the following section of this chapter will award intensive attention to the attempt to set the demarcation line between cloud services, information society services and electronic communication services.

Additionally, it needs to be stressed that while the telecommunications regulation has sector specific application, the E-commerce regulation applies to all cloud providers established in Europe.

Returning to the remark regarding the telecommunication provider's interests of having their cloud services as information society services, the following section launches the discussion about the legal regime applicable to cloud computing.

On a more rudimental basis, the main distinction between telecommunications and information society services is that "telecommunications concerns the cables and other transmission links, while information society services are e-commerce offerings which will use telecommunications"[194]. However, pointing to the complexity of the issue we can start by briefly introducing an example that demonstrates the waterfall of questions coming from the perspective of applying the telecommunications regulations to the cloud model. In this sense, we can consider the example of a cloud provider offering Voice over IP services (VoIP)[195] to business clients. Since VoIP presents elements of both information society and electronic communications, the question to what regime this type of services might be subject to.

Cloud Computing Hearing with Telecommunications and Web Hosting Industry, the participants have agreed that indeed cloud offerings are similar to hosting services. See Meeting Note (16 November 2011) 2

[192] Andrew Joint and Edwin Baker, *'Knowing the past to understand the present – issues in the contracting for cloud based services'*, 411

[193] Among other, the authors mention the fact that cloud is a "one-to-many" model instead of tailored services as in the case of outsourcing deals. Furthermore, they show the fact that cloud services focus more on "availability rather than delivery". Moreover, in the case of IT outsourcing there is a wide range of pricing models while with cloud services the consumer is being charged on a pay-per-use basis. Additionally, other authors such as Tajudeen Abubakr in Navigating the cloud computing legal minefield shares the same view, thus affirming that cloud computing is more complex than hosting services. See Tajudeen Abubakr, TechRepublic, *'Navigating the cloud computing legal minefield'* (5 December 2011) <http://www.techrepublic.com/blog/datacenter/navigating-the-cloud-computing-legal-minefield/5142?tag=nl.e101> accessed 19 January 2012

[194] E-mail from David Callahan, Deputy Head of Unit, Software & Service Architectures and Infrastructures, European Commission DG INFSO to author (22 November 2011)

[195] Internet telephony refers to communications services (such as voice) transmitted through the Internet instead of using the public switched telephone network (PSTN). Therefore, Voice over IP represents the transmission techniques used for delivering voice communications over the Internet. See <http://en.wikipedia.org/wiki/Voice_over_IP> accessed 19 January 2012

Therefore, as many began to wonder[196], the list of questions starts with asking whether such services could be considered telecommunication services. Furthermore, if this would be the case, would specific regulations such as the Data Retention Directive 2006/24 and the ePrivacy Directive 2002/58/EC apply? Additionally, another major issue to be taken into consideration would be whether the position would be consistent throughout all the Member States.

Starting from this point, we can first indicate that telecommunication relationships resemble a spallation of interconnected pieces. Therefore, it might be of help to first look at the relevant definitions and then try to comprehend how the cloud model can be superposed. Our intention is to try to distinguish between telecommunications and information society, which determine the application of different legal regimes.

Having this in mind, first we will examine the information society services definition. After this we will look at the electronic communications services definition and cloud's constituting elements.

1. Information Society Services

To start with, recital 18 of the Information Society Service Directive 2000/31/EC[197] is the general source for looking at the defining limitation of information society services. As we can observe, the range of encompassing services is very broad, giving information society services a widespread dimension. Consequently, it presents numerous elements that embrace cloud computing as part of information society services. Just to name a few, information society services cover economic activities such as services "consisting of the transmission of information via a communication network" and services "providing access to a communication network and services hosting information provided by a recipient of the service"[198]. An interesting detail for our discussion is the fact that contract based agreements of activities which "by their very nature cannot be carried out at a distance and by electronic means"[199] do not represent information society services. However, since the cloud model allows off premises auditing, this interestingly contributes to our investigations of a

[196] E-mail from David Callahan, Deputy Head of Unit, Software & Service Architectures and Infrastructures, European Commission DG INFSO to author (22 November 2011)

[197] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), O. J. L 178, 17.07.2000, hereinafter referred to as the "E-commerce Directive".

[198] Recital 18 of Directive 2000/31/EC

[199] More specifically Recital 18 of Directive 2000/31/EC gives the example of statutory auditing.

classification of cloud in the sense that we can observe a transformation of traditional operational functions from physical to remote.

Particularly, recital 17 of the 2000/31/EC and article 1.2.a) of Directive 98/48/EC specify that information society services cover

> "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

Furthermore, the definition describes that

> "at a distance means that the service is provided without the parties being simultaneously present,
>
> "by electronic means means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
>
> "at the individual request of a recipient of services means that the service is provided through the transmission of data on individual request."[200]

Since cloud services present a strong resemblance to these elements, the initial conclusion points towards grouping cloud based offerings with information society services.

Additionally, in the last part of the above mentioned article and in Annex V[201] of the text it is specifically mentioned what does not fall under the scope of the directive. Therefore, among others, the exemptions from this annex refer to radio broadcasting services and telefax. Therefore, we observe that there is no general exemption in the directive to exclude electronic communications from the definition of information society service.

In harmony, a cloud consumer can be seen as a "recipient of service" since the term has a very broad sense.[202] Thus, "persons who provide information on open networks such as the Internet" and "persons who seek information on the Internet for private or professional reasons" are recipients of service. Without presenting disjunctive notions, we can notice that there can be a superposition between the notions of cloud consumers and recipient of services.

Additionally, if we take into consideration the characteristics of the cloud services, namely highly scalable on-demand self-services, which are paid-per-use and provided with minimal

---

[200] Article 1.2.a) of Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217, 5.8.1998

[201] Annex V of Directive 98/48/EC

[202] Recital 20 and article 2.d) of Directive 2000/31/EC

provider interaction, we can see an inclination towards a more commercial side of the service rather than a service that purely operates the transmission of data.

In conclusion, we have seen that cloud services can be easily catalogued as information society services. Yet, there are particular indications that grant us to pursue in making further considerations about the classification of cloud offerings and therefore not freeze at the application of the E-commerce Directive. Namely, the indications were first the fact that cloud computing allows a change in the very nature of some activities such as auditing because the model offers nowadays the possibility to do such types of operations "at a distance and by electronic means"[203]. Therefore, the clear limitation initially specified in Recital 18 dissipates when it comes to cloud based services. The second indication was the fact that the text presented no general exemption of excluding electronic communication based services from the scope of the directive.

Having this in mind, the following section will analyze the electronic communications definition and will try to assess whether we can speak of an overlap between cloud offerings and telecommunications. Additionally, the comprising elements of cloud computing will be analyzed with the attempt to provide further insight on the classification issue between electronic communications and information society services.

2. Telecommunication services

Before starting with the definition analysis, as a related side note, we can link back to the formerly expressed idea regarding the telecommunications industry's interest to have their cloud services seen as information society services. In this sense, revealing a certain amount of concern, we can specify that some cloud computing providers, perturbed by being catalogued to "telephone-style regulation", shifted from providing their own data center interconnections to outsourcing those services.[204]

A revised definition of electronic communication networks can be found in article 2.(a) of Directive 2009/140/EC. The amended text also contains the definition of public communications network in article 2.(d). However, the electronic communications services definition can be found in article 2.(c) of Directive 2002/21/EC.

> "(a) 'electronic communications network' means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic

[203] Recital 18 of Directive 2000/31/EC

[204] Christopher S. Yoo, *'Cloud Computing: Architectural and Policy Implications'*, 16

means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;[205]

(c) 'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;[206]

(d) 'public communications network' means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points;"[207]

It becomes clear to see that the definition of electronic communications service contains one important element which indicates the detachment from the cloud paradigm, namely the exclusion of "services providing, or exercising editorial control over, content transmitted using electronic communications networks and services".[208] Simply by interpreting the definition, other than this exception, no other impediments have been identified as to block the possibility of classing cloud services as electronic communications services.

Before moving forward with the analysis, as a clarifying note, we would like to discuss the function of the hypervisors. The reason for this is that they might trigger some confusion whether editorial control is exercised over the transmitted content.

First, it is important to mention the fact that in a virtualization setup, such as the one in cloud computing, the technical term of editorial control does not exist[209]. Second, the role of a hypervisor is to manage the available resources (processor, memory) and to distribute them based on specific rules between virtual machines such as priority and limits.[210] Additionally,

---

[205] Article 2.(a) of Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337, 18.12.2009, hereinafter referred to as "Directive 2009/140/EC".

[206] Article 2.(c) of Directive 2002/21/EC

[207] Article 2.(d) of Directive 2009/140/EC

[208] Article 2 Directive 2002/21/EC

[209] Relevant sources such as scientific journals and technical dictionaries have been searched but no definition has been found.

[210] E-mail from Radu Epure, UNIX Administrator at Gameloft to author (20 December 2011)

what can be interpreted from the legal definition of 2002/21/EC is that editorial control refers to content control as in news or pornography filters on the internet. In opposition to this concept, a hypervisor can modify certain content of communication, but only in the sense of translating the instructions between the virtual components of the virtual machine and the physical components of the computer.[211] Therefore, the only circumstance where the cloud model would be excluded from this category[212] would be when the legal definition of editorial control would be broad enough to encompass the mere distribution of data as editorial control. Since this is unlikely to be the case or to be desired in the future, we conclude that there are no reasons, solely based on definition interpretation, to force us to exclude cloud services from electronic communications services.

Moreover, a Communication issued by the Commission explains in more exact terms what is included in the Framework Directive and what is not.[213] Therefore, it is specified that infrastructure and "associated services" such as access services are covered by the directive while the services provided over networks fall outside the scope of the Framework.[214]

> (ea) 'associated services' means those services associated with an electronic communications network and/or an electronic communications service which enable and/or support the provision of services via that network and/or service or have the potential to do so and include, inter alia, number translation or systems offering equivalent functionality, conditional access systems and electronic programme guides, as well as other services such as identity, location and presence service;[215]

Following this, we need to refer to the definition of "access" from the revised Access Directive 2009/140/EC extending the definition to incorporate

> "the making available of facilities and/or services to another undertaking, under defined conditions, on either an exclusive or non-exclusive basis, for the purpose of providing electronic communications services, *including when they are used for the delivery of information society services or broadcast content services.* It covers inter alia: access to network elements and associated facilities, which may involve the connection of equipment, by fixed or non-fixed means (in particular this includes access to the local loop and to facilities and services necessary to provide services over the local loop); access to physical infrastructure including buildings, ducts and masts; access to relevant software systems including operational support systems; access to information systems or databases for pre-ordering, provisioning, ordering, maintaining and repair requests, and billing; access to

---

[211] E-mail from Radu Epure, UNIX Administrator at Gameloft to author (20 December 2011)

[212] Once again we emphasize the limitation of this conclusion, strictly relating to the interpretation of Directive 2002/21/EC definition.

[213] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 27

[214] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 27

[215] Article 2.(ea) of Directive 2009/140/EC

number translation or systems offering equivalent functionality; access to fixed and mobile networks, in particular for roaming; access to conditional access systems for digital television services and access to virtual network services."[216] (emphasis added)

Even tough this definition gains substantial significance from competition law point of view, in connection to our discussion about cloud, Sluijs and others highlighted an important question that can be addressed. In this sense, the revealed issue is whether cloud providers could call upon the access requirements set forth under the amended definition in order to obtain access to an ISP network.[217] The authors further continue the reasoning and ask whether the purpose with which access to electronic communications is used matters in any extent. More specifically, they debate whether in order for a cloud service provider to be granted access to an ISP network it is necessary to also offer electronic communications services. Unable to clarify this aspect the authors furthermore point to the already recognized difficulties content providers (and implicitly also cloud providers) face in relation to the ISP. The authors observe that ISPs are not fundamentally distinct from service providers such as providers of electronic communications networks and therefore conclude that cloud based relationships could "usefully be dealt with under the electronic communications framework"[218].

Moving forward with our analysis, we can also point out a very interesting deduction. From the per a contrario interpretation of the last sentence of the electronic communication service definition, we can conclude that an information society service which *is* entirely or partially based on transmitting signals through electronic communication networks is also an electronic communications service.[219] Therefore, as the graphical translation in figure 1 shows, there is a partial overlap between electronic communications, information society service and cloud services. In any case, we would like to underline that the overlap cannot be extended to a general incorporation of all cloud services (S/P/IaaS).

Moreover, when debating this finding with technical experts and field advisors, we have been helped to support the conclusion with practical examples of SaaS and IaaS services. [220] In this respect, for SaaS, a cloud service that enables collaboration between users was brought into discussion and for IaaS, the link with ECS was made by pointing to storage services. However, in order to draw a final conclusion about this type of cataloguing, our attention was pointed to the fact that some additional definitions were lacking.

---

[216] Article 2.(a) of Directive 2009/140/EC

[217] Jasper Sluijs and others, *'Cloud Computing in the EU Policy Sphere'*, 30

[218] Ibid., 31

[219] Article 2.c) of the Framework Directive

[220] E-mail from Erik Mark Meershoek, senior consultant at Verdonck, Klooster & Associates to author (30 January 2012)

In conclusion, in order to make a full assessment, we would need complementary legal definitions to describe what a "transmission service" is. However, even if such texts would point to the clear the conclusion that some SaaS and IaaS service are ECS, we will see in the following analysis that these examples would still prove to be faulty and misleading for answering our central research question.

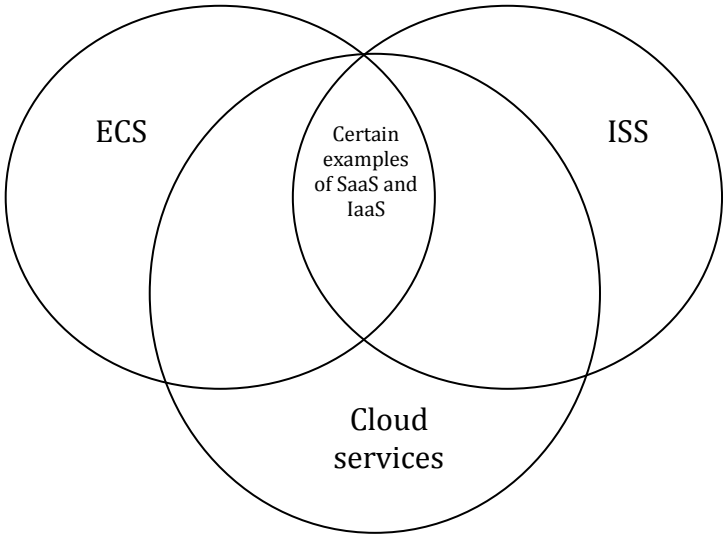

Figure 1. Overlap between information society services (ISS), electronic communication services (ECS) and cloud services

Complementing our analysis, from the perspective of US law, there are two important arguments why cloud computing cannot be seen as electronic communications services under the Stored Communications Act.[221] Firstly, cloud computing does not have as traditional function to send and receive communication. As the author observes, cloud computing generally has the purpose to store photographs and process documents. Second, cloud computing does not qualify under the regulation's provision regarding storage. The document clearly establishes a limitation of the meaning of "electronic storage" and this is not applied when dealing with cloud services.[222] However, it also has to be specified that electronic communication has a very wide meaning under the American legislation.[223] The Electronic

[221] William Robinson, *'Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act'* (2010) 98 (4) Georgetown Law Journal, 1209 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1596975> accessed 8 January 2012

[222] Section 18 U.S.C. § 2702(a)(1) of the US Stored Communications Act (USC) stipulate that electronic storage is storage of a "temporary [and] intermediate" nature that is "incidental to the electronic transmission" of the communication or (2) storage of the communication by the ECS provider to provide backup protection.

