ETAG

European Technology Assessment Group
ITAS · DBT · FCRI · ISI· IST ·ITA ·TC · Rathenau

Impacts of Cloud Computing

Report

Deliverable No.3 of the STOA Project
"Potential and Impacts of Cloud Computing Services and Social Network Sites"

Commissioned by STOA and carried out by ETAG

Order Form No. IP/A/STOA/FWC/2008-096/LOT4/C1/SC11

Ref.: Framework Contract No. IP/A/STOA/FWC/2008-096/LOT4

Paper prepared by

Dr Timo Leimbach (Fraunhofer ISI)
Mr Dara Hallinan (Fraunhofer ISI)
Dr Arnd Weber (ITAS)
Mrs. Maggie Jaglo (ITAS)
Dr Leonhard Hennen (ITAS)
Dr Michael Nentwich (ITA)
Mr Stefan Strauß (ITA)
Mr Rasmus Øjvind Nielsen (DBT)
Dr Theo Lynn (DCU/IC4)
Mr Graham Hunt (DCU/IC4)

July 2013

European Technology Assessment Group

- Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe
- Danish Board of Technology (DBT), Copenhagen
- Catalan Foundation for Research and Innovation (FCRI), Barcelona
- Fraunhofer Institute for Systems and Innovation Research (ISI), Karlsruhe
- Institute Society Technology (IST), Brussels
- Institute of Technology Assessment (ITA), Vienna
- Rathenau Institute, The Hague
- Technology Centre AS CR, Prague

Contact:
Dr Leonhard Hennen (Co-ordinator)
Institute for Technology Assessment and Systems Analysis; Karlsruhe Institute of Technology
c/o Helmholtz-Gemeinschaft
Ahrstr. 45, D-53175 Bonn
Leonhard.Hennen@kit.edu

Project Description

Contract number IP/A/STOA/FWC/2008-96/LOT4/C1/SC11

The project is being carried out by the
Fraunhofer Institute for Systems and Innovation Research (ISI), Karlsruhe
(project co-ordinator);
together with the Institute of Technology Assessment (ITA), Vienna; the Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe; and the Danish Board of Technology (DBT), Copenhagen, as members of ETAG.

Project Leader: *Timo Leimbach, Fraunhofer ISI*

Authors:

Dr Timo Leimbach (Fraunhofer ISI)
Mr Dara Hallinan (Fraunhofer ISI)
Dr Arnd Weber (ITAS)
Mrs. Maggie Jaglo (ITAS)
Mr Rasmus Øjvind Nielsen (DBT)
Dr Theo Lynn (DCU/IC4)
Mr Graham Hunt (DCU/IC4)

Members of the European Parliament in charge:

Mrs Silvia-Adriana Ticau

Mr Malcom Harbour

STOA staff in charge:

Mr Peter Ide-Kostic

Submission date:

July 31st, 2013

CONTENTS

EXECUTIVE SUMMARY

This report focuses on the impacts of Cloud Computing and the resulting challenges. It is based on an evaluation of the available scientific and industry literature, as well as on expert interviews. It should be mentioned that statements regarding Cloud Computing in reports and media on this are often contradictory. One reason for this is that various definitions are used. Some authors apply "cloud washing" and rename traditional outsourcing or web services. Based on the previous deliverable we focus on common used definitions such as the one from NIST. A second issue is that statements often are based on experts estimation due to lack of reliable time series of data. This explains the great bandwidth of results, which have to be taken with care.

Socio-economic impacts

In the chapter on socio-economic Impacts we present some typical cases of such Cloud Computing, e.g. elastic hosting services by Amazon and Google. We observed that there are several such companies, mostly US-based, which earned revenues between a few hundred million and about US-$ 2 billion, in 2012. Positive impacts which we observed comprise:

- Cost savings of services of, e.g., 10-20%.
- Convenience of using services, e.g. by private consumers, but also by employees and small companies.
- Flexibility, e.g. for hosting a mobile app.
- Professional security management, relevant for consumers or SMEs.

But at the same time there are costs and risks, e.g.:

- Loss of control over data, loss of confidentiality, and a potential loss of availability.
- For consumers, costs of mobile roaming, costs of backups in the cloud, etc.
- Need to control using the Cloud, e.g. dealing with contracts, deletion, and migration.

We also observed limits to Cloud Computing. For example, for certain operations, such as in telecommunications or manufacturing control, latency requirements are so high that using remote servers does not appear to be an option. Also, many large corporations already use outsourcing and/or internal load balancing and therefore cannot reap additional benefits. Accordingly, we observed no large layoffs, due to migrating computing services into the cloud. It has been anticipated that using Cloud Computing will lead to general savings of 10% - 30% of IT costs. However, it has not been possible to identify empirical studies supporting this. Consequently the significant productivity growth, as estimated by some authors based on this, have to be taken with care. However, this may change in future.

Currently, there is a widespread fear that Cloud Computing providers and foreign governments abuse data, that providers go out of business, or suffer from severe outages.

The effects of the US Patriot Act, the Foreign Intelligence Surveillance Act, and the National Security Letters have been widely discussed in the media. If problems with confidentiality, availability and migration of data could be overcome, however, Cloud Computing would have a much brighter future. Also, the low entry prices of Cloud providers mean that new businesses can easily enter the market and scale their operations. Both effects can influence the future growth of productivity and jobs and therefore justify supportive policy actions today.

Regarding the impacts on the IT markets and the IT industry itself it can be stated that Cloud is fast growing segment and will gain of importance in the future. However it might also be that within some years Cloud as segment will merge into new or other market segments, but the underlying technology and models will remain as a part of the future IT landscape. While markets will change, the structure of the industry will not change significantly as it seems now, i.e. the dominance of US based providers will continue. But European policy makers could use their power to support the emergence of providers which provide perfect confidentiality and availability, which could lead at least to rebalance of the industry structure.

The analysis of socio-economic impacts shows that there are many positive expectations associated with Cloud Computing. This should be taken with care because they are often based on optimistic estimation on productivity gains. These would require that all obstacles are removed as well as the cost savings can be fully realized. Moreover further research shows that it requires specific framework conditions like education to turn productivity gains and growth also into growth of employment and not the other way around.

Achieving both, changing the structure of the industry as well as to realize to potentials of Cloud Computing for Europe need to address barriers and challenges researched in the following.

Relevance of privacy and security

Security, privacy and data protection remain key concerns with regard to Cloud Computing. However, the ability to act on such concerns is very low for individual users and SMEs, who make up the largest potential user groups. Citizens in general remain unaware of the deeper security implications of adopting cloud services, while many SMEs lack the capacity to carry out proper risk assessments. Both groups are in a very uneven position against cloud providers with regard to knowledge and means for influencing the relation. Large companies and governments demanding greater transparency and more useful contractual arrangements from cloud providers may in some degree act as trail-blazers for the development of societal acceptable relations between cloud providers and users. But self-regulation on the part of industry, such as security standardization, contract standardization and assurance mechanisms, has of yet not been able to deliver an overall image of transparency and trustworthiness. And independent security experts still have substantial concerns with regard to security in the cloud. Societal-level interventions to establish mechanisms for reliability and trustworthiness in the cloud industry in general

therefore seem to be needed to harvest the overall societal benefits, which the cloud could provide to a society that could trust it.

Data security

In Chapter 3, key security and privacy issues are discussed. The most important security issue appears to be confidentiality. Currently, no cloud services are available which prevent insiders or governments from reading data. Technical solutions would most likely have to rely on large, mass-manufactured tamper resistant devices using tamper-detecting membranes, or on new cryptographic algorithms. While the latter is a research topic with open outcome, the former could be explored in a study, in order to estimate its costs. Another important security issue concerns the availability of the Internet. Servers may not be accessible in case of denial of service attacks or misrouted Internet traffic. As rare as such instances are, their sheer possibility makes it clear that using several providers in parallel, with easy migration, or local backup procedures, is advisable for critical computations.

A third issue are attacks on the servers, or clients, e.g. by malware. As identified in the STOA project on eGovernment security, Europe would benefit from having a reliable, proven computing base, without any scope for zero-day exploits or Trojan horses. Only this way a solid base for future computing can be achieved. This is similar to the US DARPA Crash program. Based on this, high quality applications could be used.

Cloud computing, privacy and the EU data protection regime

Cloud computing is a development in data processing which opens up a range of economic and social possibilities. However, as with many developments in data processing, it also brings with it the potential to infringe on individual rights. Data protection law is the most significant European legal regime aimed at safeguarding individual rights in the processing of data. It is currently elaborated by Directive 95/46. However, law often reflects the context in which it was drafted. Technological developments – for example cloud computing – can serve to change this context, and accordingly ask questions about the continuing functionality of the law.

Accordingly, the section analyzes the problems created by the specificities of cloud computing – as a new form of data processing – for data protection law. There are four core problems identified. 1. The problem of jurisdiction and applicability: One of the core features of cloud computing is that the physical location of the data or service is irrelevant. Data protection law, on the other hand, employs criteria in defining its applicability which are inextricably linked with concepts of location. When data processing is difficult to relate to geographical location, these criteria can be very difficult to apply. 2. The problem of defining roles and responsibilities: The data protection framework relies on categorizing entities involved in data processing as specific sorts of actor. Each form of actor then has roles and responsibilities in ensuring that the requirements of the directive are fulfilled. The complexity of processing in cloud environments and the unique arrangements this has required between cloud provider and cloud client, has brought into question the

applicability of the roles and responsibilities imagined by the Directive. 3. The problem of worldwide and continuous data transfer: Cloud computing service provision can utilise service providers, and be called up by service users, located outside the EU. In order to ensure that EU citizens' data is protected regardless of where they are processed, the Directive puts certain restrictions on the transfer and processing of data outside the EU. Whilst there are exceptions to these restrictions, the cloud computing scenarios in which these exceptions can be applied are limited. This can needlessly prevent the provision of cloud services. 4. The lack of a binding European interpretation mechanism: The above issues remained problematic, as the Directive provided no mechanisms to adapt to them. This was attributable (at least partly) to the fact that the mechanisms designed to interpret the Directive had no binding power at European level.

Beginning in 2010, the EU began a process of data protection reform. Recognition of the unsuitability of Directive 95/46 to cloud computing was one of the driving forces behind this reform. In 2012, this process produced a draft Regulation aimed at replacing the Directive. Whilst there may be changes to the text before the Regulation becomes law, the general framework and approach look likely to remain the same. The section thus proceeds by looking at the significance of the changes made by the Regulation. First, as to how they address the problems identified in relation to the Directive 1. The Regulation offers a clarification and expansion of scope: This is aimed at ensuring the application of data protection law is clear and that EU citizens' data is protected regardless of by whom, or where, it is processed. 2. The Regulation offers a clarification of the distribution of roles and responsibilities: The Regulation moves away from strict definitions of roles, toward a scheme which ensures that the actor best placed to fulfill a controller's obligation, is the party obliged to fulfill that obligation. 3. The Regulation envisages a revamp of the rules allowing international transfers of data: These are aimed at removing the legal obstructions to transborder data flows, whilst maintaining a high level of protection when personal data leaves the EU. 4. The Regulation institutes a number of novel interpretation mechanisms which will allow the Regulation to be bindingly interpreted at European level: These will provide, in advance, mechanisms aimed at allowing the law to be adapted to meet the challenges posed by any further new developments in data processing. Second, the section addresses how the novel features introduced by the Regulation will affect the provision of cloud services. Three innovations seem of particular importance. 1. The right to be forgotten: This will give the data subject the right to have their personal data deleted and will impose the obligation on the data controller to effectively delete the data. 2. The right to data portability: This will give the right to a data subject to obtain their data in transferrable format. 3. Data protection by design and default: This will create the obligation on the data controller to implement data protection principles throughout the life cycle of a cloud service, from design, through deployment and use.

Governance issues related to data retention and enforcement outside the EU

While the difficulty of governing cloud computing arising from the plurality of jurisdictions involved is well-known, over the past year the world has gained insight into trans-legal (if not illegal) practices of 3rd party access to data for the purposes of data mining by both private actors and government agencies. This has shown that cloud governance is not only

about legal frameworks, but also about their enforceability. With the proposed European data protection regulation, the European Commission has taken one step towards a more unilateral approach to upholding European standards of data security and privacy in a globalized economy.

This approach has both benefits and drawbacks. On the one hand, more active means of enforcement become available to Europe while providers under the proposed Regulation will be forced to provide greater transparency. As such, the proposed legislation relies less on trust in individual actors than previous frameworks. On the other hand, with this approach Europe moves one step closer to the strong-arm style of diplomacy, which have otherwise been associated with other major world powers. Maintaining this course may well lead to ripples in the EU-US relationship.

As Europe debates its data protection approach, it is important to ask difficult questions about the relationship between vested interests and viewpoints being put forth in the debate. European citizens, SME cloud users and government agencies are all at a disadvantage in negotiating terms of service and security practices with major cloud providers. They may need the strong leadership of Europe. Such leadership may additionally help further home-grown European providers of primary cloud services. It might, however, also stifle the growth of secondary providers of cloud-services. Striking the necessary balance between these concerns is no simple matter. To achieve it, is advisable to scrutinize closely the viewpoints in the debate with regard to which interest they serve, to beware of exclusively trust-based solutions to cloud governance issues, and to look further into ways of promotion cloud architectures designed from the beginning for security and privacy.

Contractual issues

While the discussion of data protection and data retention attracts much attention, there are other contractual issues that also impact the adoption of cloud computing, in particular in business. Typically, the contractual relationship between service providers and their clients is laid out in one or more documents typically comprising commonly the following one: Terms of Service ("TOS"); Service Level Agreement ("SLA"); Acceptable Use Policy ("AUP"), and Privacy Policy. Each of them serves specific purposes and clarifies different issues. The analysis tried to cover the main features including the choice of law, data location (including transfers outside of the EU), Policies for data integrity, availability and security, liability, acceptable user requirements, monitoring and service levels, backup, termination and a few smaller aspects. Beside a description of these contractual features also their consequences are discussed. Similar to the overall situation of Cloud Computing this analysis shows that the related legal framework for the provision of cloud services is complex, fragmented and at early stage of conceptualization due to the multi-tenant nature, the underlying chain of service provision (and the consecutive nexus of contracts) and the reliance on the Internet. This requires that intervention, if even possible, needs to be taken with care. In the current situation the framework mostly favors the cloud service provider, which is shown in many of the following points.

First of all, the choice of law and thereby the applicability of EU law is of one important concern, because it provides a greater legal certainty. It is of relevance in particular in the relations to non-EU providers, which often stipulate US law into cloud service contracts disproportionately impacting exclusions and limitations on liability, and indemnifications. Though many of these issues for consumers are addressed by the current draft regulation on data protection, the situation in business differs and need to be addressed in many ways. This goes along with the usage of a language that may not be feasible for clients to meet in the Acceptable Use Policies. Especially the end users are often affected by this, which needs to be addressed by standardizations and simplifications. Regarding the IP issues the analysis showed that there is degree of incompatibility between the current IP frameworks, which are based on geographic location, and the locally independent cloud computing. It refers to many cases such as the user's development of applications utilizing tools of the Cloud provider or the question of ownership in customization and bug fixes. This may refers to a general set of issues in the current IP scheme and raises the questions if and how these issues should be addressed.

In particular the formulation of the AUP also refers to another broad set of contractual issues, which all can result in a lack of trust in Cloud services. This could form one further barrier for the adoption of Cloud. One major reason is the lack of transparency regarding security of data, performance levels and metrics, audit rights, use of metadata, the identity of data processors and subcontractors along the chain of service provision and indeed the location of data in storage, in transit and while being processed. Other major aspects for a possible use of Cloud by consumer and businesses are the perceived redundancy and resilience provided by Cloud offers. Consequently the uncertainty regarding backup policy and the security arrangements, which are often not disclosed, creates further intransparency. In this regard consumer and businesses can only rely on third party certification of security and IT governance policies used by Cloud providers. But the currently most used information system assurance and related trust marks are criticized because of many reasons, including for example limited scope, passive, periodic and retrospective character, or lack of warranties. Consequently there is the need for new trust marks in the cloud computing context, which could have as research suggests positive impacts on the perceived trustworthiness, including influencing respondents' beliefs about security and privacy, general beliefs about firm trustworthiness, and willingness to provide personal information.

Finally there is the issue of the location of data in storage, transit and processing, which was identified as one major concern. One main reason behind this concern is the question of uncertainty regarding the provision of access to third parties, i.e. law enforcement agencies. Though the data retention directive should clarify this at least on the EU level, there are strong differences within the member states. Even more concerns exist regarding the treatment of that in the US, where it is often not possible to know if the data was accessed. Together with the lack of transparency all this increases concerns, so that the underlying issues need to be addressed.

Competitiveness of the markets

The competitiveness of markets is a crucial point for the further development of Cloud Computing in Europe for both, users as well as for providers. Given the fact that Cloud Computing is a two-sided market shaped by network effects, the current development bears some risks for the competitiveness. The reason is that there is the tendency that only a few players will establish strong platforms, which create their own closed ecosystems consisting of a strong user base and a broad numbers of further solutions and applications. In this context the first challenge to competiveness is that a platform owner could create barriers that make it hard to migrate easily to offers of other providers, which would create an effective barrier for competition. These barriers have legal aspects like the issue of contract termination, data portability, etc. as well as technical aspects like standards and interoperability. Possibilities to reduce the risks of such behavior are the clarification of rights related to data portability as well as the support for further measures ensuring better standardization and interoperability of platforms.

Due to the fact that many of the currently leading providers are not of European origin, there exists the possibility of creating vivid and competitive market by supporting of a competitive landscape of European providers. The low share of Europe in the worldwide ICT industry, which contradicts its position as the second largest market, is subject of research for a long time. Regarding Cloud Computing there are two major points our analysis has identified and further reviewed. The first one is the fragmentation of the market. It refers to broad set of issues all dealing with challenges to cross-border activities in Europe. As shown by the analysis there are still issues that need to addressed to enforce the creation of a single market for digital services. This includes further reviews of the eCommerce regulations like the case of VAT systems for Cloud services as well as further harmonization of the regulatory framework like in the cases of consumer rights and data protection. Though there many initiatives on going related to these points, some issues that are important in particular from the point of view of Cloud Computing still need to be addressed. The second point related to vivid landscape of European providers is the lack of fast growing European enterprises becoming global player. As shown by many analyses over the last decade there is set of issues that hinder the creation of such companies. In recent time the lack of entrepreneurial activities and culture as well as the role of the state in this process became focus of the discussion. The latter point relates in particular to role of the state as procurer (innovative and normal procurement) as well as to the level of public R6D funding. Beside of specific challenges in all of these areas, the lack of coordinated strategies combining funding and procurement is an issue that needs to be addressed. The first two points refer to low level new business creation and innovation as well as to the lack of venture capital and a related culture supporting both. While there are many activities to increase the level of Venture Capital or stipulate founding activities, which need to be continued like the creation of single European market for venture capital, there is also some point in the question why it did not succeed until now. Some analysis indicate that similar to the lack of a coordinated approach for R&D funding and procurement also a lack of stimulation for a true venture culture. This is an issue that should be explored and if possible addressed.

Finally there are two issues, the provisioning of infrastructure and the creation of human capital, which might not directly impact competitiveness. Nevertheless, in a long term perspective both will have a strong impact on the competitiveness due to their character as framework conditions for it. Skilled personnel are fundamental for both, provider of Cloud services as well as their users. Especially the ability of users to exploit the potentials of Cloud and related other emerging technologies like Big Data is fundamental to realize the positive societal and economic benefits of it. Based on the already existing lack of skilled workforce, the further development of the human capital base will strongly impact the competitiveness of Europe in Cloud Computing. The availability of network infrastructure, mobile as well as fixed connections, will play a similar role in the future development. The reason is that Cloud Computing will enable more and more digital business, which will lead to a strong increase in the demand of network. Consequently, it is necessary to develop network infrastructures in a way that enables the realization of the potentials of Cloud Computing. Questions arising from it are the differences in the development between the different regions in Europe, the further need for more advanced network infrastructures and how these should be financed in a fair balance for all relevant stakeholders.