[223] Section 2510 (12) of title 18 of USC "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce". As case law shows in *In re Pharmatrak*

Communications Privacy Act of 1986 (ECPA) contains two relevant titles for our discussion. First, the Wiretap Act[224] which addresses wire, oral, and electronic communications *in transit* and the Stored Communications Act[225] which protects data held *in storage*.

The critique that can be addressed to the author's conclusion is that his view of cloud services is too limited in relation to the potential of this model. Therefore, his statement is not so well founded since he puts aside the complexity of the cloud service delivery model. As an example, we can mention Hotmail and SkyDrive as services which besides regular e-mail also offers free cloud storage. Therefore, this could be a translation of both SaaS and IaaS services. Thus, two aspects further reveal the blossom of the intricacy. First, it is necessary to point out that cloud services are offered at every layer, including from network, infrastructure, application software to customer front-end.[226] Second, as we will shortly see, the analysis of cloud services comprising elements will provide further insight in relation to the cloud-telco overlap discussion.

Therefore, some complementary aspects need to be further pointed out. First, we need to observe that the cloud sphere consists of the provided service in itself and the access to service.

Second, we need to have in mind the fact that the regulation of electronic communications is divided into regulation about transmissions on one hand (addressed by the Privacy Directive, ePrivacy and Data Retention Directive) and regulation about content (addressed in the Television without Frontiers Directive and the E-Commerce Directive) on the other hand. Therefore, the core element of the cloud is the service, which undoubtedly represents content, being thus an information society service.

Third, we need to make some additional remarks related to the access to the service since this element contains the particularities of an electronic communication service. Consequently, the discussion in connection to access to service determines if we can speak of an information society service or not. In translation to clouds, we need to remind the fact that because clouds contain this type of component, allows for the discussion of cloud being an electronic communication service; in other words only in this respect the cloud (via its intrinsic access element) service can be ECS. However, we also need to point out the fact that access is usually provided by a third party and not a cloud provider. Therefore, the access constituent is not as a general rule always performed by the same provider.

Privacy Litigation, 329 F.3d 9, 18 (1st Cir. 2003) transmission of completed on-line forms to pharmaceutical company websites constitutes an electronic communication.

[224] Sections 2510-2522 of title 18 of USC

[225] Sections 2701-2712 of title 18 of USC

[226] Cloud computing, Hearing with Telecommunication and Web Hosting Industry, 3

Going further with this analysis, we can see that the core element - once again, we emphasize, the information society service - can be separated from access. Consequently, since core and access can be separated, we draw the conclusion that the telecommunications framework is of no influence.

However, some obscurity exists when we consider the two cloud components - core and access - provided in a bundle.[227] This type of provisioning is implicitly covered in article 2.c) of the Framework Directive through the specification of the words "*wholly* or mainly conveyance of signals". Therefore, "wholly" refers to bundle provisioning while "mainly" redirects to the sub-service provided, namely access.

Additionally, we also need to point out that in the bundle model there are two possible provisioning situations. First, there is the dedicated access, meaning access provided only for particular purpose and not as a public ISP service. Second, there is the classic ISP scenario providing both ISS and ECS, meaning a full bundle (without a private line).[228]

Therefore as we have seen so far, when we talk about a stand-alone product, we speak about information society service. Additionally, when we consider the bundle model, we speak about bundle dedicated access information society services because an internet service provider having a subscription does not mean a private line.[229]

Consequently, given the above mentioned description, we observe that the main element of cloud services is ISS and therefore, the electronic communications service component remains marginal. Thus, when talking about the bundle type of provisioning the core element outweighs the access element. In other words, we observe the fact that access is just a means while the core of the service is the IT content; and IT content is not an electronic communication service.

Therefore this interpretation offers a possible way of establishing the regulatory application for cloud computing. Falling from this analysis, the deduction is that the determinant factor for performing the legal differentiation should be the main component of the model and not the side elements. To put it differently, if there is no contamination of the ISS, meaning it remains the central element of the service while being just supported via ECS elements, then the cloud service remains an ISS.[230] In conclusion, the electronic communications is a

---

[227] Pending approval for permission to use personal communication information between sender and the author (31 January 2012)

[228] Pending approval for permission to use personal communication information between sender and the author (31 January 2012)

[229] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 3

[230] Pending approval for permission to use personal communication information between sender and the author (31 January 2012)

required component but not an essential part in itself that influence the way we catalogue cloud offerings.

Offering additional support, Larouche's analysis on the European regulations from the point of view of convergence shows that "services involving content could thus potentially be affected by the new regulatory framework, but not so as to supersede other laws and regulations"[231]. The author further adds that the approach was not to separate content from networks and this therefore allowed "the regulatory framework to apply to services building upon electronic communications when suitable and adequate, while letting rules that are specific to those services prevail"[232]. Taking this into consideration, we observe that it is consistent with the above conclusion, thus allowing us to presume that there is the possibility of distinguishing and applying regulation depending on the type of service and not based on "cloud" as a whole. Moreover, the author underlines the fact that, because the regulation focuses on networks and only *potentially* interferes with content, content providers have the same role as any user of electronic communications.[233]

Therefore, given the more subtle nuances, the per a contrario reasoning applied in block to the last part of the definition of electronic communication services proves to be insufficient in order to give the final verdict. Moreover, this type of reasoning initially redirected our attention to a partial overlap of electronic communication services and cloud services, which consequently implied the possibility of cataloguing cloud providers as telecommunication providers.

However, the conclusion related to our research question is that the circumstances when a cloud provider will have its offerings classed as telecommunications services still seems to be left for future strategy targeting-wise considerations since the present definitions and rules are not specifically addressing this aspect.[234] In other words, since there is no clear cut direction for the cloud model, one could interpret that specific parts of it (namely fractions of SaaS and IaaS services) can be both electronic communications services and information society services. However, we have also seen that in a scenario such as Hotmail for instance, the service could solely remain an information society service. This conclusion can be drawn if we follow the reasoning conduced by the fact that the nature of the core element of the service should determine the applicable regulatory framework. Therefore, as a result for our example,

---

[231] Pierre Larouche, 'Communications convergence and public service broadcasting' (21 June 2011) 6 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=832444> accessed 2 February 2012

[232] Ibid.

[233] Ibid.

[234] This problem has also been addressed in a recent European Commission Cloud Computing Hearing with Telecommunication and Web Hosting Industry, but no definite answer to this question was set forth. However, it has been underlined that irrespective of set of obligations cloud providers will be subject to, they should be the same for *all providers*. As a result, telecommunications operators should not be deemed to follow different provisions, rather a level playing field for all cloud providers should be established.

the reason for webmail-plus-storage type of services being and ISS is that the ECS component of this type of service is provided by third party and therefore, not as a bundle offered by the same cloud provider.

Therefore, we have seen that, roughly put, a cloud service can be an electronic communications service because as shown above it is wholly or in part based on transmitting signals through electronic communication networks; at the same time a cloud service can easily be seen as a information society service given its unique nature of on-demand, pay-per-use, ubiquitous and heterogeneous characteristics. To support this, a recent European Commission Hearing with Telecommunication and Web Hosting Industry also shared this conclusion.[235]

Hence, service cataloguing does not provide the circumstances when a cloud provider would be seen as a telecommunication provider. Consequently, it also does also not show a clear demarcation of circumstances when the telecommunications framework will apply in the cloud environment.

Thus, the difference that determines the balance of the scale one way or the other must therefore be searched in other directions. As a possible answer we already mentioned the legal interest of telecommunication providers to have their cloud based services catalogued as information society services; and this is mainly because of the more favorable legal obligations deriving from it. However, the legal implications that would fall back on cloud providers as electronic communications providers are very interesting to analyze. Among them, the obligations related to data retention, data breach notification, jurisdiction, security constitute the prime aspects that require both industry and policy attention.

To sum up, the possible directions for determining the appropriateness of applying one set of regulations or the other are: policy traditions, state or industry interests, jurisprudence and state sovereignty and specific legal obligations.

Chapter four will consider the last element of this enumeration and it will underline the most problematic issues that emerge from cataloguing cloud providers as telecommunications providers. Additionally, it is important to mention that in a recent European Commission Hearing with the Telecommunications and Web Hosting Industry, a conclusion has been reached in a sense that there is the risk that cloud services would be hindered by the application of the telecommunications regulations. Moreover, the participants argued the fact that "cloud services should not be contaminated by existing regulations".[236]

[235] Cloud computing, Hearing with Telecommunication and Web Hosting Industry, 3

[236] Ibid.

CHAPTER FOUR – Security, privacy and liability issues

Before diving into the fourth chapter, in order to give a structural view of the paper until this point, we would like to synthesize the fact that the previous chapter launched into analysis dwelling with the a priori premise of telecommunications regulations application to cloud computing. This premise was rooted in the fact that, due to its model of delivering services, cloud can be seen as information society service but also as electronic communications service. Therefore, the last chapter explored classification possibilities for cloud providers and it demonstrated that a determinant or leading position cannot be appropriated. Thus, the conclusion of the third chapter is that considerable questions still remain open and that while the cloud model irreversibly advances towards its maturity, the corresponding institutions should flag the appropriate development signals for encouraging the cloud habitat to prosper.

Having this in mind, the fourth chapter is comprised of three parts that address important security, privacy and liability questions for the cloud model. Part I will discuss Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Given the recent amendments brought to this piece of legislation, references to the Directive 2009/136/EC will also complement the analysis. Additionally, Part II will round out the discussion with an analysis of the newly released proposal on data protection and will highlight the new set of challenges cloud providers might have to face. Part III will focus on Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Part IV will particularly deal with matters of liability springing from the regime set out by Directive 2000/31/EC.

These pieces of legislation have been chosen as subject of analysis because they allow us to witness how the fact that while having one set of regulations with sector-specific application adding to another set of provisions entailing a more general application lead to fragmentation and generate a general lack of understanding for the providers of the services in terms of apprehending their "rights and obligations set out in the legal framework, hence creating a legal vacuum".[237] Therefore, the following pages are direct proof of the above statement seen from the perspective of the cloud computing context and in particular from the viewpoint of a European cloud provider.

[237] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 883

Part I. Directive 2002/58/EC[238]

This section is first going to present the legislative background of the ePrivacy Directive and the resolution for its implementation. At the same time, we will not loose focus of the 2009 set of amendments this directive was subject to. Thus, after analyzing the set of obligations and pointing their importance for cloud providers, part I will end by addressing our conclusions.

Therefore, our focus comprises of a thorough analysis of the most important obligations deriving from these directives. Although not generally applicable to all types of service providers, our findings will reveal a suite of rules with substantial implications for cloud providers from the already announced perspective of security, privacy and liability. In this respect, we are going to discuss the security and confidentiality of communications obligations but also the provisions related to cookies and spy-ware, traffic and location data, subscriber directories and unsolicited communications as correlated between the directive and the amendment.

1. Legislative background

Upon its adoption, the ePrivacy Directive constituted a completely new legislative ground for electronic communications. However, it also added up to the previous established privacy legislation.[239] As we will shortly see, the ePrivacy Directive performs three functions. First, it aims at harmonizing the electronic communications rules, second it replaces Directive 97/66/EC[240] which addressed privacy rules specifically for the telecommunications sector and third, it "particularizes and complements"[241] Directive 95/46/EC[242] on the processing and free movement of data.

---

[238] 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 (Directive on privacy and electronic communications), O.J. L 201, 31.7.2002, hereinafter referred to as "e-Privacy Directive"

[239] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'* (2006) 61 (34) Annals of Telecommunication, 444 <http://www.springerlink.com/content/1q786u1515u45476/fulltext.pdf> accessed 9 February 2012

[240] Directive 97/66/EC of the European parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998

[241] Article 1.2 of Directive 2002/58/EC

[242] 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 on the free movement of such data, OJ L 281, 23.11.1995, hereinafter "Data Protection Directive"

As for the first function, we have seen that the legislative pack for the telecommunications sector initially consisted of the Framework Directive and was supported by other four directives, among which, the ePrivacy Directive. The complete set of regulations, including the ePrivacy Directive, aimed at harmonizing the European regulatory policies for electronic communications that will contribute to the achievement of the established goals of the Treaty.[243]

Second, the ePrivacy Directive replaces Directive 97/66/EC by broadly addressing the electronic communications sector; therefore the provisions here do not limit themselves only to the traditional telecommunications sector, hence the importance of taking them into consideration when addressing cloud computing.

Regarding its third function, it is important to underline the fact that the principles related to data quality, as set forth in article 6 of the Data Protection Directive, are entirely applicable to the electronic communications architecture, thus constituting essential aspects of the legislative, technological and related financial affairs of the service. However, Dumortier draws attention to the fact that we cannot speak of a simple exercise of transposing the rules enshrined in the Data Protection Directive to the more restricted environment (of electronic communications) by means of the ePrivacy Directive.[244] As an example, the author points out the fact that the ePrivacy Directive also covers legitimate interests of legal entities[245] while the Data Protection Directive is limited to physical persons.[246]

An additional aspect important to remind about the regulation of electronic communications is its division into regulation about transmissions on one hand (addressed by the Data Protection Directive, ePrivacy and Data Retention Directive) and on the other hand regulation about content (addressed in the Television without Frontiers Directive and the E-Commerce Directive).

---

[243] Specific for our discussion we can specify the development of a single internal market and the free movement of people, goods, services and capital. See Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007

[244] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications',* 445

[245] Article 1.2 of Directive 2002/58/EC

[246] Recital 24 of Directive 95/46/EC. Additionally, we have to mention the fact that the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data, 25.01.2012, hereinafter the "General Data Protection Regulation" mentions in article 89 the relationship with 2002/58/EC and amends it by specifying that:

> "1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.
>
> 2 Article 1(2) of Directive 2002/58/EC shall be deleted."

2. Obligations for cloud providers

Since the electronic communications definition has been already discussed in the previous chapter, we will directly step towards analyzing the obligations this directive sets forth and to which cloud providers can be deemed subject to.

1) Security

The obligation related to the security of service in article 4 of the ePrivacy Directive is two-fold. On one hand, the service providers must assure the necessary safety measures[247] but they also have to notify the subscribers about inherent security breach risks[248]. Furthermore, the service providers have the duty of information towards their customers even if "the risk lies outside the scope of the measures"[249].

Having this in mind, we would like to discuss the practical implications this article has for cloud providers. Not only the cloud model itself is more vulnerable to attacks in general[250], but also the interconnection of clouds poses significant problems. As Cary Calderone warns in his article, the unavoidable interconnection of clouds, poses important security risks regarding the security of a company's network not only in itself but also on the data security of the cloud provider[251]. For example, if a cloud subscriber is hacked, the security threats will be as serious for the other companies in the cloud network as for the targeted victim of the initial attack. Calderone explains that if a hacker attacks a victim within the cloud, there are serious chances that other networks will be affected as well.[252] Therefore, Calderone advises particular attention to issues such as control provisioning, existing bandwidth vulnerability and guarantees of protection in general.[253]

As a result, the provisions of article 4 may be cumbersome for cloud providers and due to the permanent invention of circumvention methods and never-ending ingenuity of hacking techniques, many of them may not be able to reduce their liability in case of possible attacks.

---

[247] Article 4.1 of Directive 2002/58/EC

[248] Article 4.2 of directive 2002/58/EC

[249] Article 4.2 of directive 2002/58/EC

[250] Cloud Computing Software Blog, Cloud Computing Software, *'Hackers Feast on Cloud Computing – Vulnerability of Cloud Computing'* (27 August 2011) <http://www.cloudcamb.org/software/hackers-feast-on-cloud-computing-vulnerability-of-cloud-computing> accessed 9 February 2012

[251] Cary Calderone, *'Up In the Cloud and Risk from the Other Guy's mistakes'* (19 January 2011) Data Retention and Electronic Discovery Law <http://www.dredlaw.com/2011/01/up-in-cloud-and-risk-from-other-guys.html> accessed 9 February 2012

[252] Ibid.