Conclusions and policy options

Concluding it can be stated that the report shows the potentials of Cloud Computing for Europe. But like most developments in IT the story also has two sides. There is also the risk that these impacts cannot be realised or even worse turn into the other direction, if it is not possible to provide sufficient environment for the uptake of Cloud Computing.

This led directly to the analysis of barriers and issues, but already the discussion of the direct impacts as well as overall impacts on economy and society indicate first issues that need to be addressed. The following analysis of challenges and issues also detailed this analysis. In a first set all issues related to data security, the current data protection regime in the EU and it ongoing changes and data retention and enforcement of EU law outside of the EU were addressed. The results show that there are many options ranging from technical development of trusted Cloud platforms or certification schemes up to new approaches like privacy by design or measures as increased cooperation of DPA and international collaboration that can be considered to address the needs of the different stakeholders. While these issues are of relevance of all users of Cloud Computing, the second set is more aimed at two specific points. The first part is directed at the contractual relationships between user and provider. While for consumers many of the issues are addressed with the new draft regulation on data protection, business users in particular need to deal with further points such as IP rights or service and quality levels. The analysis shows a clear need to strengthen the rights of users for example by the standardisation of contracts, certification process or trust marks. Another point is the competitiveness of the market, which addresses issues for the creation of a competitive European Cloud market. Consequently issues addresses partly users as well as providers like standards, interoperability and vendor lock-in or market fragmentation as well as more aspects important for the long term competitiveness such as broadband coverage or the lack of skilled workforce. Finally also specific issues for the competitiveness of European providers are analysed. Due to this broad focus the identified options vary from support of data

portability rules and interoperability up to industry policy like for example the use of pre-commercial procurement and infrastructure provision for future network requirements. Overall this leads to broad list of policy options, in total nearly 60, which can help to improve the current state of Cloud Computing in Europe.

It is obvious that due to the strong interrelation of the identified issues some identified options emerge from more than one field. Consequently we consolidated the list of options. In course of this process we also reordered according to the approach of a functional analysis in the framework of a technological innovation system, which was introduced in the initial analysis of the previous deliverable. Within the process we identified five clusters of issues split into the following functionalities:

- provisioning of infrastructures, which addresses the availability of secure and sufficient technical computing and network infrastructures;
- mobilizing resource, which addresses the need for human capital base, i.e. extension of total number as well as enhanced education of developer and user, as well as the need to improve the financial capital situation, i.e. the access to financial capital for innovation and growth;
- legitimation and creation of markets, which addresses the need for acceptance of new technologies such as Cloud as well as the support for the creation of a working and competitive market for Cloud;
- adapting the regulatory environment, which addresses the needs to adjust and harmonize the legal framework, in particular contractual issues and data protection regime, according to the challenges of Cloud Computing;
- encourage entrepreneurship and competition, which addresses the support of entrepreneurial culture and activities as well as a fair competition environment.

The full list with remaining 58 policy options can be found in section 5.2.

Outlook

The aim of the following final phase is to produce a high quality final report that will be considered useful by European decision-makers. Based on this aim the work of the final phase is split up into two main tasks. The first one is the compilation and consolidation of the results of the previous phases. This includes an internal review, the integration of the results of the extra module on social networks sites as well as the integration of additional inputs made by the MEP's, the STOA secretary or received during the policy workshop. The second task is to take up the policy options identified here as well as further inputs from the policy workshop, presentation and further consultations with experts to derive a set of final policy recommendations for European-decision makers. This includes internal reviews, prioritization and validation of possible options and will result in a concrete set of measures that can be undertaken to foster the potentials of Cloud Computing in Europe.

1. INTRODUCTION

1.1. Aims of the report

Many of the controversial discussions on Cloud Computing focus on its possible impacts and related challenges of Cloud Computing. But a short review of them reveals easily that many of the different views on the impacts are caused by different understandings what Cloud Computing is. One general problem is the practice of "cloud washing", meaning that many companies rename services already offered before to the name "cloud" (Colt 2011, 10), which often leads into uncertainties. Consequently, we want to clarify our understanding of Cloud Computing as laid down in the deliverable on the "Foundations of Cloud Computing". It shows that the definition of Cloud Computing is an ongoing process driven by different actors with varying interest. Consequently we decided to focus on the current definition by NIST, which state that Cloud Computing is *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* (Mell/Grance 2011, 2). Additionally the review of service, distribution, revenue and business models showed similar problems. In particular revenue and business models are still in flux and cannot be used for a further, more distinctive classification. Based on this the project focuses on public and with some limitations hybrid Cloud offerings offering services such as IaaS, PaaS, SaaS and some of their variations. In reverse it implies that private Cloud offering, which is technical continuation of previous virtualisation efforts and traditional IT-Outsourcing are excluded, but that the boundaries between this can be sometimes blurry. It also means that other services like social network sites or the streaming of video or music are not in the focus, because these services either use different technologies and/or existed in some cases before the term "Cloud" was coined. Both points are also reasons to exclude all kinds of traditional eCommerce services such as online retailing, online booking or similar, though there are nowadays often based on Cloud infrastructures (Leimbach et al. 2013, 7-21).

Based on this focus setting one aim of this deliverable is to review the existing literature in order to identify and analyse socio-economic impacts related to Cloud Computing. This includes direct impacts on consumers and business like for example impacts on the productivity or privacy. Above that we will also analyse indirect impacts on the society and economy as a whole. This includes for example impacts on economic growth or job creation as well as societal aspects like sustainability. The second aim of the deliverable is to perform an in-depth analysis of challenges for Cloud Computing like security, privacy or other legal implications. Both, the analysis of impacts as well as of challenges, are based on, but not limited to the results of the initial analysis of drivers and barriers in the previous deliverable, which shows that they are often interrelated. Finally the last aim of the deliverable is to discuss identified policy options, which can help to foster the potentials of Cloud Computing in Europe taking into account business user and consumer needs and expectations

1.2. Structure of the report

Given these aims the deliverable is structured into three main parts. The first part of the report takes up the discussions of possible direct impacts of Cloud Computing, which is closely related to the initial analysis of drivers for for the adoption and usage of it. As a first step the recent scientific and technical literature will be reviewed to see which direct impacts, positive as well as negative one, are associated with Cloud Computing. This includes direct impacts such as security or privacy on business, public services and consumers. This includes also one part on direct impacts like changes of market structure or business models on the IT industry itself. A further analysis is directed at analysing and assessing these direct impacts. In a second step the overall economic and societal impact of Cloud Computing will be discussed based on a review of the current literature on economic effects in terms of job creation and growth as well as a discussion on further societal impacts such as energy savings or improved public services.

The second part of the deliverable is aimed at in-depth analyses of challenges for a further adoption and usage of Cloud Computing in Europe. This part is split into two sections following the initial clustering of challenges in the previous deliverable (Leimbach et al. 2012, 81-85). The first one deals with the challenges related to data security, data protection and privacy as well as data governance, i.e. the challenges related to the location, the transfer and the access to data. All of these points have a high importance for consumers and citizens as well as for business and public administrations. While in many cases this results from the same expectations or needs, it differs and complement each other in other cases. The second sections deals with the challenges of contractual relations like IPR or compliance and challenges for the market competitiveness like technical standards and interoperability. In particular the latter one is mainly of importance for business, but also the first point is often more important for business as for consumers. Although the clustering is mainly based on the results of previous deliverable, each analysis has been supplemented by further desk research and expert interviews. The analysis focuses strongly on the situation in Europe, but given the fact that Cloud Computing is global phenomena we will also take the situation and developments in other regions worldwide, in particular in the US where many of the leading providers are situated, into account as far as possible.

Finally the report will conclude with a comprehensive overview and discussion of policy options. These options were either identified during the review of existing documents or result directly from the analysis of the different challenges and impacts. This task will serve as an input for the following final phase of the report dedicated to recommend different policy actions.

2. SOCIO-ECONOMIC IMPACTS OF CLOUD COMPUTING

2.1. Introduction

This first part of this deliverable deals with the socio-economic impacts of Cloud Computing that will be analysed based on review and examination of existing literature on it. In a first step the direct impacts of Cloud Computing, in particular on consumers and businesses, will be identified and analysed. This is based on the initial analysis of obstacles and drivers in Deliverable 2, but has been complemented and extended based on the literature, interviews and further case studies. It also includes an appraisal of impacts on the IT industry itself. This is followed in a second step by an analysis of the impacts on economy and society as a whole. This is mainly based on a review of the current literature on economic effects in terms of job creation and growth as well as a discussion on further societal impacts such as energy savings or improved public services.

In the remainder of this section we describe some cases of public Cloud Computing services which are typical, according to the literature. There are only few independent case studies available which describe the costs and benefits for the various parties involved, e.g. for the Cloud Computing provider, for the customer and, if applicable, for the private or business end user. An often mentioned case is that of email, which is therefore mentioned below. Other cases describe the benefits of running scalable applications remotely. These brief case studies are presented in order to shed some light on how use cases of Cloud Computing look like which have impacts as described further below.

Nuremberg Airport Customer Information	
Customer	Nuremberg Airport
Application	The airport uses AWS Elastic Cloud Computing, Elastic Load Balancing, Simple Storage Service and CloudFront for handling their web hosting. The access to the homepage through passengers depends very much on season, disruptions etc. and therefore creates peaks, which can be handled with AWS cheaply.
Benefit for customer	Low cost: The airport saved 60-70% of IT costs through the use of AWS while having high availability in case of peaks.
Reference	Leclerque 2012

Zotero Literature Service	
Customer	Zotero
Application	Zotero is a free to use service to organise research and literature. It is available offline and online with the option to synchronisation. It offers collaboration, offline and online access and storage. It uses the AWS Simple Storage Service.
Benefit for customer	The service is free to use and free of advertisements. It is funded by the United States Institute of Museum and Library Services, the Andrew W. Mellon Foundation, and the Alfred P. Sloan Foundation.
References	Zotero 2013

Viadee Bar Ordering App	
Customer	Viadee
Application	"Bestellbar": free mobile app for ordering in restaurants. The app is used by a few restaurants in Münster, Germany. The company uses the Google App Engine.
Benefit for customer	The App Engine is cheaper than buying hardware, elastic and fast to implement.
References	Interview with company representative.

University Mail Services	
Customer	Many universities, especially in the US.
Application	Use of GMail and Drive.
Benefit for customer	Cheaper to use than to operate an e-mail system of their own; wider arrange of services (like calendar or Google Drive) and more storage available.
References	Wimmer 2011

2.2. Impacts on business user

Here we focus on the general use of Cloud Computing by businesses, including all size of firms and different branches of business. The reviewed literature provides many insights and expected impacts. The estimated numbers regarding some impacts such as cost and revenues vary between the different studies. We will comment on these findings and assess their accuracy.

2.2.1. Positive impacts

Real Impacts

Cost savings

The starting costs for using a cloud service are low, compared to running one's own servers. This is especially important for start-up companies who don't have the necessary capital, but are in need of one or several servers. It has been difficult to access reliable numbers for those cost savings; the case studies above indicate the nature of some savings. Bradshaw et al. (2012) conducted an online survey with 1056 selected businesses and found that 78% saw cost savings compared to traditional IT services, the average cost savings being between 10% - 19% (Bradshaw et al. 2012, 22).

Flexibility

Businesses can experiment with and implement new services faster than through traditional IT (Fielder/Brown 2012, 36). Through Cloud Computing services can be implemented faster because there is no time needed to deal with computer hardware and the starting costs are low (Ecorys 2009, 63). For example: If a program developer is hosting an app and needs more computing power than s/he has at hand at the moment, it is easier, faster and cheaper to rent computing power via a cloud service than buying the needed servers (Meyer et al. 2012).

Scalability

The factor scalability is related to flexibility, but focuses on the demand for computing power. Through cloud services like, e.g. Amazon S3 (Scalable Storage Service) it is easy to adapt the computing power to what is really needed. This is much faster and cheaper than building up a data centre (Meyer et al. 2012, 4). An example is the video hosting service "Vimeo": If a video is downloaded very often, or if many videos are uploaded, the computing capacity can be increased easily and cheaply (Venkataraman/McArthur 2011). So a startup may start with limited capacity, but can increase capacity very easily and cheaply. If such a company had their own servers, they might have costs for overcapacity, and at the same time might not be able to match demand if it suddenly increases.

Professional Security

Cloud providers can offer higher security for data than businesses without the necessary IT know-how. Thinking of very small medium sized companies, one can observe that some medium sized ones today have a very professional administration regarding, e.g. attacks and backups. Some, however, do not, and regarding very small ones, certainly IT-security is not one of their core competencies. In other words, SMEs without the highest level of IT-management may benefit from professional management in the cloud. Also data can be stored in more than one location and not only in the company itself (Fielder/Brown 2012, 48). This is not to deny that they will then have to deal with issues of transmission security, trust in the Cloud Computing service provider, and the possibility of insiders eavesdropping there.

Estimated Impacts

Cost Savings

This is the most often mentioned impact that Cloud Computing has or is going to have on businesses. Also governments, e.g. local and regional ones, could possibly create significant savings if they use certain specific applications, centrally provided in the Cloud only.

IDC did several studies on behalf of the EC, and we quote the final report by Bradshaw et al. (2012) as well an early, partially more detailed version (Cattaneo et al. 2012). The authors conducted an online survey with 1056 selected businesses and found that 78% saw cost savings compared to traditional IT services, the average cost savings being between 10% - 19%, as briefly mentioned above (Bradshaw et al. 2012, 22). The authors use a very broad and somewhat unclear definition of Cloud Computing services as "consumer and business IT products, services, and solutions delivered and consumed in real time over the Internet" and they only focus on public clouds (Bradshaw et al. 2012, 9). They name services like Gmail, Salesforce, Microsoft Azure or Amazon Web Services. These cost savings are not explained by the respondents in any detail , e.g. what cloud services have been used to reduce costs (Cattaneo et al. 2012, 28). It can be assumed, however, that the mentioned cost savings of 10% – 19% derive from services like Gmail or Salesforce, otherwise we would have heard of significantly shrinking IT-departments and IT-service provider staff. The questionnaire appears to be unavailable, but the studies mention that respondents were given exactly such examples. So it appears that those examples were

given (Cattaneo et al. 20), then respondents were asked whether they use it, and then they were asked for cost savings. It can't be said with certainty that from this cost savings arise *in general* in such an amount. There is no evidence that 64% of companies saved between 10% or 20% or 30% percent on their entire IT spendings. Against this this background it is unclear what the real cost savings from Cloud Computing are, i.e. the ratio of saved IT-costs to total IT-costs.

Hogan et al. (2010) differentiate between three methods of cost savings. They base their findings on proprietary research provided by EMC, but do not describe their methods and findings it in detail. The authors differentiate between (1) IT capital expenditure: servers and computers. Overall 40% can be saved in public clouds, they write. (2) IT labour costs: 31% can be saved in public clouds. 3. IT power and cooling costs. 80% can be saved in public clouds (Hogan et al. 2010, 33).

The majority of companies still manage their data on premise or in traditional outsourcing to a nearby data centre. We have not been able to spot any reports according to which IT departments actually shrank by 10% or 20%, the figures provided by IDC, or 30% or 40%, as provided by Hogan et al. Therefore we suggest treating those figures with care. In 2011, the European Commission expected 25% - 50% savings through the adoption of Cloud Computing (European Commission 2011, 1). A year later the Commission is quoting the estimation of cost savings between 10% - 20% (European Commission 2012b, 4), referring to the IDC studies described above. Accordingly, the papers from the European Commission suggest macroeconomic savings of IT-costs between 10% - 30%, apparently based on the same studies. However, there is no clear evidence for such large savings.

Time to Market

The flexibility and scalability of Cloud Computing can reduce the time that products hit the market. The implementation of new services that rely on computing power or storage can be achieved in a shorter time. An example for this is Dropbox, which was able to grow quickly thanks to using Cloud storage services themselves (Woloszynowicz 2011).

Innovation & Creation of Companies

Cloud Computing itself is an innovation that already has given the opportunity to create new services and businesses, not only for specialized markets but also for wider consumer use (cf. Ecorys 2009, 67). Many examples for companies that use Cloud Computing can be found, e.g. Airbnb, Ubisoft and Spotify (Amazon 2013b). Especially start-ups that use cloud technology can be innovative.

2.2.2. Negative impacts

Real Impacts

Loss of Control

If a business transmits data into the cloud, it might lose control over it. In Cloud Computing services the user often is in danger of losing control over his or her data. It is often not clear what legal authority would be in charge and how to pursue a trial if needed. The

assessment of the security of cloud service providers can be difficult for business users due to its complexity (Robinson et al. 2012, 68).

Another factor is that a cloud provider goes out of business and data cannot be accessed anymore (Fielder/Brown 2012, 48). In a study about concerns of businesses surrounding Cloud Computing "loss of control over data" was named by 26% of respondents (Aumasson et al. 2010, 246). They had interviews with over 60 self-selected "experts". The general anxiety of malicious attacks aimed at cloud providers also increases the fear of loss of control (Borgmann et al. 2012, 11). In 2013 there have been attacks on cloud services (not to be addressed here), e.g. on the cloud service "Evernote" which had 50 million users in 2013 world-wide. The service is used for taking notes. User names and passwords were stolen (Vaughan-Nichols 2013).

Summarising one can say that business customers need new competencies to negotiate with a Cloud Computing provider, to control it, to prepare for migration or disasters, etc. Some of these competencies are new, for an SME at least, and some are in the legal realm.

Problems with Availability

It is crucial for businesses that their services are available; otherwise they can lose customers and revenues. This availability consist of two main points.

The first point is the issue of "downtime", which is crucial in particular for business users. Even if the provider offers to make monetary amends for downtime, the amount of money, reputation etc. lost is often bigger than the bonus provided by the cloud service (Borgmann et al. 2012, 51). "Availability concerns" were named by 25% of the companies interviewed (Aumasson et al. 2010, 246). An example is Amazon: Amazon.com itself was down for one hour in January 2013 which caused Amazon a loss in general retail sales of 5,7$ million and also of reputation and customer satisfaction (Wohlsen 2013). Amazon Web Services had several outages in the last years, e.g. in 2012 the TV-on-demand service "Netflix", which heavily relies on AWS, was down on Christmas Eve (Cook 2012). In case of an outage of a large provider, more than one company will be affected. Also, cloud service providers do not necessarily have an infrastructure which automatically ensures the availability of backup resources like processing power or that even ensures immediate access to backups of customer data (Schubert/Jefferey 2012, 11-14).

The other point is the availability of sufficient bandwidth. Although the access to fast internet connections is growing in Europe, it can still be a problem. Broadband access is available in cities but still not in many rural areas. Since businesses not only reside in cities, this can be a problem for Cloud Computing. It is a challenge to deal with bandwidth limitations (Schubert & Jeffery 2012, 11 and p. ii). The limitation of network capacity makes the use of Cloud Computing for some companies impossible, because the amount of data transferred is too big and would take too long, e.g. it would take 45 days to transfer 10 Tbytes from San Francisco to Amazon in Seattle (Hofmann & Woods 2010, 92). Furthermore, Cloud Computing is not suitable for many services which require high speed, such as in banking, telecommunications or control of machines on the shop floor.

Liability / Contract Issues

The questions that arise with the issues of liability and contract issues are crucial for businesses and are quite difficult to handle. Since Cloud Computing providers are often located in different countries both inside and outside the EU, it is difficult to assess liability (Aumasson et al. 2010, 243). At the moment the laws and regulations cover important aspects of how to deal with liability and contracts. Typically contracts are made at the vendors' discretion, except with large customers. This especially weakens SMEs, since they don't have the resources to properly negotiate terms (Bradshaw et al. 2012, 65). A discussion of cloud contracts can be found at Bradshaw et al. 2010. In some contracts the customers are held responsible if something happens to their data which is not in their power but in the power of the vendor. Since the users are still the owners of the data and not the provider, they are held responsible for what happens to the data.