[253] Ibid.

Complementing our analysis with observations deriving from Directive 2009/136/EC (which amends the ePrivacy Directive), we notice that in Recital 23 of the directive there are additional specifications such as providing "clear and transparent information in the initial contract and in the event of any change in the access provision"[254], but also additional indications about the level of reliability of access. Therefore, it becomes even clearer that the sector-specific set of regulations urge for a much stricter compliance regime for service providers. Consequently, cloud providers may face extra requirements that could fundamentally impact their activity.

Before ending the section related to security obligations, we would like to point out the fact that Recital 20 of the ePrivacy Directive offers further guidance related to the measures a service provider can adopt for remedy (different types of software or encryption technologies). Moreover, the costs related to notifying the customer are discussed. Additionally, it states that the security breach notification does not exclude the duty to take suitable and prompt actions for new and unpredicted risks and to restore the normal level of security.[255]

Nevertheless it is important to note that the amended version of the ePrivacy Directive institutes new personal data breach notifications[256] for publicly available electronic communications providers in order to prevent the considerable losses and damages resulting from unfortunate security breach events.

Transposed to the recent Sony chase, the fact that this provision targets telecommunication operators shows that it creates leeway for some types of providers to avoid being held responsible. As such, Georgiev ironically draws attention to the fact that despite the European Parliament insisting the personal data breach notification provision be extended to also address information society service providers[257], the final decision of construing it only to telecommunication operators created a clean get away for the Sony Play Station Network

---

[254] Recital 23 of the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, hereinafter referred to as "Directive 2009/136"

[255] Recital 20 of Directive 2002/58/EC

[256] In the meaning of article 4.c).3 of Directive 2009/136/EC "personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community".

[257] CCR Magazine, *'Telcos' data breach notification amendment is passed'* (6 November 2009) <http://www.ccrmagazine.com/index.php?option=com_content&task=view&id=2123> accessed 9 February 2012

security breach incident. [258] Needless to point out the fact that Sony cannot be seen as a telecommunication provider and thus be outside the scope of this sector-specific regulation.[259]

On this account, we underline once more the severity of the compliance regime cloud providers may have to follow and the possibility for it to represent inconsolable drawbacks for the cloud model.[260]

2) Confidentiality of communications

Article 5 enshrines the principle of confidentiality by "prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned"[261]. However, as we will shortly see, there are three exceptions from this rule.

First, the directive specifies that there are situations when a person is legally authorized to restrict the confidentiality of communications, namely "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system"[262]. Evidently, this provision has the purpose to allow state authorities to make use of "eavesdropping, wiretapping, storage, or other types of interception or surveillance of communications in the fight against crime"[263].

---

[258] Reguligence Weblog, *'Sony PSN: Clueless And Breaching'* (30 April 2011) <http://reguligence.biz/tag/2009136ec/> accessed 9 February 2012

[259] Nevertheless, if the recently released proposal updating the data protection and privacy provisions will be adopted, such companies will not be left out of the scope of applicability since the proposal's rules will have general practical application. Therefore will include all types of service providers via its new provision on personal data breach notification in articles 31 and 31, formally only addressing electronic communication via article 4(3) of the ePrivacy Directive 2002/58/EC. Hence, the proposal builds on the sector-specific rules from the ePrivacy Directive and thus, installs a wider application for all types of providers.

[260] Once again, we specify the fact that the personal data breach notification provision is *currently* a sector-specific one, addressing only electronic communications providers. However, if the new data protection proposal will be implemented, cloud providers will also be subjects of the regulations' broad applicability.

[261] Article 5.1 of Directive 2002/58/EC

[262] Article 15.1 of Directive 2002/58/EC

[263] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 891

Second, the article allows for technical storage inherent to the transmission of communications when it does not interfere with the principle of confidentiality.[264]

Third, the recording of communications is allowed for evidence purposes in the context of lawful economical activity practice of a commercial transaction or of any other business communication.[265]

It is important to underline the observation mentioned in Recital 21. The ePrivacy Directive aims at prohibiting both the intentional unauthorized access to the contents and data related to such communications, as well as the unintentional unauthorized access. However, as the Recital mentions, in particular Member States only the unauthorized access to communications is prohibited.

Therefore, in special, cloud providers may need to meticulously monitor and compile the regulatory differences across EU countries as regards the chosen meaning of "criminal offences". However, in general, they need to be aware of the exception for "security and law enforcement purposes"[266] in article 15.1 given de wider scope of harmonizing the provisions of the Directive with the Cybercrime Convention.[267]

3) Cookies and spy-ware

An important principle introduced in this directive is the fact that terminal equipment of users of electronic communications networks *and* the data stored in there represents a private element of the individual who seeks protection of his fundamental rights.[268] Additionally, as appropriate, users are given the right to deny access to or storage of their information. Therefore, the above mentioned recital prohibits the use of spy-ware, web bugs and cookies if the user or subscriber has not been correctly informed about it.[269] In this respect, the ePrivacy

---

[264] Article 5.1 of Directive 2002/58/EC

[265] Article 5.2 of Directive 2002/58/EC

[266] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 891

[267] Recital 53 of Directive 2009/136/EC

[268] Recital 24 of Directive 2002/58/EC

[269] Recital 24 of Directive 2002/58/EC. With the aim to further strengthen users' right, Directive 2009/136 introduces new rules regarding the use of cookies. Among them, the requirement of prior consent is of particular importance. Additionally, we mention the fact that Recital 66 of the 2009/136/EC Directive indicates that the browser settings could represent an appropriate method to obtain user consent. The analysis of this method is treated extensively discussed in Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertizing (2010) WP 171, 11, 17 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf> accessed 21 January 2012

Directive brings an important resolution; as Dumortier notes, before the implementation of the ePrivacy Directive, such operations, which did not reveal the user or subscriber's identity were generally not covered by the European privacy framework.[270]

Therefore, the advantageous situation the directive brings for the users is translated in article 5 that demands that "the use of electronic communications networks to store information or to gain information stored in the terminal equipment of a subscriber or user"[271] must be accompanied by specific and understandable information related to the purpose of processing that information. Additionally, the user or subscriber must have the option of refusing such processing.

As we can see, through the fulfillment of the two conditions of article 5.3 - acquiring precise information and denial of the use or storage of information - the users have been empowered with better means to act for the protection of their private sphere. In support of these rights, Recital 25 specifies that the process of obtaining knowledge and the manifestation of the refusal have to be implemented through user-friendly methods. Going even further, the recital mentions the fact that the user should be prompted only once and the expression of his right either accepting or refusing should also cover any further use that may be made by those devices in the following connections sessions.[272]

Similar to the case of the confidentiality of communications, article 5.3 mentions the exception of technical storage that is exclusively used for "carrying out or facilitating the transmission of a communication over an electronic communications network"[273]. Furthermore, the article specifies that technical storage or access is permitted only when absolutely necessary to provide an information society service explicitly requested by the user.[274]

Additionally, Jones and Tahri address the technical difficulty of website operators to identify the users who have indeed consented[275] to the use of cookies. Since the operators are not able

---

[270] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 450

[271] Article 5.3 of Directive 2002/58/EC

[272] Recital 25 of Directive 2002/58/EC

[273] Article 5.3 of Directive 2002/58/EC. In addition, we have to point out the fact that Directive 2009/136/EC leaves out "facilitating the transmission of a communication over an electronic communications network".

[274] Article 5.3 of Directive 2002/58/EC

[275] Additionally, we point out the fact that the Opinion of Article 29 Data Protection Working Party is that children are not capable of giving informed consent and, more importantly for cloud providers, failure to implement appropriate notice and permission may create liability issues. See, Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertizing (2010) WP 171, 13-15 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf> accessed 21 January 2012

to store such information, the practical question of how they will maintain record of such users still remains open and implies that these users need to be prompted each time they surf a website or opt for a service.[276]

In conclusion, the new 2009/136 Directive, which has gained the name of the "Cookie Directive", raised a wave of discussion due to the "opt-in" mechanism; nevertheless, providers now have to ask for prior consent, to inform the user how and what type of data is going to be used and give him the possibility not to allow that information to be collected. Moreover, given the reasoning presented in chapter three, we could also ask whether the erasure of the terms "facilitating the transmission of a communication over an electronic communications network" will present any particularity for cloud computing.

4) Traffic and location data

Before starting the analysis, we would like to clarify the fact that traffic data can be location data. The reason for this is that, in instances such as a mobile phone call, "traffic data include data on the geographical position of the terminal equipment at the beginning and at the end of a communication".[277]

In addition, articles 5, 6 and 9 of Directive 2002/58 specify traffic and location data created by private networks or in private services are not covered. However, if the data relates to individuals, then the general Data Protection Directive gains application.[278] In fact, as we will shortly see, the matter of regulation of traffic and location data is far more complex since it renders the application of three distinctive pieces of legislation and urges for considerable more thought regarding the circumstances of their application.

a. Traffic data

As already specified, the ePrivacy Directive does not address rules related to content. The directive sets forth the definition of traffic and location data[279], but nowadays the meaning

---

[276] Richard Jones and Dalal Tahri, *'An overview of EU data protection rules on use of data collected online'* (2011) 27 (6) Computer Law and Security Review, 635 <http://www.sciencedirect.com/science/article/pii/S0267364911001488 > accessed 9 February 2012

[277] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 887

[278] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 893

[279] Additionally, we would like to observe the fact that in article 2.(c) of Directive 2009/136 amends the definition of location data by inserting the terms "or by an electronic communications service", thus enlarging the boundaries of the protection of data.

> "(c) "location data" means any data processed in an electronic communications network or *by an electronic communications service*, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;"[emphasis added].

between mere conveyance of signals and content data is getting difficult to separate. In this sense, Moiny makes an interesting discussion about IP addresses as traffic or content data.[280]

Related to the discussion about IP being regarded as personal data, we would like to point out that the processing of IP addresses has been the major instrument used particularly in the fight against copyright infringement[281]; as a result, the issue has been internationally discussed by courts.[282] From a case law review Moiny makes in his article, we can see that in France, Switzerland and Belgium courts have ruled that IP addresses are personal data. The case law is furthermore supported by the Opinion of the European Data Protection Supervisor who, based on the interpretation of the definition of personal data from article 2 of Directive 95/46/EC, brings forth the following reasoning: "it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here".[283]

Article 6.1 stipulates that, except for billing purposes, both providers of a public communications network and providers of a publicly available electronic communications service who processed and stored traffic data related to users must erase or make anonymous

---

[280] Jean-Philippe Moiny, *'Are Internet protocol addresses personal data? The fight against online copyright infringement'* (2011) 27 (4) Computer Law & Security Review <http://pdn.sciencedirect.com/science?_ob=MiamiImageURL&_cid=271884&_user=522558&_pii=S0267364911000707&_check=y&_origin=article&_zone=toolbar&_coverDate=31-Aug-2011&view=c&originContentFamily=serial&wchp=dGLbVlS-zSkWA&md5=294df64994838abceecfab506eb71896/1-s2.0-S0267364911000707-main.pdf> accessed 21 January 2012

[281] And more recently even against child pornography through the Cybercrime Convention.

[282] As Moiny observes, the Hong Kong Court of First Instance ruled on this aspect in case Cinepoly Records Co Ltd et al v. Hong Kong Broadband network Ltd et al., [2006] HKLRD 255, nr 14 January 26 2006. See Jean-Philippe Moiny, 'Are Internet protocol addresses personal data? The fight against online copyright infringement', 352

[283] Opinions, European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), (2010/C 147/01) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:EN:PDF> accessed 24 January 2012.

Furthermore, in its Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April, 2008, the Article 29 Data Protection Working Party confirmed that, in most cases, cookies and IP addresses are to be considered personal data. This Opinion stated "When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned".

See Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines (2008) WP 148, 9 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf> accessed 24 January 2012

such data when it is no longer needed for the purpose of the transmission of the communication. [284]

Of considerable interest for cloud providers is the exception mentioned in paragraph 3 of the same article. In this sense, providers of electronic communications (excluding operators of a network[285]) are exempted from erasing data if they fulfill the following conditions. First, they need the consent of the user or subscriber, second the purpose has to be related to marketing their services or value added ones and last, this exemption is valid only up to the point necessary to carry on this service or marketing. Furthermore, the user has to be left the option to withdraw its consent at any point in time and has to be knowledgeable about the type of traffic data and the duration of its processing.[286] Dumortier signals a very important issue. With the help of a very conclusive example, he shows that the processing of traffic data for marketing purposes blurs the possibility of making an evident differentiation from content data.[287]

Moreover, it has to be mentioned that the scope of processing traffic data should be strictly construed. In this sense, article 6.5 shows that "handling billing or traffic data management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service" must be only performed by authorized personnel.[288]

In conclusion, we have to observe the fact that traffic data can be seen as personal data. As a result, both Directive 95/46/EC and Directive 2002/58/EC gain application. Accordingly, aside the specific provisions of the ePrivacy Directive, articles 10, 11, 12 and 14 from the Data Protection Directive will need to be followed as regards personal traffic data.[289]

b. Location data

It is important to specify that the processing of location data and particularly location-based cloud services are covered by three European Directives.[290] As we will see, the Data Retention Directive, while in harmony with article 15 of the ePrivacy Directive, is a major source of inconsistencies across Member States by allowing them the possibility to choose between a short period of retention of 6 months and the considerable margin of two years. The other two directives are Directive 95/46 addressing rules on processing personal data in

---

[284] Article 6.1 of Directive 2002/58/EC

[285] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 452

[286] Article 6.3 and 6.4 of Directive 2002/58/EC

[287] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 452

[288] Article 6.5 of Directive 2002/58/EC

[289] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 892

[290] Ibid., 885

general (lex generalis), and Directive 2002/58 establishing provisions of processing of personal data for electronic communications (lex specialis).[291]

The ePrivacy directive clarifies that location data does not entirely consist of traffic data. In other words, location data comprises of other type of data, aside traffic data. However, it has been pointed out that a clear distinction between personal data, traffic data and location data cannot easily be made. Cuijpers and Koops have drawn attention to the fact that "all kinds of combinations are possible, e.g. personal data can be location data as well"[292]. Additionally, the authors pointed out that, not only the applicable regime is difficult to identify in this respect but also that the different Directives address different parties and "the applicability of their rules is technology-dependent".[293] As a matter of fact, the authors observe "the processing of data can be governed by neither Directive, by one of the Directives, or by both Directives simultaneously, depending on the type of data and data processing".[294] We can also note the fact that the provisions of the ePrivacy Directive are more rigid than the ones in Directive 95/46/EC since for example the obligation for data location applies only to telecommunication providers while other service providers are not being required to comply with such a provision.[295]

Nevertheless, as WP185 states "[...] location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC."[296] However, Cuijpers and Koops question this statement and present a complex and overlapping diagram of relationships between personal data, traffic data and location data.[297] Additionally, the authors point out that "the Directives seem to target intentional communications in which the content of the communication plays an important role".[298]

---

[291] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 886

[292] Ibid., 885

[293] Ibid.

[294] Ibid., 886

[295] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 3

[296] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile device (2011) WP 185, 8 <http://www.statewatch.org/news/2011/aug/eu-art-29-geo-location-wp-185.pdf > accessed 23 January 2012

[297] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 888

[298] Ibid., 890

Article 9 of Directive 2002/58 concerns the processing of location data other than traffic data. Therefore, leaving aside the possibility of location data to represent personal data (e.g. relating to telecommunications subscriptions by legal persons[299]) under the ePrivacy Directive, service providers have the obligation to obtain the location data only with the user's consent, to make it anonymous and to process it only for the restricted time necessary in relation to the added value service. Also, users have to be informed about the type of data processed and whether the data is going to be communicated to third parties in the purpose of providing added value. Additionally, we can also observe the leitmotiv rule for users to have the possibility of withdrawing their consent at any time.[300]

It is important to mention that, while data can be processed with consent or by having the legal justification to do so (article 15 of Directive 2002/58), article 7.f of Directive 95/46 allows member states to balance the relevant situation in which the processing of data has to be justified.[301] Therefore, Cuijpers and Koops observe the fact that "The absence of this ground in Directive 2002/58 means that this option does not apply to location data or traffic data generated solely because of electronic communications".[302]

Disrupting the perfect parallel of the rules between traffic and location data, the directive makes a distinction from the article related to traffic data. In this respect, we identify that the activities that can be performed by authorized persons are not specifically mentioned. Therefore article 9.3 leaves unaddressed the types of activities the persons acting on behalf of the operator, provider and third party.[303] As Cuijpers and Koops point out, in some cases there will be a single relationship between subscriber and provider while in more complex scenarios the service might be provided by more than one party.[304] The authors further elaborate saying that "Here, the way in which the backend system operates and processes the data is important, as in some cases the results of the processing of location data are transferred to another device."[305]

---

[299] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 892

[300] Article 9.1 of Directive 2002/58/EC

[301] Ibid., 892

[302] Ibid.

[303] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 453

[304] The authors give the example of a service linked to data stored in a database controlled by another party and mention the possibility of a subscriber to a certain location based service not being the same person as the user. See Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 884

[305] Colette Cuijpers and Bert-Jaap Koops, *'How fragmentation in European law undermines consumer protection: the case of location-based services'*, 884

Before ending this section we would like to make reference to the fact that the ePrivacy Directive allows for an important derogation form the principle of confidentiality of communications. In this respect, article 15 shows this exception by particularizing the situations in which the principle of confidentiality can be neglected. Since this issue is going to be extensively treated in conjunction with the Data Retention Directive in part II of this chapter, for further details, we redirect the reader to that particular section of the paper.

Therefore, for cloud service providers, the direct implication is that it proves to be a real challenge to know which legal rules apply to what services and make sure they comply with them. Although we have consistently pointed out to Cuijpers and Koops' analysis which mainly addresses location based services, the conclusions are very valuable for cloud providers. Cloud providers already offer not only this type of services but they also develop social network sites. Therefore because cloud providers have to meticulously answer a vast thread of questions[306] before engaging in activity, the confusion of the current regulation undoubtedly affects the emergence of cloud services and demands eliminating the legal lacunae.

5) Directories of subscribers

The directive imposes the requirements of subscribers being informed about their mentioning in the directory and about the purpose of such register if their personal data are inserted or could be inquired. More specifically, subscribers also have to be informed about the search options this type of file has in its electronic version.[307] Furthermore, the subscriber is given the power to decide if its personal data should be included in the directory and to verify, correct or withdraw such information.[308] In support of the provisions, also Recital 33 of the Directive 2009/140/EC reiterates these requirements.

These provisions remain valid for individuals, however paragraph 4 of article 12 mentions that the legitimate interests of legal entities must be awarded adequate protection.[309]

[306] Ibid., 895

[307] Article 12.1 of Directive 2002/58/EC

[308] Article 12.2 of Directive 2002/58/EC

[309] Article 12.4 of Directive 2002/58/EC

6) Unsolicited communications

Article 13.1 reinstates the specification that electronic mail represents an automated communication system. It also urges for the consent of the subscriber in relation to unsolicited communication. Furthermore, Recital 17 mentions a possible mechanism through which such consent can be given, namely by ticking a box when visiting a website.[310] Therefore, subscribers are given the possibility to object to marketing targeted communication and consequently have their contact details such as e-mail address, instant messaging details and mobile number not openly available to any natural or legal person offering a service.[311] However, it is not clear whether the concept of customer implies some sort of financial contribution or if it can mean the receiver of a free sample of a certain good or product.[312]

Moreover, we mention the fact that the article allows for a broad interpretation of the term electronic mail, but it excludes the pop-up windows on websites.[313]

Furthermore, paragraph 4 of article 13 addresses the issue of spoofing[314] which is clearly banned by this directive. Additionally, paragraph 5 mentions the same rules about natural and legal person's interests are applied as for directories of subscribers.

Another observation important to make about the ePrivacy Directive is that it does not refer to a specific geographical application as Directive 95/46/EC mentions. Nevertheless, since the ePrivacy's role is to "particularize and complement" the latter directive, it can be argued that it follows the same application provisions.[315] However, as Jones and Tahri observe, the approach of applicable law has not been dealt with in a harmonized matter among Member States.[316]

---

[310] Recital 17 of Directive 2002/58/EC

[311] Article 13.1 of Directive 2002/58/EC

[312] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 455

[313] Jos Dumortier and Christoph de Preter, *'The European regulatory framework for security and privacy protection in electronic communications'*, 455

[314] Spoofing implies sending e-mails for marketing purposes with the identity of the sender being hidden or without specifying a valid address for unsubscription purposes. For more information see Search Security, TechTarget, *'E-mail spoofing'* (last updated July 2002) <http://searchsecurity.techtarget.com/definition/email-spoofing> accessed 23 January 2012

[315] Richard Jones and Dalal Tahri, *'EU law requirements to provide information to website visitors',* 615

[316] The authors give the example of Germany where, beside regulating communications sent from Germany to recipients on German territory, it also considers the situation when unsolicited communications are sent from another member state. See Richard Jones and Dalal Tahri, *'EU law requirements to provide information to website visitors',* 615

Aside from the issue of unsolicited communication, we would like to finalize the remarks related to the amendments Directive 2009/136 sets forth. Therefore, we would just like to mention the insertion of a new article 14a related to committee procedures, the new paragraph 1b of article 15 which establishes "internal procedures for responding to requests for access to users' personal data based on national provisions" as well as the insertion of a new article 15a which addressed the issue of enforcement and infringements related to possible violation of national provisions translating this directive.

3. Conclusion

The ePrivacy Directive represents a sector-specific regulation which renders application only to the electronic communications operators. These types of providers have more cumbersome requirements to maintain while other types of service providers are not deemed to such rigorous provisions. As an example, we can remind the provisions related to location data and point out that they are not obligatory for information society service providers. Therefore, the implications for cloud providers gain considerable thought because, as the Cloud Computing Hearing with Telecommunication and Web Hosting Industry underlines, the cloud paradigm does not reveal new privacy problems but it brings to the spotlight the gaps and discrepancies in the current legislation.[317]

Complementing the relevance of the analysis, the chapter ends with a significant remark pointing out that the rules that apply to delivering cloud services should be firm and uniform for each type of provider. In the same sense, the discussion from the recent Cloud Hearing underlined that irrespective of the set of obligations cloud providers will be subject to, they should be the same for *all providers*.[318] As a result, telecommunications operators should not be deemed to follow different provisions, rather a level playing field for all cloud providers it should be established.

[317] Cloud computing, Hearing with Telecommunication and Web Hosting Industry, 3

[318] Ibid.

Part II. New European data protection proposal[319]

First announced in the Digital Agenda for Europe (DAE) Annual Progress Report from the 22nd December 2011, an update of the Data Protection Directive was released having as triggers "developments such as cloud computing and social media"[320].

With data protection being a "wider part of cloud computing issues"[321] the proposal to reform the 17 year-old privacy framework intends to strengthen user online privacy rights related to social networks and cloud computing applications but also to contribute to the growth of the European digital economy.

The newly proposed European data protection rules comprise of two legislative texts, namely a regulation and a directive. First, the new Regulation aims at building "more trust in online services"[322] by empowering users with stronger rights related to consent and by redirecting the control of their personal information into their own hands. In this respect, cloud providers should take notice of the new provisions such as the individual's right to be forgotten, the requirement of explicit consent, the sending of personal data breach notifications and about the provisions related to data portability which sum up the major changes this regulation sets forth.[323] Second, aside the regulation, the new Directive deals with general data protection rules in relation to law enforcement and judicial cooperation on criminal matters. Significantly, the application of this directive is related to both national but also trans-border transmission of data.

Since the data protection revision is partly seeking to address some of the implications of cloud computing, this section will analyze the most important provisions that the Regulation

---

[319] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data, 25.01.2012, hereinafter the "General Data Protection Regulation"

[320] European Commission, Digital Agenda for Europe Annual Progress Report (22 December 2011) 4 <http://ec.europa.eu/information_society/digital-agenda/documents/dae_annual_report_2011.pdf> accessed 2 February 2012

[321] European Commission, Vice-President of the European Commission Neelie Kroes, *'Cloud Computing and Data protection reform'* (2012) <http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection/> accessed 30 January 2012

[322] European Commission, EU Justice Commissioner Viviane Reding, *'Data protection: strengthening your online rights'* (25 January 2012) <http://ec.europa.eu/unitedkingdom/press/frontpage/2012/12_07_en.htm> accessed 30 January 2012

[323] Additionally, we briefly mention that newly introduced elements are "the transparency principle, the clarification of the data minimisation principle and the establishment of a comprehensive responsibility and liability of the controller." See General Data Protection Regulation Explanatory Memorandum, 8 available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

of the new legislative pack contains. However, before presenting a brief analysis of these provisions in relation to cloud providers, it is essential for our discussion to describe the most important definitions and elements regarding the processing of personal data in cloud computing.

In this respect we will first see the definition of "personal data" accompanied by some remarks regarding "processing of personal data".[324] Furthermore, the definitions of "data controller" and "data processor" will be presented. Second, some brief considerations are going to be addressed in relation to the issues of applying "data controller" and "data processor" terminology to cloud relationships. Tightly connected to this, we are forced to make tangential analysis regarding liability issues. However, our study limits us to presenting few thorny aspects, thus offering just a glimpse of the intricate issues.

The second section of this part addresses the new rights of the proposal. Our focus will be on the provisions of the new Regulation and on their impact on cloud computing.

Finally, in the third section we address some conclusions based on our findings.

1. Definitions and elements regarding the processing of personal data in cloud computing

First, the definition of "personal data" relates to any information regarding an "identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[325]. Underlining the broad sense of the definition, the WP169 states that whether information is "personal data" is a question of fact, depending on the context.[326] On this

[324] Due to the limitations of this study, we are not going to address the problematic some specific cloud contexts (such as anonymization, pseudoanonymization, encryption and sharding) has on delimiting the meaning of the term "personal data" nor address issues related to the processing of certain more sensitive categories of personal data. However, in respect of anonymization, pseudoanonymization, encryption and sharding related issues we redirect towards W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1'* (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577> accessed 6 February 2012

[325] Although not specifically put out in Directive 95/46/EC, the meaning of "data subject" is present in the General Data Protection Regulation in art 4. (1). We also note that the Regulation inverts the correlation of terms by first explaining the definition of a data subject and then mentioning that "personal data" means any information related to a data subject.

[326] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (2010) WP 169, 3 <http://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf> accessed 30 February 2012

account, we observe that there is no doubt whether cloud providers are processing personal data.

Moreover, particularly important for our discussion is the fact that information which is not seen as personal data from a cloud user's point of view, *may* become personal data when found and processed by the cloud provider.[327] As an example, we can mention that this transformation can happen when the provider moves forward and processes the information obtained from the user for its personal reasons.

Additionally, we observe that the definition of "processing" has a very broad coverage of operations performed on personal data. Thus, the range of operations extends from retrieval and structuring to use and storage of personal data.[328]

Having this in mind, the definitions of "data processor" and "data controller" refer to

> (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
>
> (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;[329]

Therefore we observe that the definition covers the possibility of multiple controllers in relation to the same personal data but the concept of co-controllers is also plausible.[330]

Second, in setting the context of the above-mentioned rights, it is important to specify the fact that the General Data Protection Regulation introduces the direct liability regime for data processors.[331] Therefore, article 77 of the Regulation indemnifies "any person who has

---

[327] W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1'*, 14

[328] Article 2.(b) of Directive 95/46/EC. For clarification purposes, the provisions of the current Data Protection Directive in force will be the focal point of interpretation. However, where appropriate, specific references will be addressed in relation to the changes the new Regulation brings forth. In this sense, specifically addressing the definition, the insertion of "structuring" and erasure of the word "blocking" has been observed regarding the enumeration of the new Regulation, article 4. (3).

[329] Article 2. (d).(e) of Directive 95/46/EC. We also specify that there is a small adjustment in the General Data Protection Regulation to the definition of data controller now also covering the "conditions" of processing of personal data, article 4. (5).

[330] However, the possibility of joint controllers is not recognized throughout all Member States. See Kuner (n 19) ch 2.22 fn 30 as referred to by W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'* (2011), fn 44 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130> accessed 6 February 2012

[331] Article 77 of the General Data Protection Regulation

suffered damage as a result of an unlawful processing operation" to receive compensation from the data controller, from the data processor or from both of them.[332]

Having this in mind, a differentiation between the roles of data controller and data processor is *currently* crucial for two important reasons. The first one is the applicable law[333] and the second one regards establishing for which party the civil liability duty and penalties for non-compliance rules apply.[334] Moreover, it is important to underline that Recital 17 and article 2.(3) specify that "this Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive"[335], undoubtedly this being another source for triggering liability.

However, in relation to cloud computing, there are significant obstacles for separating the notions of data controller and data processor.[336] In fact, the sophistication of data processing scenarios[337] contributed to such a high degree of difficulty that the Article 29 Data Protection Working Party and the International Chamber of Commerce both issued documents providing guidelines regarding this problem.[338] Moreover, the same WP169 observed that even the "[...] definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more

---

[332] Additionally, in relation to business to business relationships, the Regulation acknowledges binding corporate rules and drafts the minimum set of requirements they should contain. Particularly, article 43.2 (f) specifies that liability rules must be included in the policy.

[333] As explained we are referring to the current provisions in force. Therefore, we underline that, if the General Data Protection Regulation is implemented, this remark will not be valid since the regulation will have a direct effect on Member States.

[334] Additionally, we also note that Recital 118 of the General Data Protection Regulation specifies that an exemption from liability is when the data controller or data processor "prove that they are not responsible for the damage; in particular where he [the controller or processor] establishes fault on the part of the data subject or in case of force majeure". Moreover, Recital 60 and article 5. (f) of the General Data Protection Regulation establish that compliance must be ensured and demonstrated for each processing operation.

[335] In connection to the discussion that will follow in the forth part of this chapter regarding the liability regime set forth in Directive 2000/31/EC, Hon and others opined that cloud computing providers should be considered "mere processing intermediaries" and thus fall aside the liability rules applicable under the Data Protection Directive. Therefore, the authors explain that cloud providers should "benefit from similar liability shields" under the E-commerce Directive.

[336] For an interesting summary of a survey regarding the position cloud providers catalogue themselves on a contractual basis see W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'*, 12-14

[337] For detailed examples in strict application to the cloud model and analysis see Ronald Leenes, *'Who controls the cloud'* (2010) 11 IDP, ff3 <http://www.uoc.edu/ojs/index.php/idp/article/viewFile/n11-leenes/n11-leenes-eng> accessed 6 February 2012. Moreover, Hon and others have argued that cloud providers could not even be data processors. In this sense, see W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'*, 14-23

[338] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor' (2010) WP 169 and ICC Task Force on Privacy and the Protection of Personal Data, Summary of the Workshop on the Distinction between Data Controllers and Data Processors (International Chamber of Commerce, Paris 25 October 2007) <http://iccwbo.org/policy/ebitt/id17704/index.html> accessed 6 February 2012

details in order to allow for a clear and unambiguous interpretation by data controllers and users alike"[339]. Therefore, it appears that there are no solid ingredients for "cooling down" the cloud tumult.