Estimated Impacts

Loss of Revenues

If the costs of business IT were really reduced by, e.g. 20%, many IT-service-providers, computer-vendors etc. would have significant reductions of revenues. If these savings existed, logically cloud customers would spend less on traditional IT-service providers, servers, etc. It has not been possible to identify any study which shows the significance of such a reduction of revenues. Also in the general IT media, no reports of significant revenue reductions with traditional IT-provision have been found. Therefore we conclude that not only are the effects of revenue reduction with traditional providers small, but also the savings which are earned due to using cloud services. Both appear to be marginal, which is in line with the total revenues of Cloud Computing providers mentioned in Section 2.2. Those in turn partially accrue from new types of businesses, such as app hosting.

Loss of Confidentiality

This deals with confidential business data and the handling of customer data abroad. For business users this means that they have or should be concerned if their data is secured in a cloud service. The question arises how well data is protected and what kind of data a business user should put in the cloud or not. This is especially important for customer data for which privacy regulations apply. Business critical data, like business secrets, is also an important issue since it is being put on shared infrastructure. Resource sharing makes a difference because traditionally a company which trusted a service provider was given its own server(s). With Cloud Computing, the infrastructure may be shared with competitors, which might bring in new risks. CIOs are particularly aware of it and are concerned about the US Patriot Act (FI3P 2011, 39). The news about the US "Prism" program on the US government eavesdropping on cloud data justify related worries: „We know the FBI has issued tens of thousands of ultra-secret National Security Letters to collect all sorts of data on people… and has been abusing them to spy on cloud-computer users." (Schneier 2013b). An earlier European Parliament report had investigated the US-dominated ECHELON system and found that "the purpose of the system is to intercept, at the very least, private and commercial communications" (European Parliament 2001, p. 11)

2.2.3. Ambiguous impacts

Increased Competition

The rise of Cloud Computing has increased the competition from outside Europe, for both large companies and SMEs. Through the cheap access to computing power via the cloud, companies from outside the EU "with lower labour costs that may provide cheap and effective standard service solutions in many areas" might enter the market (Ecorys 2009, 11). While this sounds plausible, Ecorys does not provide examples. Ecorys add that many small companies struggle to sell their services and products, especially on markets outside their national boarders, due to a lack of knowledge of how to use new services, without providing details (Ecorys 2009, 11).

2.2.4. Discussion and conclusions

As the case studies indicate, the business cases for Cloud Computing currently are limited, but definitely exist. We thus try to provide a realistic, solid picture of what exists today. Currently, there is a lack of independent empirical studies about cost savings.

Businesses will have to deal with new types of issues, such as keeping control of the whole process, assuring confidentiality and managing legal issues well. This would mean that if trustworthy Cloud Computing providers emerge, the cost savings in the future could be much larger. The European market in particular might become much larger if Cloud Computing customers could easily identify providers which comply with European legislation, and which do not give data to foreign competitors or governments. This in turn would justify the case of suitable certifications. This way Cloud Computing could have a much larger economic significance in the future and a large effect on traditional IT-providers.

2.3. Impacts on private users

Two prominent examples for consumer use are the file hosting service Dropbox and the e-mail and document service Gmail with several million private users worldwide. In December 2012 Dropbox reached 100 million users (Constine 2012). In June 2012 Gmail had 425 million users and 5 million users use Google Drive (Lardinois 2012). Another popular service is Apple's iCloud with 190 million users in October 2012 (Lardinois 2012). Indeed the standard service of web mail is not a new concept and Cloud Computing is more than an e-mail service with a simple web interface. Gmail offers not only a mail account but is also connected to Google Drive. Google drive offers the editing of files and the creating of new files stored in Google Drive. The Apple service iCloud offers the online synchronization of devices and the storage of files.

2.3.1. Positive impacts

Convenience

Data can be accessed from everywhere and on every internet-enabled device. This can significantly reduce problems with missing backups or files. A related aspect is the synchronisation of data, which can be automated (Kraus 2012, 9). Many applications may not need to be purchased or maintained, as the case of Google Docs shows. Many services can be used: "Consumers can use cloud services to store information (e.g. pictures or e-

mail) and to use software (e.g. social networks, streamed video and music, and games)." (European Commission 2012b, 4)

Low Costs

Many services are free (or at least small amounts of data), such as Dropbox, Gmail, Microsoft, Amazon, Evernote, Zotero or Apple iCloud. Of course, there are other "costs" users will face, e.g. the exploitation of data for mailings and advertisements. Also, free services may be designed in a way that they are somewhat clumsy or limited, such that paying for premium services makes them more attractive.

2.3.2. Negative impacts

Cost

In general Cloud Computing is cheap for consumer as most services are free, although often an upgrade to premium services is possible. As an example, we examined the costs of online backup of 100 GB for three years. We used some prices available in Germany in January 2013. The results can be found in Table 1.

Table 1: Comparison of costs of backups: local vs. cloud

Device	**Capacity**	**Costs**
2 external hard drives of 160 GB each (Amazon 2013a)	320 GB	2 x 45,00 € = 90 €
Dropbox	100 GB	7,5 € per month, i.e. 270 € for three years
Google Drive	100 GB	3,8 € per month, 136 € for three years

We assumed a user would wish to have two physical backups if not storing in the cloud. Without accounting for electricity costs and network access, and without taking into account how long the online backup may take, the two hard drives cost about 90 €, while the online backup would cost about 50% more (136 € vs. 90 €). Thus we found that storing a larger amount of data in the cloud is more expensive than buying external hard drives.
Slowness

Availability

The upload or download of data can be too slow, it might be too inconvenient, especially for big amounts of data. For example: in a small test, it took 38 minutes to upload 2 GB to Google Drive with a connection speed of 650 MBit/s respectively 80 MB/s, i.e. about 1MB/sec.

Another aspect is that Cloud services only work if the consumer is online, if fees for transmitting data are reasonable, and if the quality of the connection is good. E.g. mobile data roaming fees hinder the upload of holiday videos or photos or downloading big amounts of data like videos. Also, in remote or holiday areas, basements, trains etc. connectivity might be low or non-existent. Furthermore, consumers might be put under pressure by the necessity to always be online and to respond immediately, e.g. to e-mails.

Dependence on Technology

The more services that are being transferred to "the cloud", the more the consumers will be dependent on technology. This applies to their devices, like smart phones or computers, and also to the Cloud Computing provider. There may be no suitable network access, e.g. when travelling, or on holidays. If a service is down, the consumer can do nothing about it and is stuck. One example is Microsoft's smartphone "Sidekick" which struggled with data loss in 2009 and then closed down in 2011 (Cellan-Jones 2009). This outage was one of the biggest in Cloud Computing history (Cellan-Jones 2009). Also, providers can disappear from the market, their sheer size is no guarantee for survival, as the cases of Enron and Lehman Brothers have shown.

Reuse and resale of Information

Consumers' data might be sold or used in other ways. This applies to photos, documents, and personal information or in general everything that the consumers have uploaded. An example is the controversy that developed around the photo service "Instagram" in the year 2012 and its plans to change their terms and conditions of how pictures of users can be used for advertisement and even sold (Pepitone 2012, Schneier 2013a). Instagram had to withdraw their plans after critique by its userbase. A related issue is that information can be used for different purposes than originally intended if a company gets bankrupt or sold.

Loss of Data

For many private users, any online backup might be better than none. Still, users might lose data if Cloud providers disappear from the market or do not have good backups themselves. Some users of Amazon lost data in 2011 (Blodget 2011). Careful consumers might encrypt data themselves, and even store data with several providers, but this poses new challenges as they need to manage their decryption keys carefully.

Loss of Privacy

Cloud service providers may wish to use the data, for additional sales, for exchange with their business partners, etc. Insiders might read private data. Recently the photo service "Flickr" made private photos public due to a software problem and was not able to restore the prior links so that users had to manually edit them (Schwartz 2013). Also, governments may read data. Such legislation exists in many countries (Greif 2012).

2.3.3. Ambiguous impacts

Consumerisation of IT

The use of Cloud Computing services accelerates the reduction of separation between private and work life, which already has been going on for many years. Workers bring their own devices (BYOD) and use their own software or services and thus bypass their company IT-department, e.g. using Dropbox for team work or rent an Amazon server for a few Euros. Work documents can now be accessed either from the home computer or from the mobile device. This puts additional pressure on workers to respond faster and to work more. Workers try to avoid it – only 30% of the interviewed workers say that they like to access private and work e-mails through one device (Kraus 2012, 11). On the other hand, it allows working when travelling and when at home. The pros and cons of this have been

heatedly discussed with Yahoo!'s management forbidding its employees to work from home (Goldsmith 2013).

Change of Lifestyle and Behaviour

The use of Cloud Computing services can lead to new ways of how things are being done, like working on mobile devices, exchanging documents and using online collaboration tools (like Google Drive). This change in everyday use can bring advantages to users, but for some it might change their way of living in a negative way. It can lead to a dependency on those services and devices. Users might be absorbed by the new technology. But the increase of offers and customised services can also have a positive impact.

2.3.4. Discussion and conclusion

Summarising we see some key advantages, such as the convenience of having data easily available from any Internet-enabled device. Also, consumers use many cloud-based services, such as hosted applications. Problems appear in the following fields: Availability, data losses, costs of network access, loss of privacy, and possible abuse of data for advertisements.

2.4. Impacts on the IT industry

Not surprisingly Cloud Computing will also strongly affect the IT industry, in particular the software and IT services, itself. These impacts are manifold, but strongly interrelated. In the following section main aspects of these impacts should be described and analysed.

2.4.1. Impacts on the market and industry structure

As outlined before (Leimbach et. al 2012, 33) one experiences some difficulties to assess the impact of Cloud Computing on the market and industry structure for several reasons. One reason is the different markets like the one for public Cloud services, Cloud related consultancy or Cloud technology, which are only partly covered by existing studies. Above that each market survey follows its own methodology, which varies strongly between the different market researcher as well as the market researcher themselves vary the methodology in time. Finally there is the problem of availability of these numbers. One example for these differences are the current market figures of Gartner and IDC for 2012. While IDC estimates revenues of 40 billion $ in 2012, Gartner estimates 110 billion $. Main reason is that Gartner also considers so called Cloud advertising (delivery of ads via cloud-based delivery networks) as well as parts of the some Cloud technologies as part of their forecast, which amounts for nearly 90% of the difference between both. However, most interesting might be that both estimates annual growth rates above 20%, which confirm the strong development of the market (IDC 2012, Gartner 2013).

Overall, most of the market researchers therefore agree that the share of Cloud Computing for the overall market will grow in the next years from a few percent at the moment (~3-5%) to a range of 7-10% (5 years horizon) and 10-20% (10 years horizon) in the next years. Consequently Cloud will develop to an independent, fully-fledged segment of the market. According to their estimations mostly affected is the classical software product segment (including maintaining) as well as specific parts of the IT service market such as

IT outsourcing. This also reflects that in particular SaaS (including BPaaS) is and will stay the major segment within Cloud Computing, though in particular IaaS will grow at a higher rate (Leimbach et al. 2012, 34-37, IDC 2012, Gartner 2012). Nevertheless, this development is not a revolution as promised in early phases of Cloud Computing. It is much more an evolution of the market taking up trends that were already discussed before like the orientation towards service-based business models (Cusumano 2004, 36-42).

Above that the market researchers also agree that the regional distribution in Cloud Computing follows the patterns of the overall market, i.e. North America is the biggest market also in Cloud Computing, followed by Europe. However some see especially emerging countries like India as strong pursuer in Cloud (Gartner 2013). But the even more important might be that not only the demand side follows the patterns of the existing market, but also the supply side. This includes that the majority of major Cloud players is of US origin. Examples are:

- Google: of 50 billion $ total revenues (Trevis 2013) 314 million $ where made with Cloud services (Drive, App Engine, Compute Engine) (Panettieri 2013);
- Amazon: the Amazon Cloud offers such as S3 (Storage/Back-up) or EC2 (IaaS) are estimated to have a revenue of around $1.5 – $2 billion in 2012 (Babcock 2013);
- Microsoft: the different offers of Microsoft, in particular Microsoft Azure (PaaS) are estimated to generate annual revenues of $ 1 bn (2012/2013; Bloomberg 2013);
- Rackspace: it is estimated that out of total yearly revenue of 1 billion $ roughly one third are result of dedicated Cloud services (back up, IaaS, PaaS);
- Salesforce: the annual revenue in 2012 was 2.2 billion $ of which most, but not all is related to Cloud services. The most well known offer Salesforce CRM is estimated of generating revenues 731,65 million $ (Streetinsider 2013)

This list shows at least two points. Firstly that like in the traditional market for software and IT services US companies dominate. This dominance become even more significant if other aspects like underlying technologies for example hypervisor etc. are also considered. Here companies like VMWare or Citrix dominate clearly, though the virtualisation software of Citrix, i.e. XEN, has been designed in the UK. The second point is that though this companies sum up for maybe a quarter of all revenues, there is a broad landscape of other suppliers for Cloud services. This spectrum reaches from existing global or regional player like SAP, Oracle or Atos and T-Systems, who are latecomers in the market, as well as many small and medium sized enterprises. This varies between the "cloud or digital born" start-ups like Zimory, blueKiwi, Datameer or even Dropbox or specialised suppliers of software products or IT services, which uses Cloud services as an extension or entrance to their products.

Overall it can be stated that Cloud will change the market structure worldwide, but it will not revolutionize the market as some forecast said at the beginning of the hype. At the moment it seems obvious that the industry structure will only change a little, in particular the dominance of US companies in the traditional software and IT markets will continue, which fits to the point that it is not revolution, but more an evolution.

2.4.2. Impact on innovativeness and business creation

Though most studies that deal with innovation and Cloud Computing focus on the increased ability for innovations and improved time to market for Cloud user, it is obvious that Cloud offers also many new opportunities in the software and IT industry itself. Therefore Cloud offers chances for existing and new IT companies.

It is self-evident that in particular the provision of infrastructure for Cloud Computing is in particular a chance for existing companies that already maintain server and data centre infrastructures. One group are data centre provider and hosting companies such as Terremark, Strato or most of the telecommunication providers such as BT or Deutsche Telekom. Others like Amazon may be a surprise at a first glance, but given the fact that the main business requires a worldwide, scalable infrastructure due to seasonal effects it seems reasonable to try to exploit this. Other examples are software product companies who can now create new business opportunities out of their main business by providing new usage models, which may also attract new user. One well known example for this is SAP by Design. Moreover also smaller software companies could also exploit these opportunities by using the infrastructure of other provider such as Amazon.

Overall Cloud Computing offers foremost many opportunities for existing software and IT companies, but there also cases where Cloud Computing enables new business and new business models within the IT industry. The most well known example is Dropbox. It started as backup service, founded by two MIT students and became to one of the most famous backup, collaboration and synchronisation companies in the last four years with yearly revenue of more than 200 million $. Though many user (nearly 90%) may only use the free service, it shows that freemium concepts work out (Barret 2011). One major point is that they only use Cloud services of other providers like Amazon and do not have a dedicated own infrastructure. But Dropbox is not the only example, many others in particular provider of app based services for iOS or Android often use Cloud infrastructures provided by third parties. This shed a light on a trend that already began with the spread of utility computing as one of the predecessors of Cloud Computing in the mid 2000s.

The overall idea behind it was that companies should focus on their core business while retrieving IT services as an outsourced utility service from an IT service provider. In the first line this idea addressed big user companies, but with the appearance of Cloud Computing and the world of App stores, the concept swept back to the IT and software industry itself in form so called cloud or digital born start ups. One idea behind that is that companies should focus on their core activity like in the case of Dropbox the provision of an easy to use interface for collaboration and synchronisation, but not deal with non-core activities like the provision of data centre infrastructure. This is also reflect in research on new business models for Cloud Computing, which show new type of actors like service aggregators (Leimeister et. al. 2010).

However this new approach also contains some challenges. In particular multi sourcing, i.e. the use of multiple suppliers for similar or varying services, creates several challenges regarding legal construction, IPR, compliance or data protection conformity (Duisberg 2011). Moreover other emerging like service brokers such as Zimory, which act as dealing

platform between providers and users, could be a solution for it, but until now it is unclear if their role will develop or if they will be eaten up by the dominant market players (Leimeister et. al. 2010).

2.4.3. Commoditization and the impact on business models

New business models like aggregators and brokers are one part of wider discussion on the commoditization of IT, i.e. if IT will become an utility comparable to electricity or water. As many other discussions in the context of Cloud it already started in the early 2000s pushed by an article and book of Nicolas Carr, at this time editor of the Harvard Business Review, entitled with the Question "Does IT matter?" (Carr 2003). His main argument was that IT is becoming more and more like an infrastructure and consequently would not be of strategic value anymore. This discussion became enforced by the appearance of Cloud with its typical attributes of scalability and "pay as you go". Consequently Carr (2009) published a new book that explicitly states that IT or what he called the "information grid" will become an utility like electricity. This argumentation fueled the debate of Cloud critics arguing that Cloud Computing would lead into a cannibalization of the existing IT industry. In particular many IT service provider were afraid that as a service models would influence strongly their value chain, but also classical software producer were often reluctant against it (Giron et al. 2009).

But many others also argued against the theory of commoditization of IT. The main arguments were summarized for example by Brynjolfsson et al. (2010). They state that IT and in particular Cloud Computing can't be easily compared with utilities like electricity because of several differences in the technology and business models. Technical differences they see in speed of innovation, the limits of scalability and the latency challenge of computing. With regard to the business model they state that lacking complementarities, the problems of lock-in and interoperability as well as the security challenges posed by Cloud Computing differ Cloud Computing from electricity. On base of that they conclude that Cloud has not yet reached the state of an utility and that it is open if it ever will be in the future.

Overall it is clear that Cloud Computing will impact business models in the software and IT industry, but this development is still in the flux. As outlined before there are many open questions around Cloud, not only for technological, but in particular for business reasons. Consequently it seems clear that Cloud Computing will change the traditional revenue streams and thereby business models in the software and IT industry, but there is still a need of consolidation of revenue models or type of actors. This also implies the question whether the existing ecosystems will exist further, maybe with different centers, or if the overall structure will change in long term (Leimbach et al. 2012, 13-20). Because of that there is until now no proof on the argument of commoditization of IT implying that the market will stagnate or even shrink, but it is also clear that Cloud Computing will not lead to an explosive growth of the overall market.

2.4.4. Discussion and conclusion

Concluding it can be stated that Cloud Computing overall provides many opportunities, but also many uncertainties. Nevertheless it will impact the market and industry structure in some ways.

First of all it is obvious that will become an independent market segment, but it will not revolutionize the other sectors. Moreover it is also possible that over the years Cloud Computing to be taken up with existing or other emerging segments. Nevertheless the technical ideas will remain as a central part of the new IT infrastructure.

Secondly, like in all new waves some new players will appear that manage to become global players in the industry. But to achieve this, one major challenge will be to turn their revenues into profit and grow further meanwhile. This is a point, where many failed before. Moreover, it is obviously that many of the existing global players will develop this field of activity and try to maintain their position. One major strategy for that is based on the acquisition of promising small and medium sized enterprises, which either hold relevant Cloud technologies or in particular business services. Examples for this strategy can be found in the US like Oracle as well as in Europe like Atos.

Thirdly, as a consequence the industry structure and in particular the dominance of companies based in the US will not change overall. Only in some cases new players may appear or old disappear. From a European perspective this seems critical, because at least to some extent Cloud offers a window of opportunity, but as it seems many problems that hindered European companies to gain more importance like the limited growth potential for start-ups due to lack of unified markets and slower adoption or others did not cease to exist.

2.5. Impacts on economy and society as a whole

In this section, as before, we basically list impacts as identified in the available scientific literature.

2.5.1. Positive impacts

Creation of Jobs

Real

In the studies available, no figures for the creation or abolishment of jobs have been provided. Therefore, as an indication, a few figures from Cloud Computing companies are presented. For example, Salesforce and Rackspace, which are purely cloud-based have 8000 and 700 employees, respectively. Some European users of Cloud Computing, such as Spotify and Dailymotion, have 450 and 165 employees. Additionally many existing IT providers have created new units for Cloud Computing, but in these cases it is not possible to differentiate whether the positions created are new jobs or only existing jobs with a new label. The same is valid for user companies. Overall it is certain that there are new jobs among them, but the extent is unclear.

Estimates

While there is a lack of estimates for real job effects, there are several estimates according to which Cloud Computing will create many new jobs in the future. This is an often named impact of Cloud Computing and its adoption (Wauters et al. 2011, Aumasson et al. 2010, Bradshaw et al. 2012). Estimations are between 1.3 million and 3.8 million new jobs in the

EU by 2020, depending on different scenarios regarding changes or no changes in policy (Bradshaw et al. 2012, 9). Another estimation is 1 million jobs (Etro 2010, 108). Bradshaw et al. (2012) write: "Estimating the impact on employment is more complex. Considering only the potential of creation of new jobs, IDC estimates that in the ‚Policy-driven' scenario cloud-related workers could exceed 3.8 million, against some 1.3 million in the ‚No Intervention' scenario. This does not take into account the jobs that would be lost or the workers that would be displaced by cloud-related reorganisation of business processes. The productivity increases driven by cloud efficiencies would most probably create in the short term an overall neutral (or even slightly negative) impact on total EU employment. However, in the medium-long term the overall dynamics of economic growth driven by cloud should result in a positive driver of employment, particularly considering the creation of new SMEs." (Bradshaw et. al. 2012, 61). So in conclusion the authors say that at first jobs will even out or even slightly decrease, but in the long run the number might increase.

Etro stresses that such estimates must be carefully assessed, since there will be an increase in hours worked which not necessarily will be directly transformed to new jobs – employees might also have to work more hours. How hours are directed into jobs is not specified by the author. Over the time this increase of jobs will vanish and will be normalised.

Hogan expects 2.3 million new jobs between 2010 and 2015 in the UK, Germany, France, Italy and Spain (Hogan et al. 2010, 7) based on their study for those countries.

There are various estimates for the number of future jobs, but surprisingly no attempts and figuring out today's effect on jobs. The estimates for future jobs do not differentiate between jobs created, jobs lost and net effect. The only study which presents large parts of its method is Etro, who, however, is based on a very optimistic view of developments, see below.

Creation of New Businesses

Any rise of new jobs is closely connected to the creation of new businesses (SMEs). Etro expects that in wholesale and retail trade 156,000 new firms will be created and in real estate and other business activities 144,000 new SMEs will be created (Etro 2010, 110). The basis is unclear, e.g. it is not explained why the author expects more jobs in real estate, where Cloud Computing might as well mean more concentration.

Contribution to GDP

In the available studies, there are no estimates for the contribution of Cloud Computing to GPD during the last years. However, there are some forecasts.

The study of Etro provides one estimate. He states that the average fixed ICT costs in Europe are 5% of total costs, and hence total ICT costs, including variable costs, are somewhat larger. He states that telecommunications has a large share of ICT costs, with more than 20%, while other industries have smaller shares. He then writes that those costs can be reduced between 1% and 5% (Etro 2009, 190; similarly in Etro 2011). From the way he puts it, it becomes clear that he does not, e.g. mean, 5% of 5%, i.e. 0,25%, but

apparently he believes that Cloud Computing can reduce the total costs of European firms by 1% to 5%. Feeding this input into his economic model leads to his result that annual GDP might grow between 0.05% and 0.3% with Cloud Computing (Etro 2009, 191).

This effect depends crucially on the amount of the fixed ICT costs which would disappear. So if firms continue to need servers on the manufacturing floor (for fast response), computers to conduct banking transactions quickly, laptop computers to work anywhere at any time, then only a much smaller share of computers can be replaced. E.g. in telecommunications, due to low latency requirements, computing cannot be outsourced to a cheap remote server farm. Thus it appears that Etro's initial statement about the cost reductions going with the introduction of Cloud Computing is flawed and therefore his estimation for higher growth are unjustified.

Another estimation for the increase of GDP in Europe is 88€ billion to 250€ billion for 2020 annually (Bradshaw et al., 2012, 60). The authors do not describe their method. For the period 2015 – 2020 the cumulative impact could range between €357 billion and €940 billion (non-policy driven scenario versus policy driven scenario) (Bradshaw et al. 2012, 61). But for 6 years, it would be at least 540 billion. The numbers appear inconsistent. Based on Bradshaw et al., the European Commission expects "an overall cumulative impact on GDP of EUR 957 billion [...] by 2020" (European Commission 2012b, 2).

2.5.2. Negative impacts

Loss of Jobs

It is or was feared that through the new ways of outsourcing that Cloud Computing offers IT jobs would be lost since companies would not need their IT staff anymore after the move into the cloud (Dignan 2011, Schubert/Jeffery 2012, 35). But no such shift has been reported in the available literature, there hasn't been a wave of IT staff that lost their jobs. Apparently only few jobs can be outsourced or can be replaced through the use of the cloud. There are still special tasks that can't be performed online, e.g. working closely with customers, time-critical computations or processing of highly confidential data.

Reduction of GDP

The reduction of jobs as forecast by Dignan (2011) and Schubert & Jeffery (2012) might lead to a general reduction of costs and prices and hence to a contraction of GDP. No such effect has been reported.

Loss of Businesses

The reduction of jobs as forecast by Dignan and Schubert & Jeffery might lead to a general reduction of the number of IT services firms, but no such effect has been reported.

Dependency on US providers

US Cloud Computing providers have a strong global role because the US allowed Internet services relatively early (e.g. because powerful modems were forbidden in Europe to protect proprietary PTT-services) and developed huge economies of scale, as well as companies with significant investment capabilities. Given the above mentioned issues with service quality, privacy etc., and assuming that Cloud Computing will become economically

more attractive in the future, European service providers following European regulations would become attractive.

Adaptation of Content, Censorship

The big cloud providers already censor content and will continue doing so. They adhere to local laws and moral concepts (Van der Velden/Kruk 2012). E.g. Apple removed a Wikileaks App from the App Store in 2010 (Van der Velden/Kruk 2012, 11) although they were not obliged to do so. In 2012 Apple removed an App that showed US drones that hit targets in Pakistan, Yemen and Somalia (Van der Velden/Kruk 2012, 11).

2.5.3. Ambiguous impacts

Environmental Aspects (Resources, Energy, Waste)

It is very difficult to assess the environmental aspects that come with Cloud Computing: Will it lead to less emissions and energy consumption because companies will outsource their IT to shared resources or will those server farms and networks produce even more emissions? In their study for Greenpeace, Cook & Van Horn stress the difficulty to find clear numbers and make assumptions about emissions coming from the cloud (Cook/Van Horn 2010, 4). Cloud Computing respectively IT innovations can cut emissions; this possible advantage of cloud services is being used in advertisement but it is difficult to evaluate the companies concerning emission output (Cook/Van Horn 2010, 5). Emissions produced by ICT in general will rise unless measures are being taken. But they could also be reduced through smart use of technology which again could lead to a higher consumption in general (FI3P 2011, 105). This issue is complicated and can move both in positive and negative directions. The European Commission considers the access to information, regarding how a product affects the environment, important for consumers (European Commission 2012a, 5). It mentions the positive aspects that Cloud Computing could bring, e.g. saving energy through low-energy data centers and the use of green energy (European Commission 2012b, 4). In all four documents mentioned, no figures on a change of energy consumption because of Cloud Computing have been mentioned.

2.5.4. Discussion and conclusions

For the society as a whole, regarding jobs and growth, currently Cloud Computing has little impact at the moment. The estimates provided by Etro appear to be based on very optimistic input variables for cost savings and the emergence of new SMEs. Another point is that the model uses estimated figures on cost savings, because at the moment there is still a lack of precise data. Only longitudinal firm level studies could provide this, which will need some time between the appearance of a technology and its diffusion. As a consequence the results have to be taken with care, in particular because Europe always lagged behind in the diffusion of emerging IT technologies. This is also seen as one reason for the productivity gap between the US and Europe (van Ark 2003). However, in the long run the positive economic effects may increase, but as recent studies shows it also bears risks.

Brynjolfson and McAffee (2011), two economists from the MIT, have recently shown in their long time analysis of the impact of It technologies on the US economy that in particular job creation will only work out if certain conditions are in place, in particular the availability of infrastructures and higher skilled workforce. The reason is that as shown by their analysis productivity and growth may improve, but that many jobs especially low class jobs were also destroyed by IT diffusion in the long run. Until now this was outweighed by the creation of new more high qualified jobs, but to keep up with the increased speed of diffusion it will require targeted efforts regarding education, infrastructure and the institutional development to achieve a positive return in jobs.

Another aspect is that of service provision by US companies. This has significance in terms of jobs and income, government access to data, and even censorship. Consequently it would be desirable to have a vivid and competitive market, which would also contribute to realisation of the positive potentials of Cloud Computing, in particular if cheap, reliable, privacy-protecting European Cloud providers appear. This in turn means that companies may, in the long run, have comparative disadvantages if they will not adopt to such high quality, cheap services.

Obvious policy consequences would be to encourage the emergence of European providers with high quality services. Certifications might show law compliance, quality of backups, quality of intrusion detection, etc.

2.6. Conclusions

After this review of impacts we see that global revenues from the sales of public cloud services with shared resources are in the range of a few billion $, earned by some vendors, e.g. Amazon. Similarly, both large job growth with Cloud Computing providers and large job reductions in company IT-departments apparently have not yet appeared. Key obstacles are bandwidth, security (especially confidentiality) and outages, next to legal issues such as data protection or contractual relationships.

On the other hand, Cloud Computing offers entrepreneurs methods to kick start new businesses as we can see with examples like Air B'n'B, Zotero, the examples mentioned at Amazon or Facebook-Apps that run on Cloud Computing machines.

So in sum there appears to be much hype about Cloud Computing. Yet, if obstacles were overcome, economic benefits of resource sharing might be earned. Moreover it also requires that framework conditions are in place that allows realising the benefits of a strong adoption and utilisation. . Therefore we address some obstacles and requirements in other chapters of this report, and intend to evaluate them all at the planned project workshop. Still, some policy options can already be mentioned:

- Address bandwidth and availability in rural areas, e.g. through licensing “light”, unlicensed communications with higher reach, or mandatory coverage.
- Address costs for network access, such as an abolishment of mobile data roaming fees.
- Review the Safe Harbour principle, negotiate conditions for government access or encourage the development of Cloud systems which protect secrets reliably.

- Make portability easy, e.g. by enforcing providers to provide interfaces and data formats.
- Provide a right to have data deleted.
- To encourage the use of provider certification, which show compliance with European regulations. Certifications could also cover quality of backups, quality of intrusion detection, etc.
- To encourage the emergence of European providers with high quality services.
- Organise a portal for addressing problems with Cloud Computing services.
- Address the educational needs caused by Cloud Computing.

3. SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

3.1. Introduction

As shown in our initial analyses of drivers and barriers of Cloud Computing (Leimbach et al. 2012, 83-85) as well as in the previous section on socio-economic impacts, there is one cluster of barriers and impacts focusing on the topics of data security, data location, privacy and trust. These issues have a high importance for all type of users, business and administrative as well as consumer, though the reasons and perspectives might differ.

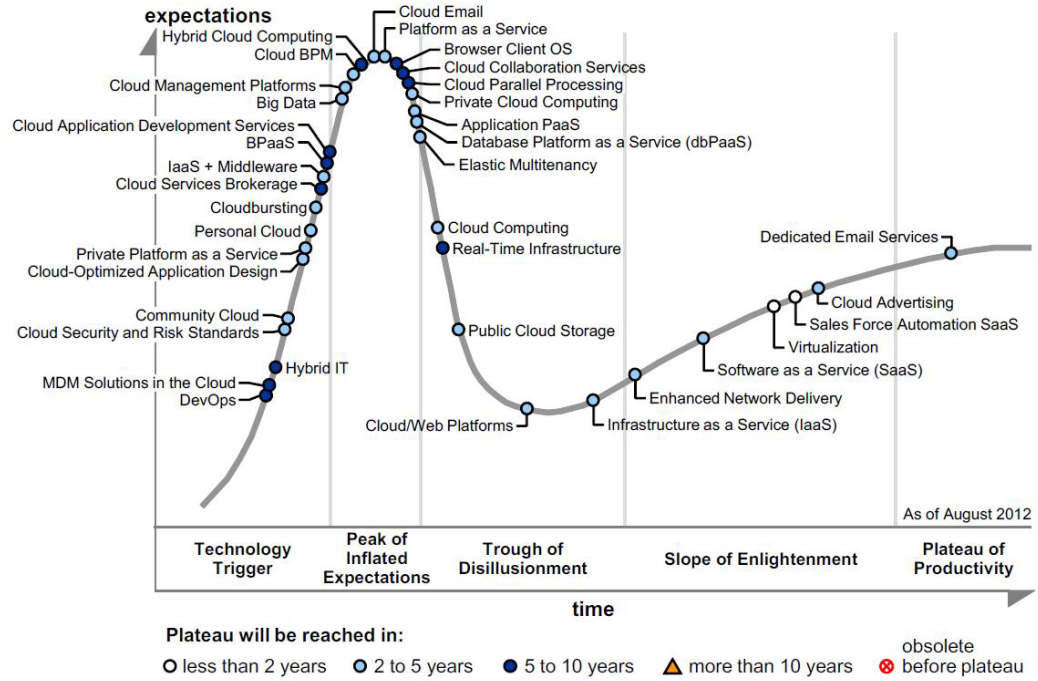
Consequently the next section will try to depicture these reasons and show why these aspects are of importance and what are the related concerns, problems, expectations and challenges in it. The following section will then analyze technical threats and responses to data security. This will be followed by an analysis of the current data protection regime in the EU as well as the ongoing changes from the point of view of Cloud Computing. In the final section will address the question of data location, in particular the question of enforcement of EU standards and laws outside of the union, as well as the question of data access by third parties.

3.2. Overall relevance of security and privacy

This section first provides an overview of debates surrounding risks connected to the adoption of cloud computing, interjecting along the way introductory remarks to support the reader's comprehension of the issues at stake. The section then goes on to highlight particular risks as seen from three main user perspectives, namely businesses, governments and private citizens. The section is meant to provide an introduction to the basic problematic of cloud computing security, the implications of which are explicated in the subsequent sections on security solutions, data protection legislation, competitiveness and international cloud governance.

A few years ago, cloud was often branded as a "paradigmatic shift" in ICT development and there was much talk about a "transition to the cloud" implying that cloud computing could and would very rapidly replace most of the existing on-site ICT infrastructure owned by companies, governments and personal users. The key driver for this hype was the idea of cost savings and increased flexibility in ICT infrastructure. These factors remain at the forefront today (Rader 2012, Vanson Bourne 2012, KPMG 2013). However, societal attitudes towards cloud computing seem to be maturing as real-world experiences with the complexities of technological transformation have been harvested by different user groups. In 2012, Gartner placed cloud computing as a whole in the downward-turn part of the Gartner hype-cycle ("the trough of disillusionment") with a number of concrete cloud applications still being surrounded by the kind of hype leading to a "peak of inflated expectations" (see figure 1 below). In 2013, if we are to follow Gartner's 2012 predictions, cloud computing as a whole should be moving into the "slope of enlightenment" with concrete services reaching the downward-turn phase.

Figure 1. Hype Cycle for Cloud Computing, 2012



Source: Gartner (August 2012)

Such predictions are highly speculative, of course, but worth mentioning here since they seem to fit roughly with the picture drawn by our research for this report. Concrete user experiences are gradually reshaping opinions on the practicalities of cloud computing and the potentials to be harvested from it. From an early phase of naïve assumptions about the cloud providing a "technical fix" for many of the inefficiencies haunting modern knowledge-work, a greater awareness of the organizational transformations needed on the part of users to harvest such benefits is apparent in cloud debates involving business and government users. This involves a shift of attention away from the immediate gains from 1-to-1 replacement of on-site ICT functions with cloud replicas to the gains to be had from process innovation making use of novel opportunities which cloud technology presents.

Positive impacts

The positive impacts of adopting cloud computing are generally associated with cost savings out of which comes a lowered threshold for trying out new ICT solutions and a higher degree of organizational flexibility. As shown in section 2 of this report, however, the picture of how such cost savings are harvested, however, is becoming more refined. A first generation of cloud services including cloud-based e-mail, file storage and office applications have naturally played a central role in the formation of personal users' attitudes towards the cloud. And for businesses and government, access to the raw computing power of giant server farms to support existing types of ICT infrastructure such as websites and databases has also played an important role in cutting cost. Cost savings have thus been harvested by replacing software and hardware as products with service equivalents. But in a second generation of services developed in recent years, providers are providing cloud-based solutions that go much deeper into the workings of organisations, such as accounting, business intelligence, and even ICT support of manufacturing

processes (KMPG 2013). Implementing these deeper seated types of solutions demands of organisations that the organisational processes to be facilitated by cloud services are adapted to fit to the limitations of the cloud service – a classic example of technology-driven transformation. A cloud services mature, they thus come into contact with the heavy questions of organisational innovation and transformation and what was originally viewed as an easy fix becomes one element of many in the on-going efforts of organisations to optimize processes. While it may not make sense to expect a general "transition to the cloud" taking place in one fell swoop, still cloud technology will most likely come to take up an ever increasing part of the total ICT infrastructure supporting business, administration, and our daily lives.

Security risks

The situation, however, is not all roses. The dangers inherent in the centralization of data processing have received explosive attention on the heels of the leaks by NSA contractor Edward Snowden of information about secret surveillance programs in the U.S. and the U.K. According to the Guardian, Snowden has documented a secret program of the U.S. National Security Agency (NSA) entitled PRISM through which the NSA has obtained access without warrants to personal information such as search histories, e-mail contents, file transfers and live chats from users of services provided by Google, Facebook, Apple and other U.S. internet giants (Greenwald and MacAskill 2013a). Followed by a number of other revelations about trans-border intelligence gathering taking place by way of access to the high-speed fibre cables and centralized centres for data storage and communication, which support the information society (e.g. Poitras et. al. 2013), Snowden revelations may have already fundamentally changed public perceptions of the risks/benefit calculus in connection with cloud computing.

Even before the Snowden leaks, security and privacy consistently scored among the most prevalent concerns with regard to cloud adoption for businesses and government agencies in Europe as well as for individual citizens (Cattedu and Hogben 2009b; Cattedu 2011; WEF 2011; KPMG 2013). The key argument seems today to turn around the total security value of cloud solutions versus on-site solutions. On one hand, professional cloud providers are more often than not able to provide much more advanced data protection at both software and hardware levels. On the other hand, amassing the data of potentially millions of users in one great cluster of serves all connected via the same hypervisor produces a highly attractive target for hackers, be they individual enthusiasts, political groups, industrial spies or foreign governments. The PRISM scandal only illustrates this point all too well. In the absence of an overarching framework for creating trust in the cloud, coming to a balanced assessment of these issues still rests on the shoulders on the individual CIO of business or governments.

Among the top security threats in the cloud are:

- **Data breaches:** While cloud providers are able to uphold much more professional data security than the average cloud user, amassing great amounts of data together in centralized systems also creates a focus point for hackers and spies. So while security

holes will be fixed quicker, the risk associated with them is greater than in ordinary ICT use.