Revealing just one particular issue of the intricacies, we can note that a cloud provider could be a controller *in relation to one processing operation* but also a processor in relation to another.[340] Moreover, a cloud provider can simultaneously have the status of a controller *for certain processing operations* while performing as a processor for other processing operations; also the "specific set of data or operations" must be evaluated for determining the role.[341]

In conclusion, the obstacle of "allocation of responsibility"[342] comes to question from the difficulty of determining whether a cloud provider is a data controller or processor. In fact, this almost herculean task has led some authors to question whether the distribution of responsibility can actually be assessed. For more in depth analyses and insight into the complexities we refer to authors such as Leenes and Hon et all.

Finalizing the first part of the discussion regarding the most important definitions and elements in respect of processing of personal data in the cloud environment, we end by emphasizing the relevance of this issue and by pointing out that since cloud providers have difficulties in identifying their legal role and position, there will unavoidably be problems in complying with requirements and respecting consumer's rights.

2. The General Data Protection Regulation's new rights

Having this in mind, we turn to our discussion about the proposed EU data protection regulation. Since one of its main goals was to assure users the right and control over their personal information, we can see that the rechanneling of information control is sought to be achieved by specific provisions which can be found in articles 15 to 19. In this respect, individuals obtain a right for an easier access by having the possibility to ask the data controller at any time whether their personal data is being processed[343]. Additionally, they are

---

[339] Article 29 Data Protection Working Party, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive (2006) WP126, 3 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_en.pdf> accessed 30 January 2012

[340] Ronald Leenes, *'Who controls the cloud'*, 8 and W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'*, 12

[341] W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'*, 9

[342] Ronald Leenes, *'Who controls the cloud'*, 4

[343] Article 15 of the General Data Protection Regulation

given the right to rectify any incorrect information related to them[344]. More importantly, with few exceptions, article 17 introduces the right to be forgotten and to erasure. Therefore, although not an absolute right, the right to be forgotten gives individuals the power to have their information permanently deleted from social media sites and bank databases.[345] It is important to underline that the reason behind the decision of introducing such a right was the worrying consequences of social network sites. In this respect, the popularity these sites have among young people and the easiness with which personal data can get out of control have been identified as threats. Moreover, the Commissions' intent was to introduce stronger means of protection for children. Therefore, we can imply that this article has as grounds the desire to offer individuals the possibility of avoiding possible negative effects coming from the carelessness of spreading personal information on the internet. Consequently, we can notice the fact that this right affects only the consumer cloud and it is not intended to have targeted impact on private clouds. However, the effect this right will generally have will mainly be determined by enforcement procedures.

Furthermore, the individuals will have the possibility to move their data from a service provider to any other internet company. Thus, the regulation introduces the principle of data portability[346]. In this respect, it has to be reminded that data portability is currently a problematic scenario for the cloud model. As in the case of the right to be forgotten, the enforceability of such a right will play a major role.[347] Basically, we know from experience that the industry is always on the look out for adding new functionalities to services in order to maintain competitive on the market. Therefore, we can envision the fact that data portability will become part of the services' functionality that helps companies to compete on the market. Consequently, the less portable data will be, the more unattractive will be for consumers. Data portability could represent therefore a value added element for which companies would require a fee. The underlying idea behind this is that the more basic the service is, the easier it will be for data to be ported and, vice-versa – the more complex the service gets, the harder it will be to assure data portability. Therefore, it remains to be seen whether the Commission will interpret data portability as a default option. Since data portability involves the development of certain standards, a commonality of all services will need to be agreed upon. Thus, everybody will have to perceive data portability in the same way but it will also mean that there will be certain elements that cannot be ported. Yet, a

---

[344] Article 16 of the General Data Protection Regulation

[345] EurActiv, InfoSociety, *'Reding unveils new EU data protection rules'* (25 January 2012) <http://www.euractiv.com/infosociety/reding-unveils-new-eu-data-protection-rules-news-510381> accessed 6 February 2012

[346] European Commission, *'How does the data protection reform strengthen citizens'* rights?' <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf> accessed 6 February 2012

[347] It has been highlighted that the new data protection directive has to be revised in order to allow European service providers to remain competitive on the market. See Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 4

clarifying position regarding data portability is to be expected before the adoption of this proposal.

In relation to consent, it is specified that it must be given in a direct and explicit matter and that the text has to be clear and easy understandable even for children. Therefore, the regulation addresses particular attention to the consent of children and tries to protect the vulnerable from any unwanted effects the processing of their personal data might have.

Furthermore, of major impact is the personal data breach notification introduced in articles 31 and 32. The controller is now obliged to inform both the relevant authority and the data subject without undue delay about the event of a security breach that involves its personal information. It has been clarified that in the event of data "accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorized persons", were feasible, the notification must be sent within 24 hours.

Additionally, for business, of crucial significance is the fact that there will be a single set of rules that will apply to all companies established in Europe regardless if they choose to have their servers based within or outside the European Union. As a consequence, it seems that cloud providers would benefit from a much more solid and harmonized regulatory approach.

Furthermore, another aspect that contributes to legal certainty is the fact that there will be a "one-stop-shop"[348] for business. As article 51 and Recital 98 set forth, companies will only have to deal with a single data protection authority, the supervisory authority of the Member State in which the controller or processor has its main establishment. We would like to emphasize the importance of the rules enshrined in Chapter V of the proposal. In this sense, because they relate to the transfer of personal data to third countries or international organizations they gain particular relevance for cloud computing due to the "globalised nature of data flows".[349] Therefore, these provisions seek to provide clear rules for international data transfers and make exchanges of information more secure.[350] Moreover, the same chapter explicitly mentions binding corporate rules (BCR) as another instrument that will award data controllers or processors with certain flexibility while strengthening the protection of individual rights and freedoms.[351] It is important to mention that BCR will become legally

---

[348] Article 51 of the General Data Protection Regulation

[349] Also explained in European Commission's, *'How does the data protection reform strengthen citizens'* rights?'

[350] European Commission, Vice-President of the European Commission, EU Justice Commissioner Viviane Reding, *'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age'* (22 January 2012) SPEECH/12/26 <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26> accessed 30 January 2012

[351] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 5 and Rohan Massey and others, National Law Review, *'Proposals for Reform of the Data Protection Regime and Binding Corporate Rules'* (31 January 2012) <http://www.natlawreview.com/article/proposals-reform-data-protection-regime-and-binding-corporate-rules> accessed 6 February 2012

binding for companies, thus this aspect is also of importance for the development of cloud computing.[352] Additionally, as article 35 specifies, companies with more than 250 employees will have to appoint a data protection officer.

Having all this in mind, some have raised warnings about the possible "chilling effect" the new provisions can have in the European online environment.[353]

As we have mentioned the proposal pack contains a regulation and a directive. The new directive will deal with general data protection rules in relation to law enforcement and judicial cooperation on criminal matters. The application of this directive is related to both national but also trans-border transmission of data.

Considerable critique has been addressed related to the European Commission's approach by calling it a "two-tier systems on citizens' rights"[354]. Moraes emphasizes that "privacy rights should also be strictly enforced in criminal investigations and judicial procedures". Moreover, the European data protection supervisor (EDPS) Peter Hustinx stated that "the Commission has not lived up to its promises to ensure a robust system for police and justice.[…] It is difficult to understand why the Commission has excluded this area from what it intended to do, namely proposing a comprehensive legislative framework." [355]

At the same time, the proposal was also the target of a number of objections. Already, significant critiques has been addressed by the industry calling the penalty for not immediately reporting data breaches "taxes" on companies[356]; others have reiterated the same idea but also added that it could "put some companies to jeopardy"[357]. Moreover, despite the recurrent recitals of the regulation safely addressing the issue of processing data for historical, statistical and scientific research purposes, historians and US institutions have also raised critique related to this matters. In this sense, they expressed the fear that significant information for historical records will be negatively affected by "the right to be forgotten".[358]

---

[352] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 5

[353] EurActiv, InfoSociety, *'Reding unveils new EU data protection rules'* (25 January 2012)

[354]Claude Moraes, S&D spokesperson for civil liberties, justice and home affairs quoted in EurActiv, *'Reding unveils new EU data protection rules'* (25 January 2012)

[355] The European data protection supervisor (EDPS) Peter Hustinx quoted in EurActiv, *'Reding unveils new EU data protection rules'* (25 January 2012)

[356] BBC News, *'EU data protection law proposals include large fines'* (25 January 2012) <http://www.bbc.co.uk/news/technology-16722229> accessed 30 January 2012

[357]Adam Malik quoted in BBC News , *'EU data protection law proposals include large fines'* (25 January 2012)

As a matter of fact the "draconian"[359] new rules appear to some as "the most radical global attempt ever to regulate exploitation of personal information"[360]. Even the International Chamber of Commerce expressed its concerns related to compliance and the innovation curve of the companies on the long-run.[361]

In this sense, we can connect the above warnings addressed by industry, practitioners and institutions with the already expressed idea that cloud computing needs a solid, clear and feasible policy that leave room for its prosperous development. Whether or not the proposal will have a positive impact on the cloud model cannot be assess at the moment, but it might also be that this set of rules add up to the current unsatisfactory regulatory framework[362] that do not permit a solid approach for cloud computing regulations. However, as observed by practitioners, the opportunity this regulation gives to companies is to promote themselves as "safe processors" by adjusting to the new rules.[363] However, despite this possible scenario, the question remains if the new piece of regulation brings the correct balance the cloud environment needs to develop. Apparently, practitioners have already stated that this new piece of regulation is a "missed opportunity". It was said, "the Commission had the opportunity to implement a law that both protects consumers and recognizes the reality of global data sharing and new technologies (such as social networking and cloud computing)"[364] but that it failed to succeed in achieving this.

Additionally, we note that the current the data protection legislation is not implemented uniformly throughout EU/EEA and therefore, where different set of rules and where several

---

[358] Claire Davenport, *'Breach of new EU online data rules to carry high fines'* (25 January 2012) <http://www.reuters.com/article/2012/01/25/us-eu-dataprivacy-idUSTRE80O0X220120125> accessed 30 January 2012

[359] Timothy Kirkhope MEP quoted in EurActiv, *'Reding unveils new EU data protection rules'* (26 January 2012) and Jane Finlayson-Brown, Allen & Overy data protection team quoted in Warwick Ashford, *'EC publishes proposed data protection reforms'* (25 January 2012) <http://www.computerweekly.com/news/2240114326/EC-proposes-a-comprehensive-reform-of-data-protection-rules> accessed 30 January 2012

[360] Eduardo Ustaran, partner and head of the European data protection team at Field Fisher Waterhouse quoted in Vanessa Wozniak, *"Proposed online privacy rules are a 'missed opportunity'"* (25 January 2012) <http://www.thelawyer.com/proposed-online-privacy-rules-are-a-missed-opportunity/1011080.article> accessed 30 January 2012

[361] Stephen Pattison, the UK CEO of the International Chamber of Commerce quoted in Claire Davenport, *'Breach of new EU online data rules to carry high fines'* (25 January 2012)

[362] As concluded by Jasper Sluijs and others in *'Cloud Computing in the EU Policy Sphere'*

[363] Vanessa Wozniak, *"Proposed online privacy rules are a 'missed opportunity'"* (25 January 2012)

[364] Furthermore, it is stated "Setting businesses an unachievable goal, whether they are European or the US technology giants that the Commission unfairly seems to be seeking to curb, is unhelpful in terms of compliance and frankly bad for consumers." Mark Watts, data protection partner at technology law firm Bristows quoted in Claire Davenport, *'Breach of new EU online data rules to carry high fines'* (25 January 2012)

jurisdictions apply, it is difficult for providers to inform their users about their rights and obligations towards law enforcement bodies.[365]

3. Conclusions

The first part of our discussion showed us how problematic is for cloud providers to identify their position in terms of controller or processor of personal data. As immediate consequence, this implies that cloud providers cannot properly assess the respective application of civil liability and penalties for non-compliance with data protection laws. Hence, this unclear context in which cloud providers have to interact with consumers leads to serious threats in relation to safeguarding consumer's rights and complying with requirements. In fact, due to the substantial issues at stake some authors concluded that the analysis should be made on a case-by-case basis[366] and others to suggest new models of approach[367].

The second part provided an overview of the newly introduced rights of the General Data Protection Regulation and made a brief analysis of its major provisions targeting individuals and business alike. Additionally, we also highlighted the significance the enforceability of these rights will have on their practical materialization. Moreover, we saw a glimpse of the amount of critique this proposal has received so far. However, more importantly, we underlined that the new data protection proposal is on its way to represent the first pan-European set of privacy rules[368]. Furthermore, we pointed out that it contains significant provisions bringing along specific problematic targeting cloud providers. If the provisions analyzed above will come into force, they will bring another set of cumbersome requirements cloud providers need to comply with. If fact, using Hon's metaphor, this Regulation does little to brake the riddle of the "cloud of unknowing".

---

[365] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 5

[366] Ronald Leenes, 'Who controls the cloud' (2010) 11 IDP

[367] Hon and others suggest cloud providers should be seen as neutral intermediaries, and therefore that the intermediary liability provisions of the ECD should apply. See W Kuan Hon, Christopher Millard and Ian Walden, *'Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2'* (21 March 2011)

[368] BBC News, *'EU proposes 'right to be forgotten' by internet firms'* (23 January 2012) <http://www.bbc.co.uk/news/technology-16677370> accessed 30 January 2012

Part III. Directive 2006/24/EC[369]

This section will start with a short introduction regarding the scope and background of the directive and the subjects to which this regulation applies. Furthermore, the directive's provisions will be analyzed followed by a series of conclusions and implications for the cloud model.

To begin with, Directive 2006/24/EC deals with the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and it amends Directive 2002/58/EC.

For a better understanding of the regulatory build-up in this sector, we will present the chronological sequence that led to the adoption of the Data Retention Directive. In 1995, Europe became a pioneer by adopting specific privacy regulation in order to ensure a better protection of individual rights and freedoms. Thus, Directive 95/46/EC was adopted to ensure the free flow of personal data in the Community. Additionally, as we have already seen, in 2002, the Privacy Directive was complemented with a set of privacy rules that specifically address the electronic communications sector – Directive 2002/58/EC. Following this, Directive 2006/24/EC amends Directive 2002/58/EC. Consequently, this amendment aligns Directive 2002/58/EC's article 6 provision of erasing data after the purpose of the transmission has been achieved with the new data retention rules. Hence, the Data Retention Directive contains derogations from article 6 of the ePrivacy Directive.

The range of actors towards which the Data Retention Directive and consequently the Cybercrime Convention are aiming at, constitutes of a large palette of service providers, from telecommunication providers to all types of cloud providers (SaaS, PaaS and IaaS).

As part of a larger fight against terrorist attacks and other sorts of criminal activities, the data retention directive was created as a response to the disruptive events following London and Madrid. Therefore, next to the Cybercrime Convention and the Framework Decision on Attacks against Information Systems, the provisions from the data retention directive serve as an important instrument for law enforcement purposes.

The European retention duties can be discussed via the provisions of Directive 2006/24/EC but also through contractual agreements.[370] Therefore, first we will discuss the provisions of the directive and then shortly refer to the contractual retention.

---

[369] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006 hereinafter the "Data Retention Directive"

The derogations from this directive sum up the fact that service providers are asked to identify any electronic communication that runs through their service.[371] A first element that opens the discussion about retention duties under this directive is the fact that the retention and communication of data is only available for appointed national institutions and is done for the purpose of "investigation, detection and prosecution of serious crime as defined by each Member State in its national law".[372] Recitals 7 through 10 of the directive shed light upon what could fall under the category of serious crime, namely terrorism and organized crime. However, Recital 5 refers to the investigation, detection and prosecution of criminal offences; therefore it generalizes the purpose of retention of personal data. In this respect we have to underline the fact that criminal offences can comprise of a wide range of behavior. Accordingly, crimes such as copyright infringement, child pornography, denial of service attacks and why not, harassment, unlawful parking[373] and trespassing are included. Additionally, Recital 9 mentions article 8 of the European Convention on Human Rights and therefore widens even more the limits of the exception to the confidentiality principle.