- **Data loss:** Attacks by hackers, accidental erasure by providers, physical catastrophes like fire or earthquakes, and providers going out of service all represent ways in which permanent data loss may be suffered by cloud users.

- **Hijacking of accounts:** Techniques for hijacking electronic communication via phishing or out-right fraud have a long history unconnected to the cloud. But with cloud service use, the gravity of such access gained can be much higher. Cloud-based e-mail accounts, for instance, quickly become the centre for access to almost all other communication channels of a user and thus enable identity theft as well the ill-willed use of users' online identity.
- **Denial-of-service:** Distributed denial-of-service (DDoS) attacks are a primitive, but effective way of causing disturbances to online communications. By overloading communication channels and computing resources, such attacks slow everything to a grinding halt. While the scalability of the cloud initially creates a greater tolerance at system level for such attacks, DDoS methods are continually evolving.
- **Management interface (API) compromise:** As cloud services evolve into whole ecosystems of services built upon the infrastructure of just a few providers, the security of the interfaces providing access to the systems of those core providers becomes more and more important.
- **Loss of governance:** Perhaps the most key issue in the debate about data protection practices and legislation having to do with the cloud, the basic observation remains true that users lose control of their data (data governance) when transitioning to the cloud. This issue underlies debates about transparency, standardization, and auditability of cloud services as well as information assurance systems.
- **Malicious insiders:** The enormous mass of data stored in clouds represent and unprecedented gathering of information value. Having access to such values creates temptations for exploiting that value by malicious insiders. Beyond the cloak-and-dagger scenario – the risk of which is very real – of cloud employees going rogue or becoming moles for outside forces, the "malicious insider" may also be the cloud provider itself exploiting personal data in illicit ways or governments gaining direct access to the cloud.

Establishing reliability and trust

On the basis of these well-known threats, the question of establishing trust in the cloud has become more and more complicated, continually driving towards a need for societal-level solutions. The process of public and private actors working towards establishing such trust and reliability can been divided in 5 major steps:

- **Threat identification:** Firstly, the agency identified "top security risks" associated with the cloud, which still remain key to the discussion of security in the cloud (see figure 2 below). These risks are identified to act as a framework for understanding cloud-specific security issues. These are not, as documented in by the Cloud Security Alliance (CSA

2013), necessarily the most pressing matters at any given time. But conceptually, they are fundamental to the relationship cloud users enter into with their cloud provider. Other institutions have sought to provide on-going monitoring of security concerns based, among these the CSA mentioned above, the IEEE, and the KPMG consultancy. Until recently, however, no official body had been established to provide European-level CERT (Computer Emergency Response Team) services with regard to the cloud. This was changed in April this year when ENISA was awarded official EU CERT status by the European Parliament, mandating the agency to extend its capacity to counter cyber-attacks and to support other European agencies such as Europol's cyber-crime division as well as national level bodies such as data protection agencies (EP 2013).

- **Information security assurance:** Secondly, ENISA along with others identified the lack of auditability and trustworthy security assurance as a threat to the ability of data controllers (cloud users) to verify the basic security of their data. This represents a fundamental weakness in the total technical and legal data protection situation exists in the relationship between a cloud user and a cloud provider. The lack of clear assurance measures in typical cloud contracts interjects a layer of uncertainty into the risk assessment of the user. And it weakens the ability of users to make a qualified choice between cloud providers' service offerings. The Article 29 Working Party has in its opinion on cloud computing highlighted the need to create measures to gain greater clarity about data protection measures taken by cloud providers and has in that context welcomed the provisions in Article 26 of the EC's data protection regulation proposal for making cloud providers more accountable towards users (WP 196: 23). In terms of practical solutions for establishing easy security assurance, and thereby greater transparency and accountability, ENISA has provided an assurance framework (ENISA 2009c) meant to be immediately useful to business leaders and CIOs in assessing security in connection with cloud adoption. The framework was also made to inspire the work of cloud providers attempting to create common standards and European policy makers in their work of providing legal measures and economic incentives for the development of trustworthy cloud solutions. Similar frameworks have been produced by other organizations, both public and private, including the SCAP automated system based on NIST standards, the CloudAudit and Cloud Controls Matrix initiatives under CSA, the ISACA Cloud Computing Management Audit/Assurance Program, and the U.S. Federal Risk and Authorization Management Programme (FedRAMP) aimed at streamlining cloud providers' authorization as providers to the U.S. government (ITTL 2011). From a European perspective, however none of these initiatives has managed to establish a truly global consensus on assurance standards. For this reason, the European Commission included as a key pillar in its 2012 cloud strategy the commitment to work with industry and relevant public sector actors to establish such a consensus (COM 2012/529). Soft governance alone, however, will not be enough to determine the specific boundaries within which the cloud can develop. The outcome of the on-going negotiations to revise the European data protection directive and the regimes of international data governance collaboration, which accompanies the directive, will play a key role in deciding, which standards of system development and which practices of information security and assurance will shape future developments.
- **Addressing SME data protection concerns:** SMEs are key to the economy and their attitudes and experiences concerning the cloud are thus crucial to the question, which

role the cloud can ultimately come to play as an economic factor. We will look closer at the specific impacts and risks of the cloud on SMEs below. Importantly, ENISA and others (WEF 2010, 2011, EC 2011, IDC 2011) have documented clearly that they are highly concerned about security issues in the cloud and the dangers implied, such as data loss due to failure and security breaches due to system flaws, hackers, industrial espionage. Although cloud providers typically focus on the security upside of the cloud, which is increased professionalism and presumably, scrutiny be foreign governments should now be added to the list. Since SME cloud adoption has been pointed to as a necessary step to reap the society-level economic potential of cloud computing (Etro 2009, 2011, Liebenau et. al. 2012), it becomes particularly pertinent to address such concerns. But at the same time, the lack of capacity in typical SMEs for conducting proper risk assessments accentuates the need for societal-level solutions to cloud security. Individual SMEs will in many cases be unable to utilize even the most standardized assessment and/or auditing systems. They will need security issues to be solved "behind the scenes" so to speak by providers and legislators so as to ensure the provision of fundamentally safer (and more trustworthy) solutions. We will look into such solutions in section 3.3.

- **Data security for governments:** Governments-as-customers make up an especially important category of actors in the development of the cloud. Due to their sheer size and their central role in societal development, adoption of the cloud by government bodies could pop the cork for the society-wide transition to the cloud. But for governments, there are areas where risk vs. benefit calculations, where possible efficiency gains could never truly outweigh the losses suffered in case of security breaches and subsequent malevolent use of information. Such areas include health, financial information, and social services information among others. Technically, these risks are identical to those run by any type of user: data loss We will look closer at examples of such risks below. Due to the severity of risks in this area governments have moved slower than business actors in adopting cloud technology (KPMG 2012). Again, individual risk assessment comes into focus as a key practice necessary for step-wise adoption of cloud services. ENISA (2011) provided guidance for such assessment and for negotiating service-level contracts and assurance conditions with cloud providers. In a similar vein, but with an even more hands-on approach to the safe adoption of cloud services, the U.S. National Institute of Science and Technology (NIST) is currently in the process of creating finalizing its Cloud Computing Security Reference Architecture which will allow individual government organisations to assess the most appropriate cloud services to adopt. From a certain point of view, such security assessments carried out by government bodies and the negotiations with cloud providers which follow from them could act as a crowbar for the establishment of best practices in contracts and assurance practices. This could especially be the case in those countries, where government cloud adoption has been put into an overall systematic, such as in the U.S., the U.K, Japan and to some degree France. All of these countries have so-called G-Cloud initiatives in place, which we will look into in some detail below. But again, the overall legal framework cannot be ignored and individual negotiations seem unable to solve the more fundamental issues of security and privacy. We have thus seen cases in which the Danish and Swedish Data Protection Agencies have denied local government access to proprietary cloud solutions on the basis that risk assessment

and security assurance were not possible to the satisfaction of the Agencies based on the information provided by the private cloud providers in questions (refs). Also here, the need for universal standards seems pressing.

- **Societal level risk assessment:** The latest step taken by ENISA in assessing risk associated with cloud computing is to assess the aggregated risk effects on society as a whole from widespread and increasing cloud adoption (Dekker 2012). So far, it seems that ENISA is the only government risk assessment organization to take up this perspective. With the adoption of cloud services by ever more critical sectors of society (key examples are the energy, finance and health sectors) cloud computing in itself comes to take a place in the critical infrastructure of society. Here again, with even greater gravity, we come across the "double-edged sword"-argument: that on the one professional cloud providers are able to employ state-of-the-art security measures; but that on the other hand, such massive concentration of important data hugely increases the impact of breaches and provides an alluring target for malevolent intruders. This last step firmly connects the cloud debate to the debate over public governance of ICT security. Without mandatory incidence reports and continual monitoring, auditing and testing of systems, no real progress can be made towards truly trustworthy cloud services. Such demands can only be made by governments and inter-governmental institutions. At the same time, the widely heard call for standardization is reiterated, since also here the swift and efficient spread of best practices is key to providing users with safe solutions.

With the Snowden leaks and the ensuing scandal, the cloud debate is now moving into a more explicitly political phase. The main questions so far have regarded benefits to users and the risks associated with security breaches. The cloud in itself has been viewed as a neutral, purely technical space defined entirely by its utility to users. The possibility of breaches of security and privacy occurring from within the cloud itself has been attributed to the possible acts of the "malicious insider" acting on behalf of outside interests. But now, questions are being raised about the inherent neutrality of cloud providers. Can we in fact trust that cloud providers act first and foremost to serve users? On the one hand, there seems to be a real risk that private information can be monitored by government intelligence (a risk we will look at more closely in section 3.5). On the other hand, the very possibility of such data monitoring within the cloud and the use to be made of it also brings into question the use, cloud providers might themselves make of the data. If cloud data has in fact been subjected to data mining by the U.S. government, can we trust that major cloud providers - themselves cutting-edge experts in data mining – do not make similar, albeit commercially oriented uses of our private data? As recently stated by Vice President Neelie Kroes, we live in an age of "total information" (MEMO/13/654). But will this also prove to be an age of total information abuse? Clearly, the political work to establish and maintain trust in cloud services is only now beginning and cannot clearly be isolated from broader questions of data security in an age of big data and ubiquitous computing.

3.2.1. Security and privacy for businesses

Businesses have been the frontrunners in cloud computing uptake, European businesses lacking somewhat behind the more mature U.S. market. KPMG (2013) indicates that while security remains one of the top concerns of IT and business leaders with regard to cloud

computing, it is no longer *the* top concern (as it was in a 2011 survey by the same company) (KPMG 2013, 14). Ranking as top concerns are now issues of implementation (IT leaders) and business transformation to make use of cloud to realize long-term gains (business leaders). "Gaining real cost savings from the cloud is about more than simply moving from fixed costs to operating costs; the greatest cost savings – and, more importantly, the transformational business benefits – will come from the longer term outcomes such as more efficient processes, more flexible operating models and faster entry into new markets and geographies" (KPMG 2013, 9). Harvesting these long-term benefits will, according to KPMG, demand that IT and business leaders work together over long enough stretches of time and under a strategic perspective focusing on process innovation and transformation.

The KPMG survey respondents rank security concerns acting as barriers to cloud uptake and the gravity of each (scored on a 1-5 scale) as follows:

- Data loss and privacy risks: 30% (Gravity: 4.19)
- General security risks: 26% (Gravity 4.11)
- Risk of intellectual property theft: 21% (Gravity: 4.21)
- Legal and regulatory compliance: 18% (Gravity 3.95)
- System availability and business continuity risks: 16% (Gravity: 4.03)

The KPMG survey furthermore indicates that while security remains one among top concerns, it seems no longer to be hindering adoption in terms of real-world behaviour (KPMG 2013, 17). In a European context, this result might not be duplicable as the U.S. cloud market from which respondents were drawn has been faster to mature. It might, however, be indicative of experiences to come for European business users.

One last point to note from the KMPG survey is that cloud is being adopted in an increasing breadth of business areas, which rank: HR (57%), IT management (54%), e-mail/collaboration software (53%), sales/marketing (52%), customer care (51%), office tools/productivity (51%), supply chain and logistics (42%), finance and accounting/financial management (41%), business intelligence/analytics (41%), security management (40%), content management (39%), sourcing and procurement (36%), tax (36%), operations/manufacturing (35%).

Cattaneo et. al. 2012 clustered a group of barriers to cloud uptake by businesses as follows:

- Data jurisdiction and location
- Security and Trust
- Portability and technology transparency
- Business (usefulness, local support/language)
- Industrial policy (internet connection speed, taxes)

Analysing the relation between these barriers as perceived by survey participants and as indicated by their actual cloud adoption behaviour, the report indicated a high degree of

alignment between perceptions and behaviour on the part of large European companies while SMEs were shown to suffer from a disconnect between perceptions and behaviour; SMEs also point to legal jurisdiction/data location and security as main barriers uptake, but behavioural indicators point to evaluation of usefulness and trust as main barriers (Cattaneo 2012, 39).

ENISA (2009b, 15) identifies "confidentiality of corporate data" and "privacy" as the two most pressing concerns for SMEs with regard to Cloud Computing use in their businesses. 43 of 64 responses classify "confidentiality of corporate data" as a "showstopper" while 17 of 64 classified it as "very important". For "privacy", the same numbers are 31 and 28 out of 66 respectively. Other issues identified by significant portions of respondents (more than two thirds in total) as "showstoppers" or "very important" are: availability of services and/or data; integrity of services and/or data; loss of control of services and/or data; lack of liability of providers in case of security incidents. Issues more often rated to be of "medium importance" by respondents in the survey included: inconsistency between transnational laws and regulations; unclear schemes in the pay per use approach; cost and difficulty of migration to the cloud; intra-cloud migration (i.e. vendor lock-in).

ENISA's report on Critical Cloud Computing (Dekker 2012) notes that still more sectors are adopting cloud services in still more business areas. New sectors adopting cloud services include the finance sector, the transport sector, and the energy sector. These sectors being "critical infrastructure sectors" cloud computing in itself becomes "critical" (Dekker 2012, 4-5). Increased adoption thus leads to a qualitative shift in the significance of cloud security issues, which in the first instance affect individual business users; cumulatively, these issues become issues for the broader society. As cloud services become the underlying infrastructure for more and more Internet based business and public services, daily serving tens of millions of customers and containing their private data, risks associated with failures and breaches – while more manageable due to higher competency levels – become ever more grave.

Extensive lobbying by the ICT industry has sought to establish an image of the proposed data protection regulation as being "too burdensome" for enterprises, especially SMEs providing cloud-based products and services such as apps. Areas in focus are the obligations to provide users notice of data breaches, to gain users' consent for data processing outside of the original agreement, the right to be forgotten, accountability provisions, and more. These are all treated in section 3.5 of this report. On the overall, it is important to take note that this regard for SMEs-as-providers must be balanced against of the above mentioned concerns of SMEs-as-users about security and data protection. Most SMEs are not cloud-providers, but potential users. And under current practices, they stand in a highly uneven position in relation to cloud providers (be they major or minor) with regard to knowledge and the ability to enforce data security. Furthermore, with more and more SMEs adopting cloud services, cloud services enter into the territory of critical infrastructure (Dekker 2012) and as such, into a territory where societal-level demands to uphold certain standards of security is generally accepted. While it is clear that new legislation should not stifle the growth of potentially sound businesses in the cloud industry, the growth of the industry as a whole should on the other hand not be allowed at the

expense of society. The question of who puts burdens onto who should thus be scrutinized carefully before making policy decisions in this area.

3.2.2. Security and privacy for government

Governments stand to harvest many of the same benefits as businesses from the adoption of cloud computing services, but due to the different organisational logics in play in public vs. private organisation these benefits typically play a slightly different role. By adopting cloud technology, CIOs in government organisations are relieved of many routine maintenance operations and thus free to focus on development efforts. Depending on budgetary considerations this may lead either to the slimming down of ICT staff or it may lead to more manpower going into ICT-centred innovation projects. Such saving of cost and effort are magnified when cloud services are adopted uniformly across different organisational units, who would otherwise be carrying out duplicated ICT maintenance procedures. Choosing to implement common cloud solutions can furthermore speed up inter-organisational collaboration as formats and procedures are aligned through the mediation of the commonly used technology. The manpower freed up as routine tasks are outsourced to the cloud provider can, as mentioned, be devoted to already existing ideas for innovation projects. But going even further, government organisations may experience the freedom to more flexibly experiment with new types of cloud services, which are relatively cheap to try and typically easy to implement. With this increased flexibility, innovation in government services becomes easier to implement and a greater confidence in carrying out experiments may take root.

However, due to the often more critical nature of government services, the obligation to reliably meet set quality criteria may – more often than in the case of businesses - outweigh the temptation to enjoy the cost savings and increased flexibility promised by cloud solutions (KMPG 2013). Such considerations also lead government organisations to opt for private or hybrid cloud solutions more often than public clouds. All things being equal, there is a greater degree of (legal) requirements for government organisations to maintain actual control of data security practices and ICT architecture than in the case of private organisations. And minor failings, which might be considered acceptable in connection with the service delivery of some private companies, might in some governmental sectors like energy, health, transport, or defence be entirely unacceptable. This creates an even more pressing need on the part of public sector organisations for quality standardisation and security assurance.

Cloud computing is being adopted by different national governments at different rates. On the overall, the public sectors of industrialized nations lack behind the private sector (KPMG 2013). But some countries are spearheading cloud adoption. One strategy is the creation of dedicated government clouds (or "g-clouds") to provide cloud support for individual government units through some system of centralised provisioning and quality assurance. Countries following this strategy include the U.S., the U.K., France, Japan and Singapore. Another strategy, followed by smaller countries such as the Netherlands and Denmark, is to create commonly strategy for evaluation of cloud offerings and adoption procedures to be implemented locally by individual organisation with the support of one or more centres of excellence in cloud use and implementation. ICT agencies of the Nordic countries have

worked to establish collaboration on potential synergies between cloud adoption in the different countries (TemaNord 2011). A similar transnational approach to governmental cloud strategies is being promoted by the European Commission (the European Cloud Partnership) (COM 2012/529).

The main security concerns with regard to government cloud adoption have to do with the protection of classified or personal data. In the public sector, assessing and establishing security governance measures can be far more complicated than for many private organisations, since legal compliance with data protection legislation at many different levels of governance must be established. Adding cloud solutions with their possible multi-site and multi-national data storage to an already difficult compliance puzzle creates a task of legal compliance assessment, which is beyond the capacity of most individual governmental organisations. Danish and Swedish Danish Protection Agencies have thus recently ruled to stop the use of cloud services by local government organisations precisely due to the lack of established security compliance (Danish Data Protection Agency, decision 2010-52-0138; Swedish Data Inspection Board, decision 263-2011 and follow-up). And symptomatically, while the private cloud provider in the Danish case did in fact provide the required documentation of security practices in order to allow for the assessment of compliance, the local government ultimately chose to abandon the use of the cloud service because of the complications involved. This underscores the need for some central strategy of trail-blazing by centres of excellence or dedicated government agencies to allow for the use of cloud solutions by smaller agencies and organisations. It is also an area in which the question of cloud solutions evolving and entering the territory of critical infrastructure becomes pertinent. Out of government experiences with cloud adoption may arise the need for national and trans-national CIIP overview of cloud adoption strategies (cf. Dekker 2012).

3.2.3. Security and privacy for consumer

From a private consumer perspective, the experience of using cloud services is often indistinguishable from using the broader field of web 2.0 user-content driven websites such as YouTube, Flickr or Picasa or social networking sites like Facebook, Twitter or LinkedIn. Using all of these involves online storage of data and content and possible collaboration with other users. For many services in this broader field, cloud technology does in fact provide the underlying infrastructure necessary to run the online services in question. And historically, it was precisely the massive need for scalable resource to support huge internet services like the Google search engine, YouTube and the Amazon web store, which led to the build-up of server capacity and development of virtualization technology that became the cloud.

Personal services branded specifically as "cloud" can, however, be functionally differentiated from other second generation internet services. Whereas web 2.0 content sharing sites and social network sites are created to share by default, a key point in the business models of these often free services, cloud services are by default private with the option to share.

Personal cloud services provide the ability to store and access data independently of individual computing devices and across different platforms. They ease the hassle of keeping day-to-day information processing routines in order such as note-taking (e.g. Evernote), photo storage (e.g. iCloud), document research (e.g. Endnote, Zotero), document collaboration (e.g. Podium, Basecamp, Google Docs) and many others. The main advantages for individual users of cloud services are mobility, greater flexibility in choice of services, and greater access to products due to their lower costs. Once adopted, cloud services can easily replace many of those applications that come packaged with the operating systems of individual devices. The advent of cloud services may thus prove to move the personal computing market in the direction of a "slim device – big cloud" paradigm, in which computing devices are delivered more or less empty but with easy access to populating it with the user's preferred cloud services (Lo 2013). Some speculate that such a shift may in turn lead to the realization of "cognizant computing" (or smart, ubiquitous computing) in which services will come to function automatically across platforms and devices, indeed across entire ecosystems of ICT devices present in our man-made environment (Gartenberg and Ekholm 2012).

Back in the real world, however, user experiences of cloud services are still very closely connected to everyday use of laptops, smart phones and tablets. Here, personal communication via e-mail, text messages, chat services and social network sites is a core driver for uptake of the devices themselves, while cloud services are often taken on board as an afterthought to maintain an otherwise highly complicated regime of data storage and application updates (Fielder et. al. 2012). In this market, providers which can supply easy integration between different services, such as Google, Microsoft and Apple, have an edge in comparison with single-service providers. Many users' choices of adopting specific services are made on a whim and based on convenience. And as both Google and Apple have proved beyond any doubt, nudging users - through the services they have already adopted - into adopting new ones is very effective. Especially in the case of so-called "freemium" service packages, where users pay nothing to use the service, but accept in return that they may be subjected to different kinds of marketing, the incentive for such nudging is very strong. Usage patterns of individual users show very little awareness of this non-monetary price paid for such services as consumers are generally unwilling to pay for cloud services if similar services are made available free of charge by competing providers (Cattaneo et. al. 2012, 52).

Interconnected freemium services are where the risks of the cloud for personal users come to the fore. In 2012, Google famously changed its privacy policy to cover at once all its services with a unitary consensus form. At the same time, Google provided itself with the privileges of amassing all information stored or gathered for an individual user through these services in one central databank (or cloud). Google argued plainly that this was simply a matter of convenience and of lowering administrative costs. But observers quickly noted that the added marketing value gained by cross-referencing content data and behavioural data across Google's many different services is so high that it raises real concerns about who is providing a service for whom – Google for the user or the user for Google? The European data protection commissioners, led by the French CNIL, said that Google's unified privacy policy was in breach of European data protection legislation and

demanded that Google give users more detailed control over how their personal data could or could not be used. (Arthur 2012). After a subsequent update to the privacy policy meant to allay such concerns, the U.K. ICO acting as spokesperson for the European data protection agencies most recently (July 4th 2013) still believes there are "serious questions" about the legality of the policy and that it still does not give users the sufficiently clear information about the use of their data and threatened to bring formal enforcement action against the cloud provider. (ico.org.uk, july 4th)

The potential threat to users posed by information amassment practices such as those of Google has to do with the links established between user behaviour and marketing efforts. With more and more personal information deposited in cloud services, the potential for analysing preferences and behavioural patterns grows exponentially. Even with existing technology such as search engine selection and presentation of online advertising based on preferences, the potential for manipulation of online behaviour and the influence of users' thinking is vast. From a more futuristic point of view, if such technology was coupled with "cognizant computing" able to track across different ICT platforms and ecosystems the real-time behaviour of people, the age of total behaviour manipulation would indeed be on our doorsteps. The case of Google must in this connection be taken as merely exemplary, the company having in many cases acted as trail-blazer for the ICT industry

Between the practices of private cloud providers and those of the intelligence community, alleged in the PRISM revelations, there are many overlaps, but also fundamental differences. In both cases, the centralisation of data storage allows for massively informative cross-reference analysis of data and metadata. With big data analysis technology, such cross-referencing can be used to predict behaviour with heretofore unimaginable precision. Such analysis can be applied equally well to individuals and groups of people. The main difference lies in the intent, which for the party is advertising while for the other it is to police citizens' behaviour. Private cloud providers operating freemium services aim to target audiences for commercial products and to manipulate their opinion formation and buying behaviour with regard to specific products and brands. Intelligence agencies aim to track and possibly prevent criminal behaviour.

3.2.4. Discussion and conclusions

Security remains a key concern with regard to cloud computing. However, the ability to act on such concerns is very low for individual users and SMEs, who make up the largest potential user groups. Citizens in general remain unaware of the deeper security implications of adopting cloud services, while many SMEs lack the capacity to carry out proper risk assessments. Both groups are in a very uneven position over against cloud providers with regard to knowledge and means for influencing the relation. Large companies and governments demanding greater transparency and more useful contractual arrangements from cloud providers may in some degree act as trail-blazers for the development of societally acceptable relations between cloud providers and users. But self-regulation on the part of industry, such as security standardization, contract standardization and assurance mechanisms, has of yet not been able to deliver an overall image of transparency and trustworthiness. And independent security experts still have substantial concerns with regard to security in the cloud. Societal-level interventions to

establish mechanisms for reliability and trustworthiness in the cloud industry in general therefore seem to be needed to harvest the overall societal benefits, which the cloud could provide to a society that could trust it.

- Societal-level interventions to secure transparent and trustworthy cloud services seem - in the light of failure on the part of industry to reach a satisfactory level of self-regulation - to be needed.
- When considering regulation of the cloud industry, consider carefully who puts a burden onto whom? Regulators onto cloud service providers, or cloud service providers onto users? Decision-makers should be wary of simple images framing a complex issue to the benefit of one societal minority group.
- When debating such regulation, remember that cloud service risks do not apply discretely to the relationships between cloud providers and individual users, but mount and grow to apply to society in the same proportion as cloud technology becomes part of society's infrastructure.

3.3. Data security challenges in Cloud Computing

In the section on impact, some security and privacy issues have already been mentioned, such as:

- A possible increase in security, as Cloud Computing providers may have a much more professional security management than a private user or an SME. Also, backups may be made more systematically.
- A possible reduction in security, as providers may have outages, may fall victim to insider fraud, may have to provide access to data to governments, may not meet European data protection legislation, may do backups irregularly, may disappear from the market, or reuse and resell information.

In this section, we briefly review some main security issues of computing. Those can arise in the three "CIA" subfields of:

- Confidentiality
- Integrity
- Availability

Regarding Cloud Computing, one needs to differentiate between consumers, small and medium businesses, large businesses as well as between using public Cloud Computing or local computing (with virtualisation), including outsourcing and private clouds.

As the review of impacts has shown, for consumers and small businesses using cloud services may mean that their security needs are addressed professionally by the Cloud Computing provider. However, at the same time new risks become relevant:

- A user will depend more on the availability of the network.
- A user will depend more on the confidentiality of the communication.

- A user will depend more on the reliability of the provider regarding keeping confidentiality, integrity and availability high.

In the impact assessment, cases have been mentioned in which cloud services were not available, e.g. Amazon, or in which providers lost data, e.g. in the case of "Sidekick" (Cellan-Jones, 2009). Other cases of potential problems are misrouted Internet communications (BGPmon, 2010) and long-lasting denial of service attacks, as on BASF (RP-online 2011). Regarding availability of services, users may need a backup service, which either means that they use several service providers in parallel, e.g. for service provision or backups, or store copies of data for migration, leading to the issue of having them in a format suitable for processing. The issues of normal backups are considered, e.g. in a Fraunhofer report (Borgmann et al. 2012), who recommend to do local encryption and use several providers. Long-lasting denial of service attacks, providers losing data or going out of business supports the need for backup and local services; as cheap as going Cloud might be, migration to a backup-solution may be needed for any time-critical business.
This section aims at focusing on the most severe issue: Is it possible to keep confidential data, such as business secrets or person-related data, reliably confidential, while processing them in the cloud?

3.3.1. Insider Problem

In this section we do not regard intrusion by third parties, but reading of data by insiders, such as administrators of the Cloud service provider, or governments. A major issue discussed in this field is that foreign, in particular US service providers, and the US government, might spy on confidential data. While legal experts pointed out that regulations in the US and in Europe are rather similar, e.g. regarding making a court decision mandatory ahead of reading data (Maxwell/Wolf 2012), in the US, there are secret courts and other secret procedures, which apparently led to a wide-range evaluation of data: "We know the FBI has issued tens of thousands of ultra-secret National Security Letters to collect all sorts of data on people ... and has been abusing them to spy on cloud-computer users." (Schneier 2013b). Forbes (2012) reported that eavesdropping even takes place on encrypted data. "The NSA saves all encrypted data it encounters; it might want to devote cryptanalysis resources to it at some later time" (Schneier 2013b). Cloud Computing providers are not allowed to inform their customers about any eavesdropping and do not have any logging data available for later clarification, as logging gets switched off (Waldmann 2013). Surveys on impact and media reports show that potential users of cloud services are worried that in particular US entities eavesdrop on their data, see, e.g. Bradshaw et al. (2012, 26), Cashin/Schunter (2011), Vehlow (2011) and Bigo et al. (2012).

It must be mentioned, however, that data stored privately, e.g. on computers owned by users, are not perfectly protected from eavesdropping either, for two reasons.

- There are no provably secure systems. Attackers may exploit vulnerabilities such as zero-day exploits, used prior to antivirus software taking care of them, as in case of the Stuxnet attack (Falliere et al. 2011).

- Hackers may conduct attacks using other means, such as spear phishing, to trick users into executing malware. This happened, e.g., to Coca Cola (Bloomberg 2012), but also RSA was not able to protect itself (Open Hypervisor 2011).

So a particularly high level of confidentiality can be achieved with a very professional, and expensive, local administration of systems, or, ideally, with physically separate systems, assuming that eavesdropping facilities have not been built in in the first place, and that no other means of observation are used. Still, using remote computers, not under the control of a private or business user, poses a particular problem for processing in confidentiality, as both insiders as well as possible governments can read data in the clear. In this section a high-level review of approaches to allow confidential remote computing is therefore provided next.

Tamper resistance

The idea is to use a tamper resistant computer to decrypt data, process them internally, and encrypt the results, for sending them back to the user. For this, a smartcard chip could be used or a somewhat larger hardware security module (HSM). Basically, there is no upper limit to the size, as many devices could be concatenated and as tamper resistant foils could be used, such as a surface enclosure with a sensor layer. Of course, the approach comes with additional costs, but at the same times makes some Cloud Computing-typical savings possible. The tamper resistant module could communicate to the user its brand and trustworthiness, using a remote attestation procedure just like in Trusted Computing. The process is different from typical Trusted Computing with only remote attestation (see, e.g. Curry et al. 2010) in that the tamper resistant enclosure would guarantee the correctness of the system enclosed, based on the module vouching for it, while with a classical Trusted Computing approach, insiders could still physically tamper with the hardware, eavesdrop data, switch logging off, etc. Some researchers stated that tamper resistant hardware is expensive and slow (e.g. Bugiel et al. 2011), but it has not been possible to identify any proof for this.

The approach will only work if there is no hidden functionality. This ultimately means that the whole supply chain used in the tamper resistant modules needs to be trustworthy, from components sourced from a reliable production process, to the operating system used, etc.
The German research project "Sealed Cloud" appears to go into that direction by using sealed racks and volatile memory for reducing options for attacks by insiders (Sealed Cloud 2013). Project Cumulus4j investigates the related approach to decrypt data only in the main memory and with a multitude of keys, to reduce what administrators can learn (Nightlabs 2013). A step to protect keys in a tamper resistant way can be seen in the offering of Amazon to use HSMs for signing and decrypting (Amazon 2013). It can only be assumed that they do not have a channel to read out keys in the clear. A low-tech approach would be the use of a cage. This is of limited value if providers have access to the data and can provide it to government entities.

Relying on tamper resistant enclosures would mean to develop a secure procedure for handing over ownership from one tenant to another. Computers would need to be erased

from customer data ahead of any handover. Solutions would also be needed for issues such as cooling and repair. Such issues should be solvable using Trusted Computing technologies. Such f solutions appear not to be available, nor any estimate of their potential costs. It would be an engineering issue to estimate the costs of a large-scale application of these principles. Also, users would need to trust the messages from a remote secure system.

Principles of Trusted Computing could also be used if a cloud customer trusts the provider, in particular if no insider reading is assumed (CSA 2011, Santos et al. 2009).

Cryptography (Homomorphic encryption)

The key idea with homomorphic encryption is to have a remote computer conduct operations on encrypted data in a way that the user can get results and decrypt them for use (Gentry 2009). It has been reported that this works with about 1 bit per second and that the speed is likely be remain low for the next decade (Henrich 2012). Another issue with this approach is that several users may wish to use remote data, e.g. in the design of components for new cars. Hence multi-party computations would be needed. These approaches are research issues with promising, but unclear outcome.

3.3.2. General Quality of Service Problem

Beyond the most difficult problem of insider access, Cloud customers who do not have such worries still need to inform themselves what quality of service is offered by a provider. This applies to the general quality of operation, such as anti-virus updates, intrusion testing, backups, downtime etc. In detail, this is a difficult issue as, e.g. often virtualization is used to keep customer data separated. However, any of today's large system contains errors (Marnau et al. 2011), and Ristenpart et al. (2009) demonstrated that side-channel attacks are possible to intrude one virtual machine from another one. If a European customer wishes to have personal data processed, the issues is whether a provider complies with European legislation, whether processing is done in the EU or Safe Harbor rules can be applied (cf. Berry, Reisman 2012; Article 29 Data Protection Working Party 2012).

Some of these issues can be dealt with certification. An auditor can state that a provider manages servers well, complies with legislation, that there is evidence for the application of Safe Harbor rules, etc. Such auditing may need to be done often, if not permanent. Therefore costs of certificates may be in the order of €1 million. Still, if governments or insiders switch logging off, or if providers send fake records to the secure logging memory, the records to be audited will be incomplete. Also, as no proven systems exist, breaches may happen nevertheless. Yet, certifications may confirm that a certain quality level has been observed. For instance, for public institutions using a certified service provider may be useful. An important issue is whether service providers take over liability for breaches, even if they have been certified.

As current systems do not have a proven base, development of a highly secure computing base as well as high-quality applications would make sense. A similar effort is undertaken by the US DARPA agency in its "Crash" program (DARPA 2013). In a prior STOA-project,

Heiser presented how a secure kernel could be built and its use made mandatory for government services (Heiser 2013).

3.3.3. Conclusions

It appears that today, there are no proven, reliable technical methods to allow confidential remote processing of data, without any known ways of eavesdropping by insiders. However, users often trust a certain service provider nevertheless, in particular when balancing the risk of trusting something remote against the need to trust components anyway as well as local staff. Still, a high assurance level of technically confidential remote computing could significantly boost the use of Cloud Computing. Note that all of the above potential means would in the end need to be implemented properly, which will require secure systems, such as trustworthy hardware, error-free operating systems, protection against side-channel attacks, and high-quality applications.

Conclusions and resulting options are:

- support measures to provide awareness of the problem of insider reading and of the technical approaches towards solutions, e.g. by producing communications or conducting workshops.
- support the development of secure servers, reliably protected against attacks (Heiser 2013).
- support research on technical measures against insider reading and their cost efficiency.
- consider taking steps towards incentives for use of those new approaches, provide recommendations or even request mandatory use, to trigger the emergence of products as well as to encourage their use once they will be available.
- support measures to achieve certification at a lower level, certifying, e.g. that a provider complies with European legislation, that processing takes place only in the EU, that a provider has a certain level of auditing, or that a provider takes responsibility for breaches.
- support steps to achieve that Cloud Computing providers which operate solely under European jurisdiction play an increasing role (Bigo et al. 2012).
- make it mandatory to notify consumers when a law enforcement request has been made (Fielder/Brown 2012).

On a different level, the technical approaches and the above options should be discussed at the planned project workshop.
As briefly mentioned, to assure availability, businesses may need to move to a second or local service provider at any time.

3.4. Cloud computing, privacy and the EU data protection regime

The processing of data is a double edged sword. On the one hand, it is necessary for the function of information societies. On the other hand, the ability to collect and process data is a powerful tool for interacting with individuals and shaping social relationships. Accordingly, data processing can pose a threat to the fundamental rights of the individual whose data is processed – particularly the right to privacy. The necessity to reconcile these two – apparently competing – dimensions, led to the creation of European data protection

law. This area of law is predominantly elaborated by the overarching piece of legislation: Directive 95/46.

The Directive applies to any processing of 'personal data' (with certain exceptions and limitations). In Article 2(a), the Directive provides a definition for personal data: ''[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.(Directive 95/46, Article 2) In essence, the concept of personal data is engaged whenever data, or a combination of sets of data, reveal information about a specific, identifiable, person – the 'data subject'. The Article 29 Working Party elaborate 3 ways in which data can be said to relate to an individual; content (what information the data contain), purpose (what the data are to be used for) or result (that the data processing will have an effect on an individual's rights or interests).(Article 29 Data Protection Working Party 2007, 9-12) As a vast number of cloud services rely on the processing of 'personal data', they fall under the scope of data protection law.

However, the Directive was drafted according to a specific perception of the data processing environment it aimed to regulate. This environment was categorized by limited numbers of actors, engaging in easily identifiable and easily locatable, data processing. The networked, continuous nature of cloud processing challenges this conception of the processing environment and accordingly poses challenges to the application of the Directive.

This contribution has the following structure. In section 3.3.1., we briefly explain the structure and function of the current data protection framework as elaborated by the Directive. In section 3.3.2, we elaborate on the difficulties faced in applying the Directive to cloud processing – a processing context for which it was not necessarily created. We consider in particular the following: the difficulty of clearly establishing the application and supremacy of European data protection law; the difficulty in identifying actors and allocating them roles and responsibilities; the difficulty with transferring data outside the EU; the difficulty in harmoniously adapting data protection law to deal with technological challenges. In section 3.3.3 we then look toward the future of European data protection, introducing the data protection reform programme and the proposed Data Protection Regulation. Finally in section 3.3.4., we discuss how the features of the Regulation may address the challenges pinpointed in section 3.3.2. and how these changes may impact on cloud computing.

On the one hand, there are numerous different types of cloud service. On the other hand, data protection law is extensive and complex. Each cloud service raises specific questions and challenges in relation to data protection law, whilst each aspect of data protection law in turn could be extensively evaluated for its specific applicability and relevance to cloud computing. This contribution does not enter into considering the problems raised by each specific cloud service or engage with the detail of applying each aspect of data protection

law, but remains on an abstract level, addressing the general challenges posed by cloud computing to data protection law.
Certain sectors processing data – for example the police – are subject to specific laws. The interaction of each of these areas of law with cloud computing also raises important issues. This contribution will focus on generally applicable data protection law – as elaborated by Directive 95/46.

3.4.1. What is Data Protection – Directive 95/46

Data protection is a fundamental right as laid out in article 8 of the charter of fundamental rights of the European union.[1](European union 2000/C 364/01, Article 8)

Data protection law is the field of law which elaborates this right by governing the legitimate use of data relating to an identifiable individual ('personal data'). The current piece of legislation giving overarching practical expression to data protection law is Directive 95/46.(Directive 95/46/EC) Beneath the Directive however, lies a range of subordinate regulation – for example, certain sectors are subject to specific regulation clarifying data protection rules, for example the telecoms sector – the ePrivacy Directive.(Directive2002/58/EC)

The scope of application of the Directive is wide. It applies to almost all data which can be connected to an identifiable individual, to almost all electronic operations concerning this data and can be relied upon against any entity or individual conducting the processing of personal data. Accordingly, whenever personal data are processed in the cloud, data protection law will be relevant. The Directive is limited in its application, however, by qualifications of geographical scope. It may not apply to certain processing actions occurring outside EU territory. It is also limited in application by the former pillar structure of the union, which means that it will not apply to much police use of data.