In conclusion, a second element valuable to our analysis is the fact that the purpose of the derogation covers both criminal but also civil matters[374]. We first saw that Directive 2006/24/EC mentions the investigation, detection and prosecution of serious crimes but simultaneously mentions the investigation, detection and prosecution of criminal offences. Consequently, as Moiny highlights, member states have the possibility to make use of the requirement concerning the disclosure of data in civil proceedings. In other words, member states are given the task to balance the use of this provision in the fight against copyright infringement with the fundamental rights referring to respect for private life and protection of property.[375]

Therefore, the derogation from the confidentiality rule of electronic communications should be fairly and clearly expressed. For this reason, Member States have the obligation to define

---

[370] Jean-Philippe Moiny, *'Are Internet protocol addresses personal data? The fight against online copyright infringement'* (2011) 27 (4) Computer Law & Security Review, 349 <http://pdn.sciencedirect.com/science?_ob=MiamiImageURL&_cid=271884&_user=522558&_pii=S0267364911000707&_check=y&_origin=article&_zone=toolbar&_coverDate=31-Aug-2011&view=c&originContentFamily=serial&wchp=dGLbVlS-zSkWA&md5=294df64994838abceecfab506eb71896/1-s2.0-S0267364911000707-main.pdf> accessed 21 January 2012

[371] Ibid.

[372] Article 1.1 of Directive 2006/24/EC

[373] Jean-Philippe Moiny, *'Are Internet protocol addresses personal data? The fight against online copyright infringement'*, 350

[374] The civil matters could represent copyright infringements, as illustrated by the ECJ in *Promusicae v. Telefonica*.

[375] Jean-Philippe Moiny, 'Are Internet protocol addresses personal data? The fight against online copyright infringement', 350

the meaning of serious crimes[376]. Also Member States have to specify the period until which data has to be retained. At this moment, the retention periods vary considerably among member states. For example, Romania, Germany and Lithuania have a retention period of six months; Bulgaria has a retention period of one year and Ireland, Italy and Slovakia adopted a period of two years.

Thirdly, by referring to article 15 of Directive 2000/31/EC, the same author points out that the duty to retain data can be present also for other types of providers (rather than electronic communications providers/public communication network providers), namely also for information society service providers which concern storage agreements.[377] Therefore, we would like to highlight the importance of article 15 of the E-commerce Directive. By analyzing its provisions, we can draw the conclusion that we can speak of two types of storage retention. On one hand, we have the Data Retention Directive imposing the retention of data and on the other hand, we also have the E-commerce Directive establishing rules for storage. Therefore, it seems that the retention regime from the E-commerce Directive is of a higher level than the one coming from the Data Retention Directive due to its larger applicability – not only telecommunications providers but information society service providers as well. Accordingly, we can therefore consider the implications for cloud providers. The retention obligation that can be enforced by the means of article 15 of the E-commerce Directive could lead to transforming information society service providers and thus cloud providers, into very intrusive parties in relation to the users. Through the existence of such a possibility, the provider-consumer relationships may be significantly affected. Moreover, through this type of requirements, providers may become the tools for governments to slip onto a highly obtrusive manner of regulating behavior. By this we mean the fact that by requiring retention of data (typically through the means of recording IP addresses), providers might be forced to step out of their agreements with clients and act as instruments which the state uses to counterattack illegal activities, thus enlarging the scope of the derogation from article 6 of the Data Retention Directive.

An additional aspect relevant to our discussion about cloud computing is analyzed by Vries and others. After examining the recent tumult related to the implementation of the data retention directive in some countries[378], the authors come to the significant conclusion that the major issue related to data retention is not only related to the storage and the retention of data,

---

[376] Article 2.b) of the United Nations Convention against Transnational Organized Crime adopted by General Assembly resolution 55/25 of 15 November 2000 contains an international definition of serious crime, seen as a "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".

[377] Jean-Philippe Moiny, 'Are Internet protocol addresses personal data? The fight against online copyright infringement', 350

[378] As early as 2010, a lot of debate revolved around the Data Retention Directive. The article which we are making reference to especially analyses the German ruling on the data retention directive but other national courts such as the Romanian, Swiss and Irish ones have dealt with this problematic internally.

but also to the importance of use and access of data, which is a matter for each member state to decide upon.[379] Additionally, the authors point out the fact that not all states award the same attention to this distinction and its importance[380]. The Federal Constitutional Court of Germany treats this matter extensively because of the fact that private companies (and not national institutions) perform the retention of data and because of the application of the defining notions of "direct" and "indirect use". The authors point out that direct use can contribute to assembling behavioral and mobility patterns, thus specific protection methods should be taken into account.[381] Furthermore, the indirect use refers to government officials to demand information from service providers about specific subscribers via their IP address. As the German judgment underlines, the requests can be permitted to a larger extent than the "request and use of telecommunication traffic data themselves".[382]

As we observe, these issues stretch beyond simple regulatory mismatches and reveal more fundamental aspects, directly connected to the principles of proportionality and transparency and to state over-interventionism on individuals' life.[383] For our discussion related to cloud computing, this unresolved and unstable arena in which the cloud model it is stepping into cannot prove to be productive; such a young, highly beneficial but underdeveloped service delivery model needs more solid grounds to anchor itself. Therefore, the first major conclusion regarding the impact of data retention obligations for cloud providers comes as a warning to be cautious regarding the possible negative effect cloud would have to endure in this data retention entanglement; therefore, we acknowledge the existence of serious barriers centrally placed on the path towards the full development of the cloud model.

A further aspect to be discusses is that, since the data needs to be destroyed at the end of the retention period[384] we can somewhat speak about a technical problem for cloud providers. As it is already known, the data stored in the cloud could be located potentially anywhere in the world. Moreover, the information is not necessary stored in full blocks; therefore, components of same data are dispersed among vast storage centers globally located. It is then difficult to reassure the exact reassembly of data but it generally relies on the implemented type of

---

[379] Katja de Vries and others, *'Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention'* (May 2010) Centre for European Policy Studies - Liberty and Security in Europe, 4 <http://www.ceps.eu/book/proportionality-overrides-unlimited-surveillance> accessed 15 January 2012

[380] The authors give the UK as an example to show the difference in approach related to this matter.

[381] Katja de Vries and others, *'Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention'*, 5

[382] Katja de Vries and others, 'Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention' quoting para 254 of the German Constitutional Court judgment

[383] Katja de Vries and others, 'Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention', 6

[384] Art 7. (d) Directive 2006/24/EC

technical solution to do it.[385] Therefore, a further look needs to be given to the complexities of full deletion. In this sense, we need to mention that every IT infrastructure has a complex back-up system[386]. Therefore, a complete deletion needs to take place both at server level but also from the back-up system. On a clarifying note, we would like to address the issue whether the back-up system is part of the publicly available communication service. Of course, a clear cut position can be taken after considering the definition of public. However, a much more evident fact shows that the discussion is not particularly relevant. In this respect, if we take the example of a public cloud such as Amazon, we can easily observe that it does not seem rational to keep the data on a back-up system once it had to be deleted; space in such type of business models is essential. Hence, since we have the argument of pragmatic business practices, we will not go further into discussing if back-up systems are part of the publicly available communication service, although even without looking at a definition we can understand that it is in fact a component of the service otherwise the service will not be reliant at all.

As a related note, Moiny makes a thorough analysis of SNS and he meticulously considers communication and related protection scenarios taking Facebook as an example. Although his analysis is valuable and relevant in the cloud environment, it detaches from the scope of this paper. However, several interesting points can be presented for our discussion about data retention and privacy. First, Moiny identifies two stages of communication.[387] The initial stage of communication is related to the use of the Internet Access by both the sender and the recipient in order to operate their connection to a Social Network Site. The second stage of communications is translated into the data stored by the Social Network Site in order to deliver them corresponding to the privacy settings of the user. The author underlines the fact that article 5 of the ePrivacy Directive does not give clues whether the confidentiality of communication protection includes this second stage of communication. Furthermore, he points out that by not offering protection to this type of stored communication the principle of confidentiality may be hampered.[388] However, a correlation has to be made with the new wording of paragraph 3 of article 5 as noted in Directive 2009/136/EC. Here, the text indicates the fact that "Member States shall ensure that *the storing of information, or the gaining of access to information already stored*, in the terminal equipment of a subscriber or user".[389]

---

[385] E-mail from Radu Epure, UNIX Administrator at Gameloft to author (20 December 2011)

[386] The term redundancy is used when an IT infrastructure relies of multiple layers of back-up systems.

[387] Jean-Philippe Moiny, *'Cloud Based Social Network Sites: Under Whose Control?'* in Alfreda Dudley and others (eds) Investigating Cyber Law and Cyber ethics: Issues, Impacts and Practices (2011) IGI Global forthcoming, ch 9, 169 < http://www.igi-global.com/chapter/cloud-based-social-network-sites/59942> accessed 21 January 2012

[388] Jean-Philippe Moiny, *'Cloud Based Social Network Sites: Under Whose Control?'*, 170

[389] Article 5.3 of Directive 2009/136/EC

Finally, we have reached the point where the contractual retention is going to be discussed. As Moiny reveals after considering the EMI Records et al. v. Eircom (IEHR 2010) case, IAPes cannot contractually identify subscribers and retain data.[390] After considering two major difficulties that can be deducted from the above-mentioned case, Moiny reaches the conclusion that in the absence of a "clear, accurate, predictable and proportionate"[391] legislative basis to identify subscribers, IAPes do not have legitimate grounds for contractually retaining data. The difficulties the author identifies are in the first place related to the consent IAPes would have to obtain from the users according to article 15.1 of Directive 2002/58/EC (and as Directive 2009/136 emphasizes, the prior consent) and second, the problem of an uninfluenced given consent.[392] The reasoning behind the second difficulty springs out from the fact that if the consent cannot be obtained through the means of article 7 of Directive 95/46/EC, IAPes could still require contractual consent provided that IP addresses are seen as personal data.[393]

In conclusion, when discussing the limitations of retaining and communicating data to the relevant authorities, reading throughout the articles and the recitals of the directive we can see that the boundaries are not perfectly shaped and leave room for considerable national law appreciation. As an example, we can mention the Greek implementation of the Data Retention Directive which obliges providers to locate their servers on national territory. As it has been pointed out, different implementations of data retention provisions will not only signify major compliance costs for cloud providers but they will also have hindering effects on the flexibility cloud services need in order to develop.[394] Moreover, of substantial importance is the fact that there have been identified two different directives that can gain application in relation to data retention.

---

[390] Jean-Philippe Moiny, *'Are Internet protocol addresses personal data? The fight against online copyright infringement'*, 352

[391] Ibid.

[392] Jean-Philippe Moiny, *'Are Internet protocol addresses personal data? The fight against online copyright infringement'*, 352

[393] Ibid.

[394] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 6

Part IV. Information Society Service Provider liability

The scope of this section is to reflect on how the liability regime set out in Directive 2000/31 renders application to cloud providers.

Briefly pointing a link to the first part of this chapter regarding ePrivacy, we can notice that the even Recital 31 of Directive 2009/136/EC attests that the provider cannot be responsible "for merely transmitting user-generated information ('mere conduit' rule)" and certifies that "it is not a provider's task to define what is lawful or harmful as to content, applications and services". Therefore, in respect of liability for the illegal processing of data, Cunha underlines the fact that the Data Protection Directive provisions need to be aligned with the ones in the E-commerce Directive, which, as we will shortly see, contains "some exemptions for ISPs, when they transmit, host, or cache user-generated content"[395]. Thus, as the author points out, "The [...] legislation seems to confirm the need to limit the liability of the provider"[396].

It is also important to observe the fact that DAE's Annual Progress Report placed the reference to encouraging cloud services under e-commerce services as key sector under which it would be fortified.[397] As Hon and others pointed out, beside stimulating development of electronic commerce within the EU, the Directive had the scope of harmonizing "liability defences for service providers which act as intermediaries, because it was felt that differences in intermediary liability across different member states were impairing the development of cross-border services and distorting competition within the EU". [398]

Therefore, the European approach[399] that has been given to the issue of online intermediaries liability is a horizontal one. This implies that, contrary to the vertical approach that addresses

---

[395] Mario Viola de Azevedo Cunha and others, *'Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web'* (2011) EUI, 5 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1953904> accessed 6 February 2012

[396] Ibid.

[397] European Commission, Digital Agenda for Europe Annual Progress Report (22 December 2011) 3

[398] W Kuan Hon and others, *'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 2'*, 26

[399] The observations in this chapter are limited to the European regime. However, we can mention the fact that, as already stated in chapter three, the issue of online intermediaries liability originated in the USA where it was adopted from a vertical perspective; meaning that liability is seen in relation to particular types of content such as libel, pornography, material infringing copyright, material invading privacy. See Charlotte Waelde and Lilian Edwards, *'Online Intermediaries and Liability for Copyright Infringement'* (2005) WIPO Workshop Keynote Paper Geneva, 4 < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159640> accessed 6 February 2012

liability arising from specific types of content, the horizontal implementation recognizes the immunity for all types of content that could allocate responsibility.[400]

In this sense, the liability regime has a wide meaning covering not only ISPs but also information society service providers or "intermediary service providers" under the terminology of the E-commerce Directive.[401] Therefore, the range of subjects falling under these provisions is also shown in the first report of the European Commission on the application of Directive 2000/31/EC. The report states that

> "The limitations on liability provided for by the Directive are established in a horizontal manner, meaning that they cover liability, both civil and criminal, for all types of illegal activities initiated by third parties."[402]

Given the definition, the intermediary service provider liability regime covers, aside the traditional ISP sector, also parties involved in transacting online goods or services online. As a result of the broad coverage of actors, also cloud providers are subject to the liability regime of the E-commerce Directive.

Furthermore, we need to underline the fundamental particularity of the internet where everybody is dependent on internet access providers to publish or distribute material on the internet.[403] Therefore, "ISPs are seen as the natural gatekeepers to the Internet" and act as tools for preventing illegal and offensive material to spread over the internet.[404]

However, the encountered difficulty refers to sticking the appropriate balance between awarding compensation to rightsholders on one side and the necessity of protecting intermediaries from being hold responsible for occurring illegal activities.

---

[400] Charlotte Waelde and Lilian Edwards, *'Online Intermediaries and Liability for Copyright Infringement'*, 4

[401] To briefly remind, an "information society service" is represented as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service."; a "recipient of a service" is "any natural or legal person who... uses an information society service...". See article 2(a) of Directive 2000/31/EC and article 2(d) of Directive 2000/31/EC.

[402] Commission of the European Communities, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF> (last accessed February 23, 2011), 12

[403] Charlotte Waelde and Lilian Edwards, *'Online Intermediaries and Liability for Copyright Infringement'*, 15

[404] Ibid., 17

In this sense, the E-commerce Directive addresses three activities of ISPs that provide immunity against claims and awards circumstantial nuances to the margins that have to be respected in order to still enjoy protection. In this sense, they avoid being held responsible for criminal liability if they have no "actual knowledge" of "illegal activity or information" and they cannot be accountable for civil liability if they have no such actual knowledge and are not aware of "facts and circumstances from which the illegal activity or information is apparent.[405] Given these circumstances, we point out that the liability immunity is restricted via the "notice and take down" system. In other words, when the circumstantial nuances mentioned above are triggered, the ISPs are obliged to "block access to or take down the content".[406] However, concerns have been addressed to the fact that the "notify and take down obligations for illegal content" present ongoing uncertainties, therefore specific procedures of the notice and take down mechanism still remain unclear, thus forcing cloud providers to include this on the list of regulatory dilemmas they need to battle with.[407]

For this purpose, we will first identify the relevant articles from the E-commerce Directive and make a brief analysis of the provisions. Second, we will make use of the recent L'Oreal v eBay case in order to show the exceptions that have been made to the established principles. Finally, we will conclude with a series of liability projections in terms of their application to cloud providers.