From the 1980s on, member states began to draft data protection legislation. This legislation followed from the recognition that the processing of data could have a significant impact on fundamental rights but that data processing was a vital part of the functioning of modern economic and social systems. The aim of these regulations was, accordingly, to protect fundamental rights (predominantly privacy), while allowing necessary processing of data. Data protection rules at European level followed the presumption that the divergence in data protection legislations between European states would act as an obstacle to the flow of data between member states – which was seen as central to the efficient functioning of the internal market.(Mayer-Schönberger 1997, 229-235) Accordingly, the Directive was drafted with dual goals. These are directly recognised in Article 1, 'in accordance with this directive, member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.... member states shall neither restrict nor prohibit the free flow of personal data

[1] One can consider the right to data protection as a transparency right. '*[T]ransparency [rights]*…come into play after normative choices have been made, in order to channel the normatively accepted exercise of power through the use of safeguards and guarantees in terms of accountability and transparency'. This form of right is to be juxtaposed to opacity rights – such as privacy – which seek to provide prohibitive, substantive protection and which outright define whether an interference with the individual is acceptable.(Gutwirth et al. 2011, pg 8)

between member states for reasons connected with the protection afforded under paragraph 1.'(2002/58/EC, Article 1)

In the case of cloud computing, both legislative aims come into play. On the one hand, cloud computing is seen as a key factor in the development of the European economy. Accordingly, it is essential that cloud services are not obstructed from developing or unnecessarily hindered by unnecessary or burdensome regulation. On the other hand, there is no reason that data subjects should be subject to reduced standard of data protection simply because data is processed in the cloud.(European Commission 2012c, 6-8)

The Directive functions first by isolating actors, to whom responsibilities and rights can be allocated. Three actors are key: The data subject (to whom data pertains), the data controller (who controls and defines processing) and the data processor (who processes data on behalf of the controller).

The directive then lays down obligations to the data controller and processor for the legitimate processing of data. Generally speaking, the controller is expected to process data only when a legitimate ground for processing exists (as laid out in article 7 for normal data and article 8 for sensitive data), for example if that processor has received the consent of the data subject (although this is not the only possibility). Further, in the processing of data, the controller is expected to follow a set of rules for fair processing (laid out predominantly in article 6) – for example the processor must make sure the data are accurate and up to date, that the purpose of processing is specific and legitimate, and that the data collected is adequate, relevant and not excessive in relation to the purpose for which it was collected.(Directive 95/46/EC, Articles 6, 7 and 8)

In turn, the data subject is invested with a series of rights – including the right to be informed about the processing of his or her data and the right to inspect or correct data being processed. The controller must make sure these rights are available and accessible for the data subject. The data subject does not always have the right to stop processing.

In certain processing contexts, special provisions are engaged. For example if a controller wishes to transfer data outside the EU, they will be obliged to follow the special guidelines related to transfers to third countries laid out in Articles 25 and 26.(Directive 95/46/EC, Articles 25 and 26)

Rights and obligations are combined within the directive to create a system under which data processing is not negatively prevented, nor is the data subject invested with a dominant right to informational self-determination. Rather, it constructs a legal framework according to which individuals' personal data can be processed provided that a certain set of rules and principles are followed. As put by de Hert, "[the data protection framework] relates to procedural justice and to the correct treatment of, and explanation to, registered citizens with the intention to increase their willingness to accept a system in which others (government agencies, companies, private citizens) have the right to process 'their' data and take decisions that have an impact on their self-determination where information is concerned".(De Hert 2009, 17)

Accordingly, when we talk of 'challenges' to data protection laws, we talk of data processing contexts in which the systems and definitions which make up data protection law, seem of diminished ability to achieve either one, or both, of the specified legislative aims.
Challenges can arise as technological development changes the possibilities and context of data processing, thus bringing into questions the presumptions on which the data protection framework was based. One may view cloud computing as just such a technological development.

The Directive was drafted according to a specific perception of the data processing environment it aimed to regulate. This environment was categorized by limited numbers of actors, engaging in easily identifiable and easily locatable, data processing. Cloud computing, on the other hand, is categorized by continuous, networked, processing, which may be very difficult to geographically locate.(Article 29 Data Protection Working Party 2012, 4-6) Accordingly, where the function of the Directive revolves around the assumptions listed above, its relevance in relation to cloud computing can be challenged.

Broadly speaking, we can consider four key areas of challenge. 1. The scope and jurisdiction of the Directive is geographically specific. Therefore, cloud computing poses challenges in light of scope and jurisdiction. 2. The definition of roles and responsibilities in the Directive (which are core to ensuring accountability and the protection of rights) was predicated on a limited number of actors engaging in limited transfers. Cloud computing thus poses challenges to these definitions and allocations of responsibility. 3. The Directive defines one set of provisions for data transfer within Europe, and another set of provisions for data transfer outside Europe. These provisions are geographically specific and reliant on the presumption of limited and easily definable data transfers. Therefore, cloud computing poses challenges to these provisions. 4. Challenges 1 to 3 have remained problematic for data protection law as the Directive did not have the inbuilt mechanisms to adapt to the novelty of cloud computing. Cloud computing thus challenges the Directive's general ability to adapt to novel technological challenges. Each of these challenges will be dealt with in turn.

3.4.2. Challenges of the Cloud to the Current Data Protection Framework

Definition of Applicability of European Data Protection law and Jurisdictional Issues

The first form of challenge posed by cloud computing to data protection law is that of jurisdiction. In a number of cloud services, the physical location of the data, or the service requested, may not be known to the client, or even to the initial cloud provider. Indeed the provision of cloud services could take place across multiple jurisdictions simultaneously. In fact, information as to the location of the data, or of the data processing activity, may be irrelevant to the provision of the service.

However, this information is not irrelevant in the definition of whether, and how, European data protection law applies. In establishing the applicability of European data protection law certain 'territorial' criteria determining jurisdiction must be met. These are elaborated in

Article 4, which states that EU data protection law applies to activities of the controller – there is no mention of the processor – which is a) is established in one or more EU Member States or b) utilises equipment based on the territory of a Member State. If these criteria are not met, European data protection law does not apply.(Directive 95/46/EC, Article 4)

If these jurisdictional criteria are not suitable to ensuring the application of European data protection law, European citizens' personal data may be processed without engaging the data protection framework. Cloud computing poses this problem.

First, in the case of cloud computing, the cloud provider may often be recognized as the data processor, rather than the data controller, despite having significant control over the means of processing. The lack of reference in Article 4 to the processor may lead to situations in which the criteria of Article 4 are not met, despite the logic for the application of the Directive being present.

Second, in the case of non-EU controllers, the definition of 'equipment' becomes key to defining the applicability of European data protection law. The concept of 'equipment' arises from a context in which data processing was done with identifiable and tangible processing 'equipment'. Cloud processing makes this concept very difficult to apply. First, in networked processing models where processing can be located across numerous actors, defining the location of the 'equipment' used may be practically impossible. Second, in cloud processing, even the idea of 'equipment' – regardless of how broadly defined - may fail to describe encompass the combination of infrastructure and data flows through which cloud service provision is achieved. (European Data Protection Supervisor 2012, 10-11)

Even where the question of application of European data protection law is unproblematic, this does not rule out a conflict of laws arising. Data controllers operating outside the EU may/will also be subject to the laws of the states in which they operate. These laws may also set out a number of obligations on the data controller – for example to turn over certain forms of data to local authorities. These obligations may stand in contrast to the rights of the data subject, or the obligations of the data controller laid out in European data protection law.(Bigo et al. 2012, 44)

In relation to controllers established in multiple states in the EU, there may also be problems in determining which Member State's law is applicable. Directives are specific legal instruments which allow Member States to choose the means and form of their application in national law. This has meant that there are differences between national laws. As interpretation of national laws also happened at national level, there can thus be a significant divergence in relevant rules.

Finally, the effectiveness of data protection law relies on the possibility for independent oversight to ensure that data protection rules are followed. Even where the question of application is unproblematic, the location of a data controller outside the EU may make oversight or investigation into a violation of the rules of data protection, or punishment for these transgressions, impossible.

Definition of Roles and Responsibilities

The data protection framework relies on categorizing entities involved in data processing as specific sorts of actor. Each form of actor then has roles and responsibilities in ensuring that the requirements of the Directive are fulfilled. Without a clear definition of these actors, there can be no clear allocation of responsibilities. In turn processing may become intransparent or unaccountable. Consequently, it will become very difficult for the data subject to rely on their rights in relation to processing and it may become difficult to conduct meaningful oversight or supervision of the processing operation.

There are three key actors defined in Article 2.
The data subject is the identifiable natural person to whom any personal data relate (Directive 95/46/EC, Article 2(a)).

The data controller is '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' (Directive 95/46/EC, Article 2(d)). The controller is predominantly responsible for making sure that data processing operations are in compliance with data protection law and that obligations toward the data subject are made a reality. In terms of data processing in the cloud, the cloud client is generally held to be the data controller.

The data processor is 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller' (Directive 95/46/EC, Article 2(e)). In the cloud, the service provider is held to be the data processor (Directive 95/46/EC, Article 2).

Although there is guidance available on the application of these definitions in the cloud environment – for example the cloud client is generally held to be the data controller whilst the cloud provider is generally held to be the data processor – in reality, it can be difficult to identify each actor.(Article 29 Data Protection Working Party 2012, 7-10)

It is primarily in the definition and delineation of the roles of data controller and data processor that problems arise.[2](Kuan Hon et al. 2012, 3-13) It has been also been suggested that the provision of cloud services has become so advanced, that it is no longer possible to describe the cloud client as necessarily being in charge of the essential 'means' of processing.(European Data Protection Supervisor 2012, 12) Whilst the cloud client may be able to fulfil certain of the duties of the controller – for example ensuring the initial accuracy of data – other duties traditionally allocated to the controller may be more clearly located with those who would, under the rules laid out by the Directive, be conceived of as

[2] In relation to the definition of the data subject, the challenges posed specifically by cloud computing are generally minor. However, it has been suggested that the limits on the concept of personal data to generally refer only to 'natural', as opposed to 'legal' persons, could be a beneficial extension of the scope of data protection law relating to the cloud.

processors – for example, ensuring 'appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction'.(European Parliament/ European Council 1995, Article 17)

Even when roles are specifically allocated – for example in a contract between cloud client and provider – these may not match the reality of control. In cloud service contracts, there is often a power imbalance between contracting parties. The cloud client may not have the ability to negotiate terms of service – for example when standard contracts are used – or may be in a weakened negotiating position. In this case the distribution of roles and responsibilities may be unsuitable for the cloud client's activity or be practically impossible to execute.

Worldwide and Continuous Data Transfer (Data Transfers Outside the EU)

Cloud service providers may utilise infrastructure and sub-contracted providers located in multiple geographical locations. In turn, there may need to be the facility to make data available for the cloud service user to access data irrelevant of location. Accordingly, cloud service providers may rely on continuous, worldwide, flows of data. Where the cloud provider, infrastructure, or client, is EU based, this will necessitate data transfers of personal data from within, to outside, the EU.

In order to ensure that citizens' data remain protected even when transferred outside the EU, the Directive imposes certain restrictions on transfers. The Directive lays out a number of possibilities for the legitimate transfer of data to third countries.

First, data may be transferred to outside the EU should the Commission decide that the legal framework in the third state provides an 'adequate' level of protection (Article 25). The EU-US Safe Harbor scheme also belongs under this category. US companies which certify that they adhere to certain data processing principles are viewed to offer adequate protection and may thus have data transferred to them.(Directive 95/46/EC, Article 25)

Second, the Directive allows transfers to third countries to take place should they fall under any one of a list of exceptions to the general prohibition on transfer (Article 26(1)). (Directive 95/46/EC, Article 26 (1))

Third, transfers may take place provided that it is subject to a contract between two controllers or a controller and a processor. Contracts must stipulate that data protection principles are to be followed in any processing operation (Article 26(2)). If cloud provision involves a longer chain of supply, each contract between further processors should ensure the same level of protection.(Directive 95/46/EC, Article 26 (2))

Fourth, transfers may occur based on Binding Corporate Rules. These rules define standard data processing practise within a company or group of company operating multinationally.(Article 29 Data Protection Working Party 2013)

However, the Directive was drafted with the presumption that international transfers would be limited, linear and easy to track. Accordingly the application of each of these options has drawbacks when applied to the networked environment of the cloud.

First, only a very limited number of countries currently qualify as 'adequate'. The conduct of an investigation into the 'adequacy' of a state's laws can take significant time and only a certain, limited, number of 'adequacy' investigations are foreseen each year. Until adequacy has been confirmed, transfers cannot legitimately be made to that country on this ground. Further, as adequacy findings are limited in geographical scope. This means they may not be suitable to legitimate all transfers within an international cloud environment. The Safe-Harbour agreement suffers not only from the above territorial limitation, but also from a lack of oversight and enforcement mechanisms. The fact that companies are permitted to self-certify under this arrangement raises issues as to the protection it offers European citizens' in fact.

Second, whilst it may appear that a number of the exceptions laid out in Article 26 may be applicable to cloud computing, the Article 29 Working Party – the primary group responsible for interpreting data protection rules at European level – have concluded that Article 26 exceptions may only be relied upon in the case that data transfers are neither recurrent, nor massive or structural – criteria under which most cloud services can be seen to fit.

Third, Binding Corporate Rules, whilst offering a good solution when processing remains within a certain organization, are of less relevance should processing take place across multiple companies.

Finally, the only way for contractual clauses to certainly meet the requirements of the Directive is for them to be standard contractual clauses as clarified by the Commission (although there is some small room for cloud providers to tailor these according to necessity and experience). There are only a limited number of standard contractual clauses and these have been tailored for certain situations. Considering the growing variety of cloud services and their constant development, it is uncertain as to whether pre-approved standard clauses will always be applicable. There are no standard clauses, for example, aimed at the transfer of data from a processor within the EU, to a processor outside the EU. The use of standard clauses outside the situations they were designed for may result in irrelevant, unfair or impossible distributions of responsibility.(European Data Protection Supervisor 2012, 16-20)

No Binding Interpretation Mechanism

The challenges in applying the Directive to cloud computing were caused partially by the fact that cloud computing represented an alteration in the way data was processed. They remained challenges due to the fact that data protection law did not have the capacity to effectively adapt to these changes (COM 2010/609/EC, 1-4).

Whilst this was partly due to the rigidity of the terms and concepts of the Directive itself, it was also due to the fact that the mechanisms foreseen for interpreting the Directive at European level were weak. Although there is a European level body responsible for providing European level interpretation – the Article 29 Working Party – its guidance is not binding.

Although interpretation can happen at Member State level, the power of the national data protection authorities was limited and national level interpretation had the counter-productive effect of leading to divergent approaches across Member States – fragmenting the European data protection law.

3.4.3. Data Protection Reform and the Data Protection Regulation

Since the drafting of the Directive, there have been significant changes in the regulatory landscape. The technological background to the drafting of the Directive has changed. The speed, scale and mobility of data collection and sharing have increased tremendously, while data processing has gained significance in defining the relationship between individuals and social and economic entities.

The legal context has also changed. The use of a Directive as the instrument of regulation was seen to have failed in its goal to harmonize protection standards. Equally, the Directive is no longer seen to reflect the European legal architecture of which it forms a part. The signing into force of the Lisbon treaty represented a moment of particular importance. In particular, Lisbon elevated the European Charter, which specifically lists data protection as a fundamental right, to the highest status of EU law.(COM 2012/0011/EC (COD), 1-2)

Accordingly, in 2009, the Commission began an investigation into the reform of data protection regulation. This process of consultation and reform was punctuated by two key pieces of documentation. First, the 'Communication on a comprehensive approach on personal data protection in the European Union' in November 2010 – broadly detailing areas of concern and points of reform.(COM 2010/609/EC) Second, the 'Proposal for a Regulation…on the protection of individuals with regard to the processing of personal data and on the free movement of such data' in January 2012 – representing the culmination of the reform process and intended as a replacement to Directive 95/46.(COM 2012/0011/EC (COD))

At each step of the process, the challenges posed by cloud computing were noted as key factors driving, and to be addressed by, the reform – with cloud computing being mentioned 22 times in the Impact Assessment conducted prior to the Regulation.(European Commission 2012a)

The overall goals of the proposed Regulation remain essentially unchanged from those of Directive 95/46. The new Regulation still essentially seeks to protect the rights of the data subject and to guarantee the free flow of data between Member States. However, considering the new legal positioning of data protection within the EU *aequis*, the focus has shifted comparatively toward the protection of the citizen. The choice of a Regulation

means that the proposed framework will be directly applicable in all Member State legal systems – no need for national transposition.

In structure and content, the prevailing mood is also that of continuity. In structure, the Regulation still aims at the provision of procedural justice through a framework in which different interests can be evaluated and balanced. In content, the Regulation retains all the concepts and principles and many of the definitions, which defined Directive 95/46.

Despite general continuity, there is innovation. On the one hand, this manifests in the strengthening of the pre-existing rights of the data subject – for example in an increased focus on transparency and a clarification of uncertain concepts, such as 'consent' – and in alleviating the administrative burden on the data controller and replacing it with a heightened responsibility requirement – for example with the introduction of the principle of accountability and a reduction in notification requirements. On the other hand, certain specific innovative features have been introduced – for example the introduction of privacy by design principles, the right to be forgotten and the right to data portability.

It is important to note that our point of reference is the current draft of the proposed Regulation. This is only the first draft in a legislative process which may undergo significant change. The Regulation is currently being debated and will be subject to a continued process of revision – being passed back and forth between Commission, Parliament and Council before final adoption. At the moment, the draft is awaiting a final vote before the European Parliament – with over 3000 amendments from the current draft having been proposed. It is unsure when the new legislation will finally enter into force, or which changes it will undergo before that point.

3.4.4. Data Protection Reform and Cloud Computing

Clarification of Scope and Applicability of European Data Protection Law

The Regulation goes beyond the Directive and introduces two novel concepts which will serve to both clarify the application of data protection law, and to broaden its territorial scope. This is aimed at ensuring that the processing of EU citizens' personal data is always subject to EU data protection standards.

First, in Article 3, the Regulation clarifies that even the establishment of a processor on Member State territory will trigger applicability. Given that the cloud provider may be regarded as the data processor, this clause will remove any doubt as to the application of the Regulation to any cloud service in the situation that either cloud client or cloud provider is established inside the EU.

Second, also in Article 3, the Regulation clarifies that 'offering goods or services to' or 'monitoring the behaviour of' data subjects inside the EU, will also trigger applicability. In the event that the cloud provider is established outside the EU, the fact that they offer cloud services to data subjects within the EU will mean that EU data protection rules could apply.(COM 2012/0011/EC (COD), Article 3)

It has been observed, however, that many cloud providers located outside the EU do not target services at individuals, but rather at businesses or organizations. A strict interpretation of Article 3 would mean that the Regulation would not apply to such providers – only a natural personal can qualify as a data subject. However, the fact that the cloud client was a business or organisation would not necessarily mean that the personal data of EU data subjects were not being processed. There have been suggestions that the language of the Article should be changed to extend the scope of the Regulation to cover this situation.(European Data Protection Supervisor 2012, 11)

Equally, simply extending the scope of application of the Regulation does not necessarily ensure compliance or ensure that European data protection law will be followed if this conflicts with other states' laws.