One of the main sources that may trigger cloud provider liability is placing illegal content such as copyrighted material in the cloud[408]. So far, cloud providers have carefully protected themselves in case such scenarios will occur by inserting vast general terms and conditions that will fully protected them against liability. However, users expect liability provisions from cloud providers. To name a few, the users are particularly concerned about the loss of data, the lack of service quality and the withdrawal of service.[409]
Additionally, we need to specify the distinction between liability springing out from bilateral contracts among service providers and business and liability born in consumer-cloud relationships which can relate to one of the following E-commerce directive provisions: mere conduit, caching and hosting. Therefore, we can observe a differentiation between liability that springs from service level agreements made between consumers (and SMEs) and

[405] Charlotte Waelde and Lilian Edwards, *'Online Intermediaries and Liability for Copyright Infringement'*, 24

[406] Ibid., 28.

[407] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 3

[408] Ibid.

[409] Ibid.

providers and responsibility born from individually negotiated contracts as in the case between large companies and providers.[410]

As an initial observation we point to the fact that cloud providers, in theory, are not knowledgeable of the content which is being transmitted. Therefore, "mere conduit" rules seems to be the most appropriate to apply. Accordingly, we can see that cloud providers are not liable when they pertain no involvement with the content that is being transmitted. Oppositely, if the cloud providers in a consumer space would pursue towards looking into content it will represent an illegal activity and thus they will be held liable. As a related side note, we can specify that the "deep packet inspection" technique (a technique which is used to prioritize the transmission of data) although it reveals the type of information transmitted (voice, video or data) it does not in any way interfere or read the content.

1. Provisions analysis

Before launching into the article analysis it is important to specify the legal context in which online intermediaries could assume responsibility for the users' activities. As Headdon observes, the relationship between an online intermediary and an infringer will have a contractual basis.[411] Consequently, any activity related to the provided service that infringes third party rights may be avoided by enforcing specific terms and conditions on the user. Furthermore, the intermediary is able to expeditiously intervene by removing the infringing content or end the contractual relationship with users involved in unlawful activities. Therefore one opportunity for the rights-owners is that it may be less costly to file claims against a single intermediary rather than against many infringing users.

The articles this section is going to work with are articles 12 to 15 under section 4 of the directive which address the liability of intermediary service providers. Under the provisions of these articles, we can observe that ISS providers have a liability regime limited to particular conditions. Therefore, the directive specifies three situations in which ISS providers can be held responsible. The first situation is when the ISS consists of the transmission or access to a communication network. As article 12 stipulates, the service provider will not be liable for the information transmitted if he does not initiate the transmission, if he does not select the receiver of the transmission and if he does not select or modify the information

[410] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 4

[411] Toby Headdon, *'Beyond Liability: Injunctions after L'Oreal v eBay'* (2011) 22 (3) Computers and Law Magazine of SCL, 1 < http://www.blplaw.com/media/pdfs/News%20and%20Views/Headdon.pdf> accessed 6 February

transmitted. These rules remain valid as long as the transmission does not involve storing the information for a longer period than it would be necessary.[412]

The second situation involves the automatic, intermediate and temporary storage of information with the specific purpose of making the transmission process more efficient. Therefore, in relation to chaching information, the service providers will not be held accountable if they do not modify the information, if they comply with the conditions related to access to information and if they promptly intervene to remove or disable the access to the information once they becomes aware of the fact that this information has been made unavailable.[413]

The third situation deals with hosting, therefore the immediate link to cloud computing does not need further underlying since we have already discussed in chapter three the specifics of providing IaaS types of services. As article 14 specifies, "the service provider will not be held liable for the information stored at the request of a recipient of service". Therefore, the provider has to be unaware of the illegal activity or information and, once he becomes knowledgeable of such an activity he has to promptly remove or disable access to the information in order to avoid liability.

Additionally, article 15 of the directive makes particular reference to the fact that there is no imposed general obligation to monitor illegal activity for service providers. However, member states are given the possibility to impose such an obligation to service providers.[414] As a consequence, the discrepancies that could appear in various Member States may create significant instability for cloud providers and will contribute to a generalized state of uncertainty regarding compliance with the requirements across European borders.

It is also important to mention recital 42 that specifies that the exemptions from liability cover only cases where the activity of the ISP "is of a mere technical, automatic and passive nature". More specifically, it describes that this type of activities presuppose that "the information society service provider has neither knowledge nor control over the information which is transmitted or stored."

[412] Article 12.2 of Directive 2000/31/EC

[413] Article 13.1.a,b,e of Directive 2000/31/EC

[414] Article 15.2 of Directive 2000/31/EC

2. L'Oreal v eBay case

After seeing the liability regime set forth by the E-commerce Directive, it is significant to present some further considerations from practice. Therefore, this section will analyze the dispute between L'Oreal and eBay that brings new insights regarding liability issues for service providers.

On 12 July 2012, the European Court of Justice released its decision regarding the L'Oreal v eBay[415] dispute. Although the case touches upon many aspects such as advertising keywords in sponsored links and trademark related issues[416], the relevance of analyzing this case mainly relates to its impact on online market place operators. Hence, this case shows that service providers will encounter much more difficulty to avoid liability under the E-commerce Directive.[417]

First, we will present a short summary of the conflict. Next, we will underline the significance the ECJ ruling has on service provider liability. Finally, the section will end with conclusions addressing the applicability of the E-commerce Directive to cloud providers.

On eBay, the well-known internet marketplace, sellers were trading authentic L'Oreal products as well as counterfeit products. Furthermore, eBay was using L'Oreal marks on its website search functionality but it also purchased keywords that triggered sponsored links on third party search engines.[418] L'Oreal filed a claim against both sellers and eBay demanding joint liability for infringing its trade marks and unlawful sales. The ECJ's decision affirmed the eBay sellers infringing acts but did not find eBay jointly responsible for its traders' unlawful actions.

An important issue upon which the ECJ had to provide guidance was whether online market places can invoke article 14 of the E-commerce Directive in order to avoid liability. The Court referred to the previous case *Google France* and pointed out that the aspect of active involvement needs to be examined. In this sense, it has to be determined whether eBay had a "neutral" position regarding the data that is stored. Therefore, the Court suggested that if the role of the service provider remained "merely technical, automatic and passive, pointing to a

---

[415] C-324/09, L'Oréal SA and others v eBay International AG and others

[416] Sara Dethridge and others, *'EU update'* (2011) 27 Computer Law and Security Review, 553 < http://www.sciencedirect.com/science/article/pii/S0267364911001579> accessed 6 February 2012

[417] Ibid.

[418] Ibid.

lack of knowledge or control of the data"[419], they should not be held liable. Still, the Court did not give a definite solution to this issue. Consequently, whether eBay could make use of the "hosting defense"[420] was left for the national courts to decide upon. However, the Court made it evident that by offering assistance to the traders on the platform (which included optimizing the presentation of the offers or promoting the offers[421]), eBay became actively engaged and therefore, by performing such a role it stepped away from the protection of article 14 of the E-commerce Directive. Following the general rule, eBay should have "expeditiously acted to remove or to disable access to the information"[422] in order to be protected under the liability regime of the directive. Additionally, the Court's motivation specified that once the provider gains the possibility to acquire actual knowledge of the illegal activity in one way or another (for example through the means of a particular unlawful advertisement), it must follow the obligation to monitor.[423]

We can observe the fact that the Court was consistent[424] in its approach of leaving the meaning of "active" and "passive" for national courts to dwell upon. Moreover, Clark and Schubert draw attention to the fact that the Court neglected to consider that the customization of offers addressed to seller-customers is not done on an individual basis but it represents a mechanical process.[425] Therefore, the authors underline the fact that confusion still resides where a mere interface is enabling the seller to advertise the offer and when it allows the tailoring of the presentation of the offer and thus showing an active involvement.[426]

In conclusion, the impact of this case translates into the favorable position of rights owners to demand notifications from online intermediaries about any infringing activities. In addition to the notifications, rights owners can ask the service provider to block or remove the infringing content. And since rights owners can threaten with injunction application[427], service providers

---

[419] Birgit Clark and Maximilian Schubert, *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'* (2011) 6 (12) Journal of Intellectual Property Law & Practice, 886 < http://jiplp.oxfordjournals.org/content/6/12/880.short?rss=1> accessed 6 February 2012

[420] Sara Dethridge and others, *'EU update'*, 554

[421] Birgit Clark and Maximilian Schubert, *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'* (2011) 6 (12) Journal of Intellectual Property Law & Practice, 886

[422] Article 14.1.b) of Directive 2000/31/EC

[423] Birgit Clark and Maximilian Schubert, *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'*, 886

[424] As in *Google France and Google Joined Cases C-236/08 to C-238/08 [2010] ECR I-0000; [2010] ETMR 30*.

[425] Birgit Clark and Maximilian Schubert, *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'*, 886

[426] Ibid.

[427] Toby Headdon, *'Beyond Liability: Injunctions after L'Oreal v eBay'*, 5

must consider their role very carefully and avoid being the target of copyright or trademark infringements. A cloud provider must be therefore very alert of this shift in the burden from trade mark holder to online operator. Moreover, we can see from the ECJ's judgment that national courts have to decide upon the "active" and "passive" elements and consequently allow a service provider to benefit from the liability exemption or not. Furthermore, the Court did not clarify the situations in which a service provider has "actual knowledge" about existing infringements.[428]

In conclusion, as we have seen in the last two sections, cloud providers have to award serious attention to the scenarios in which they could become liable. On one side, the new privacy proposal imposes cumbersome financial penalties if providers do not comply with the requirements and on the other side, as the L'Oreal and eBay case shows, there is an imminent threat for service providers to be held responsible for the user's infringing activities. Additionally, we have seen that the provisions in the E-commerce Directive also leave room for exemptions from the general obligation to monitor, generating therefore a wave of concerns and confusion for service providers in terms of the obligations they have to follow.

We would like to end with a short remark why liability has been chosen as central focus of this section. It is common knowledge that liability has a direct link to trust issues[429]. Affecting the human interaction with technology and the digital environment as a whole, sociologists[430] observed that there has been a shift in the default position of people in relation to these daily interplays in general. From this, it is facile to hypothesize that the goal major suppliers of cloud computing aim at - world wide usage - will not be embraced by fearful and reluctant users. Therefore, until measures that enable users to trust and safely rely on cloud computing are put into place, liability issues will always count in the detriment of any proclaimed benefits of technological advancement. In other words, until liability issues become clear and transparent, the envisioned welfare bringing functionality of any technological innovation will not be fully adopted by the masses.

---

[428] Birgit Clark and Maximilian Schubert, *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'*, 887

[429] Microsoft News Center, *'Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud'* (20 January 2010) <http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx> accessed 6 February 2012 and Brad Smith, General Counsel, Microsoft Corporation, *'Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing'* (20 January 2010) 3 <http://blog.seattlepi.com/microsoft/files/library/20100120smithspeech.pdf> accessed 6 February 2012

[430] Barry Glassner, *'The culture of fear: why Americans are afraid of the wrong things'*. (NY: Basic Books 1999)

CHAPTER FIVE - Concluding remarks

This chapter will summarize the series of conclusions our research has accompanied to.

The first chapter, while mainly technical and descriptive, revealed three important aspects. First, it underlined the fact that cloud computing is not a new technology or a new model. Instead, as we have emphasized throughout the paper, it represents a cyclical development in computing without presenting any novel and innovative technical aspects. Second, as various scientific and working group reports have consistently pointed out, the cloud model is still in an infancy stage and, therefore, a careful approach must be adopted to facilitate this development. Third, this first chapter showed the inherent potential and related benefits it allures not only to users and businesses, but also governments. Additionally, stressing the idea that cloud computing is at an early stage of development, this author could also launch the question whether its relationship to European regulation might change along with its future emergence.

The second chapter served as an introduction to the complexities of the telecommunications framework. In this sense, we have seen that major issues such as the net neutrality debate and convergent technologies still leave open questions in relation to the regulatory approach of IT specific technologies. Moreover, we have seen how some authors perceive the transformation of the telecommunications market to the "triple play" in relation to regulation. The chapter concludes by identifying the multitude of possible approaches legislators could consider in relation to the cloud.

The third chapter revealed a number of approaches and premises for the possibility of cataloguing cloud services as telecommunications services. In this respect, we have seen that from applying a per a contrario reasoning to the last part of the electronic communications services, there is a certain overlap between cloud services, electronic communications services and information society services. However, this author has also provided a significant analysis of the inherent cloud elements that may be another assessment point for delimiting the relationships between electronic communication services and information society services.

To sum up, although a per a contrario type of reasoning initially redirected this author's attention to a partial overlap of electronic communication services and information society services (which consequently implied the possibility of cataloguing cloud providers as telecommunication providers), this author has demonstrated that the complexities of such a situation are more far reaching. Therefore, the method of applying a per a contrario reasoning in block to the last part of the electronic communications definition does not offer a final verdict when discussing the circumstances of when a cloud provider would be seen as a telecommunications provider. Consequently, the analyzed direction did not reveal what part of the telecommunications regulations would apply to the cloud sphere.

Moreover, this author dispersed the blur created by the bundle type of service provisioning and also reached the conclusion that from a regulatory perspective there are not sufficient reasons to apply telecommunications regulation to cloud computing.

The forth chapter was dedicated to the analysis of the regulatory complexities cloud providers might become entangled. Particularly, security, data protection and liability provisions springing from both telecommunications regulations and the electronic commerce regime were presented and relevant remarks were highlighted in relation to cloud computing. To be more precise, in relation to the ePrivacy Directive, as part of the sector-specific regulation framework, a much stricter regime of obligations targeting solely at industry operators has been set. Therefore, it has been noted that other types of service providers are not burdened with such requirements. In relation to the Data Retention Directive we have seen that one of the substantial issues involved is the lack of its harmonized application. Moreover, the analysis of this directive's provisions identified a distinctive liability regime in correlation to the information society rules. Therefore, a substantial overall finding was the duality of the liability provisions set forth by the Data Retention Directive and the E-commerce Directive. In fact, from the interpretation of the E-commerce Directive and from the L'Oreal v eBay case study we have seen that the extent to which the liability regime actually applies to cloud providers is still unclear. Additionally, the forth chapter also explored the idea that the newly released the data protection proposal could add new and significant obligations to cloud providers.

However, as a general conclusion, this author has shown that cloud computing does not introduce new requirements for privacy. Instead, it has been shown that it redirects the legislative focus towards the existing gaps and discrepancies. Furthermore, it has been highlighted that the lack of harmonized rules on privacy among Member States contributes to the difficulties with which providers have to face. Therefore, because of the different laws and jurisdictions that apply to consumer data, it is problematic for providers to accurately inform the users about their rights and responsibilities in relationship to law enforcement authorities.[431]

Finally, this thesis would like to address some final remarks to the induced idea of a "cloud regulation".[432] This author remains skeptical to the adoption of cloud specific regulatory approach for several reasons. First, we need to take into consideration that due to the incipient phase of adoption and development, the current timing might not be favorable. Second, the model in itself does not pose new challenges but rather it highlights the need for a fine-tuning of the related pieces of regulation that apply. However, it is not only obvious, but also stringent, that issues such as data protection, law enforcement, security and liability need

[431] Cloud Computing Hearing with Telecommunication and Web Hosting Industry, 5

[432] As stated in RAND Europe, *'Understanding the Security, Privacy and Trust Challenges'* and European Commission Expert Group Report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'*

further and constant review and adjustments as cloud computing exposes thorny gaps and unaddressed issues. Third, the examination of the current tumultuous setting regarding privacy and security issues - in particular the new data portability, data retention obligations and data breach notification - point to a careful, balanced and wise approach in relation to the construction of a legal regime for the cloud. Therefore, we cannot stress enough the importance of a solid legislative approach instead of a hasty regulatory decision limited to seeing only the rapid economical benefits and growth this model can deliver in a fast period of time accompanied by putting more focus on the intricate web of domino legal obligations and implications it stirs up.

Bibliography

Books

Glassner B., *The culture of fear: why Americans are afraid of the wrong things* (New York, NY: Basic Books 1999)

Koenig, C. and others (eds), *EC Competition and Telecommunications Law* (Kluwer Law International 2009)

Articles & Journals

Alabau, A., Guijarro, L., *'The Electronic Communications Policy of the European Union'* (2011) Editorial Universitat Politecnica de Valencia

Clark, B., Schubert, M., *'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oreal v eBay'* (2011) 6 (12) Journal of Intellectual Property Law & Practice, 880-888

Cuijpers C., Koops B.J., *'How fragmentation in European law undermines consumer protection: the case of location-based services'* (2010) 33 European Law Review 2008, *880-897*

Dethridge, S. and others, *'EU update'* (2011) 27 (6) Computer Law and Security Review, 659–662

Dumortier, J., De Preter, C., *'The European regulatory framework for security and privacy protection in electronic communications'* (2006) 61 (34) Annals of Telecommunication, 443-457

Headdon, T., *'Beyond Liability: Injunctions after L'Oreal v eBay'* (2011) 22 (3) Computers and Law Magazine of SCL

Hon W.K. and others, --*'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1'* (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011

-- *'The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 2'* (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011

Humphreys, P., Simpson, S., *'Globalization, the Competition State and the Rise of the "Regulatory" State in European Telecommunications'* (2008) 46 (4) JCMS, 849–874

Jaeger, P.T. and others, *'Cloud Computing and Information Policy: Computing in a Policy Cloud?'* (2008) 5(3) Journal of Information Technology & Politics, 269-283

Janowiak, J.R., *'Convergence, the law and the future of the ICT sector'* (2005 North America)

Joint, A., Baker, E., *'Knowing the past to understand the present – issues in the contracting for cloud based services'* (2011) 27 (4) Computer Law & Security Review, 407–415

Jones, A., *'Convergence'* (2007) 12 (2) Information Security Technical Report, 69-73

Jones, R., Tahri, D., *'An overview of EU data protection rules on use of data collected online'* (2011) 27 (6) Computer Law and Security Review, 630-636

Kevin, W., *'The Network Utility'* (2011) 60 Duke L. J. 1761-1840

Larouche, P., *'Communications Convergence and Public Service Broadcasting'* (2001)

Leenes, R., *'Who controls the cloud'* (2010) 11 IDP

Lehr, W., Chapin, J., *'On the convergence of wired and wireless access network architectures'* (2010) 22 Information Economics and Policy, 33–41

Liu, Y., *'The Impact of Convergence on Telecommunications Law and Policy: A Comparison between Japan and Taiwan'* (2009)

Marston, S.R. and others, *'Cloud Computing: The Business Perspective'* (2011) 51 (1) Decision Support Systems, *176-189*

Moiny, J.P., -- *'Are Internet protocol addresses personal data? The fight against online copyright infringement'* (2011) 27 (4) Computer Law & Security Review, *348-361*

-- *'Cloud Based Social Network Sites: Under Whose Control?'* in Alfreda Dudley and others (eds) Investigating Cyber Law and Cyber ethics: Issues, Impacts and Practices (2011) IGI Global forthcoming

Robinson, W., *'Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act'* (2010) 98 (4) Georgetown Law Journal

Tardiff, T., *'Changes in industry structure and technological convergence: implications for competition policy and regulation in telecommunications'* (2007) 4 IEEP, 109-133

Vaquero, L.M. and others. *'A Break in the Clouds: Towards a Cloud Definition'* (2009) 39 (1) ACM SIGCOMM Computer Communication Review

de Vries, K. and others., *'Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention'* (May 2010) Centre for European Policy Studies - Liberty and Security in Europe

Waelde, C., Edwards L., *'Online Intermediaries and Liability for Copyright Infringement'* (2005) WIPO Workshop Keynote Paper Geneva

Yoo, C.S., *'Cloud Computing: Architectural and Policy Implications'* (2011) Technology Policy Institute

Working papers

Cunha, M.V. de A. and others, *'Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web'* (2011) EUI Department of Law Working Papers No. 2011/011

Sluijs, J.P. and others, *'Cloud Computing in the EU Policy Sphere'* (2011) TILEC Discussion Paper No 2011-036

Official documents, opinions, notes and technical reports

Armbrust M. and others, *'Above the Clouds: A Berkeley View of Cloud Computing'* (10 February 2009) Technical Report No. UCB/EECS-2009-28

Article 29 Data Protection Working Party, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive (2006) WP126

Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines (2008) WP 148

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (2010) WP 169

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertizing (2010) WP 171

Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile device (2011) WP 185

Commission of the European Communities, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

Cloud Computing Hearing with Telecommunication and Web Hosting Industry, Meeting Note (16 November 2011)

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Universal service in e-communications: report on the outcome of the public consultation and the third periodic review of the scope in accordance with Article 15 of Directive 2002/22/EC (23 November 2011) COM (2011) 795 final

European Commission, Digital Agenda

European Commission, Directorate General for Information Society and Media, *Digital Agenda for Europe Annual Progress Report* (22 December 2011)

European Commission, General Data Protection Regulation Explanatory Memorandum

European Commission, Information Society and Media, Expert Group report, *'The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010'* (2010) Public version 1.0

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), (2010/C 147/01)

Hewitt C., *'ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing'* (2008) 12 (5) IEEE Internet Computing, 96–99

Hogan, M. and others, National Institute of Standards and Technology, '*Cloud Computing Standards Roadmap – Version 1.0*' (2011) Special Publication 500-291

ICC Task Force on Privacy and the Protection of Personal Data, Summary of the Workshop on the Distinction between Data Controllers and Data Processors (International Chamber of Commerce, Paris 25 October 2007)

Itven H. and others, Telecommunications Regulation Handbook, *Module 1 - Overview of Telecommunications Regulations* (*Info*Dev Program of the World Bank 2000)

Mell P., Timothy G., Recommendations of the National Institute of Standards and Technology, *'The NIST Definition of Cloud Computing'* (2011) National Institute of Standards and Technology, Special Publication 800-145

RAND Europe, '*Understanding the Security, Privacy and Trust Challenges*' (Technical Report, 2011)

Legislation and other authoritative sources

Case C-202/88, *France v. Commission*, [1991] ECR I-1223

Case C-275/06, *Promusicae v. Telefonica* [2008] ECR I-271

Case C-324/09, *L'Oréal SA v eBay International AG* [2011] ECR I-0000

C-236/08 to C-238/08, *Google France and Google Joined Cases* [2010] ECR I-0000; [2010] ETMR 30

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 on the free movement of such data, OJ L 281, 23.11.1995

Directive 97/66/EC of the European parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217, 5.8.1998

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), O. J. L 178, 17.07.2000

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.4.2002

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 (Directive on privacy and electronic communications), O.J. L 201, 31.7.2002

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337, 18.12.2009

European Union, Consolidated versions of the Treaty on European Union and of the Treaty Establishing the European Community European Union 29.12.2003

Malaysian Communications and Multimedia Commission Act 1998

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data, 25.01.2012

United Nations Convention against Transnational Organized Crime adopted by General Assembly resolution 55/25 of 15 November 2000

US Stored Communications Act 1986

World Trade Organization, General Agreement on Trade in Services

World Trade Organization, Negotiating group on basic telecommunications

Websites

Ashford, W., *'EC publishes proposed data protection reforms'* (25 January 2012) <http://www.computerweekly.com/news/2240114326/EC-proposes-a-comprehensive-reform-of-data-protection-rules> accessed 30 January 2012

BBC News, *'EU data protection law proposals include large fines'* (25 January 2012) <http://www.bbc.co.uk/news/technology-16722229> accessed 30 January 2012

Calderone, C., *'Up In the Cloud and Risk from the Other Guy's mistakes'* (19 January 2011) Data Retention and Electronic Discovery Law http://www.dredlaw.com/2011/01/up-in-cloud-and-risk-from-other-guys.html accessed 9 February 2012

Davenport, C., Reuters, *'Breach of new EU online data rules to carry high fines'* (25 January 2012) <http://www.reuters.com/article/2012/01/25/us-eu-dataprivacy-idUSTRE80O0X220120125> accessed 30 January 2012

Dowling, L., *'BT says cloud gaming "just the start"'* (22 September 2011) <http://www.totaltele.com/view.aspx?ID=467896> accessed 7 January 2011

EurActiv, InfoSociety, *'Reding unveils new EU data protection rules'* (25 January 2012) <http://www.euractiv.com/infosociety/reding-unveils-new-eu-data-protection-rules-news-510381> accessed 6 February 2012

Europa, Gateway to the European Union <http://europa.eu/pol/infso/index_en.htm> accessed 7 January

European Commission, EU Justice Commissioner Viviane Reding, *'Data protection: strengthening your online rights'* (25 January 2012) <http://ec.europa.eu/unitedkingdom/press/frontpage/2012/12_07_en.htm> accessed 30 January 2012

European Commission, Summaries of EU legislation, Information Society <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm#amendingact>

Europe's Information Society Thematic Portal:

<http://ec.europa.eu/information_society/policy/ecomm/index_en.htm>

<http://ec.europa.eu/information_society/policy/ecomm/eu-rules/index_en.htm>

<http://ec.europa.eu/information_society/activities/roaming/regulation/archives/current_rules/index_en.htm>

<http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm>

<http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/eu_consultation_procedures/index_en.htm>

Global Telecoms Business, *'BT offers Ribbit cloud phone service'* (3 November 2009) <http://www.globaltelecomsbusiness.com/Article/2330030/Sectors/25197/BT-offers-Ribbit-cloud-phone-service.html?Type=Channel&ArticleID=2330030&ID=25197> accessed 7 January 2012

Kirilov, K., Cloud Tweaks, *'Cloud Computing Market Will Top $241 Billion in 2020'* (26 April 2011) <http://www.cloudtweaks.com/2011/04/cloud-computing-market-will-top-241-billion-in-2020/> accessed 10 January 2012

Microsoft Europe, Microsoft Online Knowledge Center: Could Knowledge Center <http://www.microsoft.eu/cloud-computing/cloudknowledgecentre.aspx> accessed 18 December 2011

Microsoft News Center, *'Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud'* (20 January 2010) <http://www.microsoft.com/presspass/press/2010/jan10/1-20brookingspr.mspx> accessed 6 February 2012

Search Security, TechTarget, *'E-mail spoofing'* (last updated July 2002) <http://searchsecurity.techtarget.com/definition/email-spoofing> accessed 23 January 2012

Telefonica, *'Cloud Computing isn't just a buzzword'* (19 May 2011) <http://www.publicpolicy.telefonica.com/blogs/blog/2011/05/19/cloud-computing-isn%E2%80%99t-just-a-buzzword-2/> accessed 7 January 2012

Trans-European Research and Education Networking Association (TERENA), TF-Storage conference (27 May 2011) <http://www.terena.org/news/fullstory.php?news_id=2903> accessed 18 December 2011

The ICT Regulation Toolkit, Practice Notice, *'India's Communications Convergence Bill'* (last updated 2 February 2012) <http://www.ictregulationtoolkit.org/en/PracticeNote.1222.html> accessed 10 January 2012

Wikipedia, VoIP <http://en.wikipedia.org/wiki/Voice_over_IP>

Wozniak, V., *"Proposed online privacy rules are a 'missed opportunity'"* (25 January 2012) <http://www.thelawyer.com/proposed-online-privacy-rules-are-a-missed-opportunity/1011080.article> accessed 30 January 2012

Blogs and online magazines

Abubakr, T. TechRepublic, *'Navigating the cloud computing legal minefield'* (5 December 2011) <http://www.techrepublic.com/blog/datacenter/navigating-the-cloud-computing-legal-minefield/5142?tag=nl.e101> accessed 19 January 2012

CCR Magazine, *'Telcos' data breach notification amendment is passed'* (6 November 2009) <http://www.ccrmagazine.com/index.php?option=com_content&task=view&id=2123> accessed 9 February 2012

Cloud Computing Software Blog, Cloud Computing Software, *'Hackers Feast on Cloud Computing – Vulnerability of Cloud Computing'* (27 August 2011) <http://www.cloudcamb.org/software/hackers-feast-on-cloud-computing-vulnerability-of-cloud-computing> accessed 9 February 2012

European Commission, Vice-President of the European Commission Neelie Kroes blog, 'Cloud Computing and Data protection reform' (2012) <http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection/> accessed 30 January 2012

Massey, R. and others, National Law Review, *'Proposals for Reform of the Data Protection Regime and Binding Corporate Rules'* (31 January 2012) <http://www.natlawreview.com/article/proposals-reform-data-protection-regime-and-binding-corporate-rules> accessed 6 February 2012

Plummer, D., *'Experts Define Cloud Computing: Can we get a Little Definition in our definitions'* (Gartner Blog Network, 27 January 2009) <http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/> accessed 7 January 2012

Reguligence Weblog, *'Sony PSN: Clueless And Breaching'* (30 April 2011) <http://reguligence.biz/tag/2009136ec/> accessed 9 February 2012

SNVLabs blog available at <http://blog.svnlabs.com/saas-built-using-a-paas-google-app-engine-and-using-iaas-amazon-ec2/> accessed 7 January 2012

Personal Correspondence

E-mail from David Callahan, Deputy Head of Unit, Software & Service Architectures and Infrastructures, European Commission DG INFSO to author (22 November 2011)

E-mail from Erik Mark Meershoek, senior consultant at Verdonck, Klooster & Associates to author (30 January 2012)

E-mail from Radu Epure, UNIX Administrator at Gameloft to author (20 December 2011)

Interviews

Blair, G. and others. *'Perspectives on cloud computing: interviews with five leading scientists from the cloud community'* (2011) J Internet Serv Appl <http://www.choreos.eu/bin/download/Download/UsefulResources/CHOReOS-InternetOfServices-Paper-June11.pdf> accessed 19 January 2012

Verstraete, J., *'Cloud computing critical to Digital Agenda's success'*, Deutsche Welle radio interview by Teri Schulz (8 September 2010) <http://www.microsoft.eu/digital-policy/posts/cloud-computing-critical-to-digital-agendas-success.aspx> accessed 18 December 2011

Miscellaneous

European Commission, *'How does the data protection reform strengthen citizens'* rights?' <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf> accessed 6 February 2012

European Commission, Press release, *'Digital Agenda: Commission presses 16 Member States to implement new EU telecoms rules'* (24 November 2011) IP/11/1429

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1429&format=HTML&aged=0&language=EN&guiLanguage=en> accessed 7 January 2012

European Commission, Vice-President of the European Commission, EU Justice Commissioner Viviane Reding, *'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age'* (22 January 2012) SPEECH/12/26 available at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26> accessed 30 January 2012

European Commission, Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes, *'Towards a European Cloud Computing Strategy'* (27 January 2011) SPEECH/11/50 available at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50> accessed 7 January 2012

Smith, B., General Counsel, Microsoft Corporation, *'Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing'* (20 January 2010) Speech available at <http://blog.seattlepi.com/microsoft/files/library/20100120smithspeech.pdf>

Telefonica, Public Consultation on Cloud Computing (30 August 2011) available at <http://www.publicpolicy.telefonica.com/blogs/wp-content/uploads/2011/01/Respuesta_consulta_Cloud_Computing.pdf> accessed 7 January 2012