Finally, clarification of questions of applicability, do not resolve issues relating to the transparency of extraterritorial processing operations or to the supervision and enforcement of extraterritorial controllers or processors.

Clarification of Roles and Responsibilities

The Regulation aims to readjust the definition of actors and roles. Changes focus primarily around attempts to more clearly locate the actor which truly 'controls' processing, as data controller.

First, in Article 4(5), the Regulation states that 'the controller [is he/she who] alone or jointly with others determines the purposes, conditions and means of the processing'.(European Commission 2012b, Article 4 (5)) The Regulation thus introduces the idea that controllership can be determined through control over the conditions' of processing. The EDPS suggests that this would allow controllership to be allocated more easily to the cloud provider – as the entity which creates the conditions of processing'.(European Data Protection Supervisor 2012, 12-14)

Second, in Article 24, the Regulation clarifies that, should there be more than one identifiable controller, there must be an arrangement made between the controllers so as to ensure data protection rules are followed and data subjects' rights are guaranteed – accountability and responsibility arrangements must be made clear and transparent.(European Commission 2012b, Article 24) As the cloud client is normally regarded as the controller, any definition of cloud provider as controller will lead to this situation of joint-control. The Regulation confirms that any arrangement establishing joint control ought to distribute responsibilities in line with the reality of control over processing. This should ensure not only that data subjects' rights are effectively protected, but that responsibility for ensuring their protection lies with the best entity best placed to do this.

The EDPS notes, however, that there may still be imbalances in power between cloud provider and cloud client. These imbalances may still prevent a balanced and accurate distribution of responsibilities. The use of standard contractual clauses is proposed as a

solution, but these will not always be relevant.(European Data Protection Supervisor 2012, 13)

Following a more targeted allocation of roles, the Regulation – in Article 22, directly – also generally increases the responsibly and accountability of data controllers and processors. In this regard, the Regulation also introduces a number of novel requirements which will be of relevance to cloud services. For example, the controller will now be obliged to follow privacy by design principles (to integrate privacy and data protection into the design and deployment of technologies and organisational systems) (Article 23), to implement data security measures to ensure that data are adequately protected (Article 30) and, in certain cases, to conduct a data protection impact assessment to isolate and minimize privacy and data protection risks in advance (DPIA) (Article 33). Should there be a breach of data security, the controller will be obliged to inform the data subject under the data breach notification rules (Articles 31 and 32).(COM 2012/0011/EC (COD), Articles 22, 23, 30, 31, 32 and 33)

The controller will also be responsible for making a novel set of data subject rights a reality. The right to data portability (the right to transport data across comparable services – Article 18) and the right to be forgotten (the right to have data erased when processing is no longer required/no longer legitimate – Article 17) are perhaps the most likely to be important. The relevance of certain of these novel rights to cloud computing scenarios will be expanded upon below.(COM 2012/0011/EC (COD), Articles 17 and 18)

Whilst these novel accountability and responsibility requirements have been positively received, there have been doubts raised as to their efficacy and practicality. The lack of clarity in relation to what these requirements mean in practise may lead to a situation in which each data controller defines for themselves whether they have fulfilled their obligations. Accordingly, obligations may have been met on paper, but not in reality. Key to success will be the clarity of the interpretative work which will follow the adoption of the Regulation.

International Data Transfers

The Regulation still imposes limits on the legitimate transfers of personal data outside the EU. However, whilst maintaining the options listed in the Directive, the Regulation also proposes certain changes aimed at maintaining protection for data subjects, whilst loosening the formalities which could make it difficult for cloud providers to operate in line with data protection law.

First, the regime proposed in the Regulation demands that both controllers *and processors* secure legitimation for transfers (Article 42(1)) (COM 2012/0011/EC (COD),Article 42 (1)).

Second, in Article 42, the use of contractual clauses to legitimate data transfer is elaborated. The possibility to use standard clauses remains – although these are still limited in number and applicability. However, in Article 42(2)(d) the Regulation also legitimizes the use of 'ad hoc' contractual clauses. These are 'contractual clauses

[concluded privately] between the controller or processor and the recipient of the data'. Although these clauses must be checked and authorized by the relevant supervisory authority according to Article 34(1) and would be subject to minimum guarantees, their presence in the Regulation will introduce considerable flexibility. Controllers would no longer need to rely on template standard clauses drafted by the Commission – which could be partially, or fully, unsuitable. (COM 2012/0011/EC (COD), Article 42(2)(d) and Article 34(1))

Finally, in Article 43, a detailed mechanism for the use of BCRs is specifically elaborated (not the case in the Directive). Although BCRs were originally designed to facilitate international transfers intra-group, Article 43(2)(c) innovatively allows the extension of BCRs to external sub-processors. This may prove useful for numerous forms of cloud computing. It must be noted however, that the specifics of BCR application to external sub-processors requires further clarification.(European Commission 2012b, Article 43)
There are however, certain criticisms of the approach elaborated in the Regulation. First, whilst the Regulation may aim at greater flexibility, many of the mechanisms for allowing international transfers still require prior confirmation from the Commission – for example adequacy rulings and standard contractual clauses – whilst others will require significant interpretation or elaboration before they become effective – for example, BCRs relating to external sub-processors. How successful these aspects of the Regulation are, will depend on how effectively and quickly implementing work can be carried out.

Second, the Regulation still relies on the concept of a data 'transfer' to engage the necessity to legitimate data flows outside the EU. There is no clear definition of 'transfer' in the Regulation. The EDPS suggests that this may be problematic in networked cloud environments, in which data is not only being actively transferred, but may also be being made available, to numerous countries simultaneously.

DPAs and Binding European Interpretation

The Regulation introduces a number of features aimed at ensuring legislative flexibility and European level harmony. These changes are designed so that the Regulation may adapt to future developments in data processing – for example, future developments in cloud processing.

First, the Commission retains specific power to specify and clarify the meaning and application of a number of concepts and definitions. The legal instruments used to do this are delegated and implementing acts and are listed in Articles 86 and 87. The use of these powers will allow the Commission to directly offer central, and binding, guidance on how to apply the Regulation to novel situations of data processing. It must be noted however, that the quantity and role of delegated and implementing acts imagined in the Regulation has come under heavy criticism.

Second, the Regulation imagines a central, binding, mechanism for the resolution for the interpretation of the law. This can be used when there are disagreements between DPAs as to the approach to be taken regarding interpretation of data protection law, or when novel

challenges arise. This mechanism is referred to as the consistency mechanism and is laid out in Articles 57-63.(COM 2012/0011/EC (COD), Articles 57-53)

Novel Data Protection Mechanisms in the Regulation

In addition to the changes elaborated above, the Regulation introduces certain other innovations. Whilst these innovations do not necessarily follow from the challenges cloud computing poses data protection, certain of them may have implications for the provisions of cloud services. The most relevant of these are elaborated below.[3]

The Right to be Forgotten (Article 17 of the Regulation)
The right to be forgotten is not totally new and can trace its roots to the right to erasure in the Directive. However, the right as it appears in the Regulation is considerably stronger than its predecessor. Article 17 gives the data subject a; 'right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data' if that controller no longer has a legitimate reason to retain the data. In this regard, Article 17 makes the controller responsible not only for deleting data, but also for taking 'all reasonable steps…to inform third parties which are processing such data…to erase any links to, or copy or replication of that personal data'. This will place a heavy burden on any cloud provider (or client) deemed to be processing personal data (COM 2012/0011/EC (COD), Article 17)

There remain, however, a number of uncertainties associated with Article 17. Practically, it may be technically difficult, or impossible to comply with the provision. Equally, it may be impossible to define and contact all parties who may have copies of the data. In these situations, what the controller must do to discharge their obligations is unclear. On a more theoretical level, the ideas and thresholds within this right remain unclear. Perhaps most importantly, what does 'all reasonable steps' encompass? How far will data controllers need to go to fulfil their obligations under this Article? Finally, it is unclear what the obligations of the third parties are – given that they have been informed of the request to delete by the data controller, must they follow this request?

The Right to Data Portability (Article 18 of the Regulation)
Article 18 represents one of the truly innovative features of the Regulation. In Article 18(1) the data subject is given the right to 'obtain from the controller a copy of data...in an electronic form which is commonly used and allows for further use by the data subject'. In Article 18(2) the data subject is given the right 'to transmit those personal data and any other information provided by the data subject and retained by an automated system, into another one, in an electronic format which is commonly used'. This right will have significance for cloud services – particularly those who use proprietary/unique data formats - as it will require the service to be able to provide a copy of that data in a transferrable format. In this regard, Article 18(3) states that: 'The Commission may specify the

[3] It should also be noted that, due to their novelty, the precise application and consequence of these provisions is still unclear and that they are likely tob e subject to considerable debate in the current legislative process – their final form may thus differ from the form commented upon in this contribution.

electronic format referred to in paragraph 1 and the technical standards and modalities pursuant to paragraph 2'.(COM 2012/0011/EC (COD), Article 18)

Once again, however, there are a number of uncertainties related to the Article. Importantly, the relationship between Article 18 and other Articles allowing the data subject to obtain information related to data processing and deletion requires clarification. The Article has also been subject to certain criticism. For example, it has been suggested that the Commission is not best placed to determine the specificities of a commonly used format. Indeed, it has been suggested that the central regulation of a commonly used format would be problematic in relation to the principle of 'technological neutrality' on which data protection law supposedly stands.

Data Protection by Design and Default (Article 23 of the Regulation)
Article 23(1) states: 'Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for the processing and at the time of processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'. This Article has explicitly created an obligation on the controller to take data protection rules and principles into account at each step in the technical design and deployment of a data processing system. It also requires that data protection principles are taken into account in the development of organisational systems supporting and surrounding data processing. Article 23(2) follows this up with a further obligation: 'The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose…and that personal data are not made accessible to an infinite number of individuals'. This Article has created the obligation for controllers to ensure that, in any instance where a technology could be privacy infringing, the minimum possible level of privacy infringement is set as the default.(COM 2012/0011/EC (COD), Article 23)

These provisions are not directly targeted at software or hardware designers, or at other links in the cloud service deployment chain. However, as controllers will be under an obligation only to use and deploy services which allow them to adhere to their obligations under Article 23, it would seem likely that 'obligations of controllers are likely to create some incentives for the market of relevant goods and services'. Equally, the provisions are not targeted at data processors. However, controllers will be obliged only to engage data processors who can ensure data protection standards (see above). Through this requirement, it is expected that processors, too, will be bound.

Whilst the idea behind these provisions is relatively clear, how they will function in practise is uncertain. Practically, it uncertain as to precisely what lengths the controller must go to in order to fulfil their obligations under Article 23. For example, how much 'regard to the state of the art' is enough? Nor is it clear what the consequences for failure to fulfil these obligations will be. Whilst the Commission has given itself the power, in Articles 23(3) and (4), to further specify technologies and criteria clarifying the obligations laid out in 23(1) and (2), whether they are best placed to do this, and how effective they will be, remains to be seen. Theoretically, the relationship between the obligations in Article 23, and other

obligations relating to the need to preserve privacy in data processing, needs to be clarified. For example, one could ask: what obligations are created by Article 23(2) which differ from, or are unique in relation to, those laid down by Article 5(c) – the obligation on the controller to only collect as much data as is necessary for the task at hand? (COM 2012/0011/EC (COD), Article 5)

3.4.5. Conclusions

Cloud computing challenges a number of the presumptions at the foundation of European data protection law. Directive 95/46 is based on locating certain definable actors, and allocating them specific roles. The networked nature of cloud services makes the identification of who is doing what (and who has what control) in relation to a processing operation difficult. The Directive is also based on the presumption that data transfers/processing operations would have single, easily identifiable, locations. In cloud services, the networks of actors and the continuous flows of data between them make isolating the geographical location of either data or service very difficult. Unfortunately, the Directive lacked the interpretation and adaption mechanisms required to deal with these challenges.

As a consequence, the Directive could be awkward to apply in cloud processing scenarios. As a result, the level of data protection in the cloud could not always be ensured, whilst unnecessary barriers to the provision, and innovation, of cloud services, remained.

The proposed Data Protection Regulation takes a number of steps toward remedying these issues. On the one hand, in order to ensure a high standard of data protection, it clarifies the scope of application of European data protection law and the roles of actors (whilst strengthening their accountability and responsibility). On the other hand, it loosens formalistic rules and bureaucratic requirements, allowing development and innovation in cloud services – for example by loosening the rules on international transfers of data. Finally, it elaborates European level interpretation mechanisms which should allow the Regulation the flexibility to deal with future challenges posed by advances in cloud processing.

The progress made by the Regulation in addressing the key issues raised by cloud computing has received significant positive comment. However, this is not to say that uncertainties and problems do not remain.

First, it remains to be seen how the legislative process will progress, what the final results of this process will be and when the final version will eventually enter into law. As mentioned above, we are dealing only with the first draft of the Regulation. The Regulation is currently being debated and will be subject to a continued process of revision – being passed back and forth between Commission, Parliament and Council before final adoption. At the moment, the draft is awaiting a final vote before the European Parliament. Due to the breadth and significance of the issues involved the reform proposals have been subject to unprecedented lobbying and advocacy activity. Currently, over 3000 (according to some sources now 4000) reform proposals sit before the Parliament.[4] The scale of interest the

[4] http://euobserver.com/justice/120867, 'EU wants data protection bill by May 2014', (last consulted 17.07.2013).

proposals have generated have served to repeatedly delay the date of the orientation vote before the Parliament from early 2013 to what will now may be sometime in September or October 2013.[5]

Second, it is very possible that the application of the rules of the Regulation will produce a very different result in practice, to that which one might imagine from reading the text of the proposed Regulation. The law on the page only takes on substance when it begins to be used in practise. There are, accordingly, numerous factors which will yet play a role in shaping the Regulation. First, the Regulation is one piece of legislation, operating at one legal level (the European level), how it will interact in practise with other areas of legislation, and with other levels of law (for example national systems), remains to be seen. Second, the behaviours and mentalities of the actors touched by the Regulation will be significant. Questions such as the following are highly uncertain, and highly significant: How will cloud consumers respond to the rules – will they choose to enforce their rights? Will cloud providers view the rules as a procedural burden, or as essential to maintaining trust in the cloud, and in cloud services? How will DPAs engage with their new sanctioning powers – will they take a hard, or soft approach to rule violations? Finally, with the further development of the technologies, infrastructures and capabilities of cloud computing, it is almost certainly the case that new issues will emerge which will require interpretation and flexibility within the legislation. Whether the structure proposed is up to the task, remains to be seen

Finally, when looking at the approach of the legislation, there are problems which appear to remain unaddressed. One area of particular concern is that of application, oversight and enforcement of data processing taking place outside the EU. Despite the best attempts of the legislator to address the problems, the Regulation remains a piece of EU law. It is accordingly difficult to see how true application, oversight and enforcement can be achieved when processing is carried out on territories where EU law has little, even no, claim to sovereignty. In this respect, it is not so much the Regulation, or even data protection law, which is the cause of the problem, but a much deeper rift between the concept of legal sovereignty and the properties of information.

Bearing the above in mind, it is clear that there are a number of uncertainties related to the future interaction of cloud computing and data protection. However, there are a number of policy options that can be suggested.

Recognizing the fact that the current Directive has certain critical flaws in relation to the regulation of cloud computing, recommended options could be:

- Support the current process of data protection law reform
- Support the choice of a Regulation as the proposed legal instrument replacing the Directive.

[5] http://euobserver.com/tickers/120557, 'Vote on draft EU data protection regulation postponed, again', (last consulted 17.07.2013).

Recognising that data protection and privacy are fundamental rights in the European legal order, and that trust that these rights will not be violated though the use of cloud services will be essential for the continued uptake of cloud services, recommended options could be:

- Support the strengthening of pre-existing individual rights in the proposed Regulation
- Support the integration of the range of new rights offering further control to the data subject over their personal data – for example the 'right to be forgotten' and the 'right to data portability'
- Support the novel obligations on the data controller in adhering to data protection law – for example, 'data protection by design and default' and the fact based approach to the concept of the 'co-controller'.

Recognising that cloud providers, on the other hand, require certainty in the law in order to apply it, and that bureaucracy can impede progress without adding to the protection of rights, recommended options could be:

- Support further clarifications of principles related to data protection and cloud computing
- Support the accountability principle and be cautious with European level 'command and control' approaches.
- Support less rigorous consultation and notification requirements

Recognizing that cloud computing will continue to develop as a technology, and that this has in the past, and will in the future, pose novel challenges to data protection law, recommended options could be:

- Support the creation of European level consistency and interpretation mechanisms
- Support the creation of the European Data Protection Board
- Support increased cooperation and consistency between European DPAs

Considering that, for data protection law to work, it requires oversight and enforcement mechanisms, recommended options could be:

- Support the fines mechanism proposed in the Regulation
- Simultaneously, support the discretionary power of National DPAs in the fining process

Considering that cloud computing will be an increasingly global endeavour, recommended options could be:

- Support proposals which allow justified international flows of data, whilst not risking the rights of citizens.
- Reconsider approaches which have perhaps not achieved all they promised up to now – for example Safe Harbour
- Look into further possibilities to ensure the jurisdictional applicability of European data protection law, when European citizens or services are involved
- Look into methods of oversight and enforcement when European data protection law should apply, but data is being processed abroad.

3.5. Governance Issues related to data retention and enforcement outside of the EU

3.5.1. Introduction

Cloud computing adoption has been slowed by a number of different factors having to do with the uncertainty surrounding data protection practices, which together translate into a lack of trust in the cloud (Robinson 2011). A lack of transparency on the part of many private cloud providers have made businesses and governments uncertain about their risk management situation and have caused individual users to be vary whether their right to privacy is suitable protected by cloud providers. Since cloud providers as a group have proven unable to meet these concerns on their own initiative, international level governance interventions have become necessary (Com 2012/609/EC). At this level of decision-making, however, the ambitions of cloud providers to build up truly global cloud services run into the reality that the world economy, although increasingly globalized, is neither without borders nor subject to any uniform governance regime. While political decision-makers in the U.S, Europe and Asia seem to want to support the development of universally available, trustworthy cloud services, historically conditioned differences in approaches to the governance of information and economics produce difficulties in the formulation of common governance measures. Furthermore, with the recent Snowden leaks indicating unwarranted access being given to the NSA to private information stored in cloud servers (Guardian 2013) and data from national security agencies being pooled illicitly (Spiegel 2013), the underlying issues of trust between governments has added considerably to these difficulties.

This section of the report aims to explicate some of the areas of difficulty within international cloud governance with a special emphasis on those issues that stand in the way of such international governance living up to European standards of data protection and privacy.

3.5.2. Data retention and 3rd party access to data

Provisions to oblige telecoms ad internet service providers to retain communication data and/or meta-data have been implemented in the U.S. with the Patriot Act and in the E.U. with the Data Retention Directive. The purpose of these provisions is to support law enforcement and intelligence agencies in their pursuit of terror-related activity. Under the same provisions, these agencies are therefore mandated to gain access when warranted to secret data, including personal data and business secrets. However, with cloud computing it is no longer necessary to have provisions for data retention since data storage is at the very heart of the services provided. This means that 3rd party access to secret data will take place under different conditions.

In classic data security thinking, the data controller (the user) of any cloud service carries the ultimate responsibility for data security. As we have seen in section 3.3 above, however, with the opaqueness of security practices of many cloud providers, it becomes impossible for users to assess with any confidence the quality and characteristics of the data security regime they would enter into with the adoption of any given cloud service.

Open-source cloud services provide a higher degree of transparency with regard to the software architecture upon which they rely. But transparency in this regard does not automatically translate into a similar openness with regard to security practices around staff screening and physical protective measures, and it does not touch upon an element essential to the cloud, namely the diffusion of data placement. A key element to data security management is to always know the physical location of data. This is a cornerstone of risk assessment. It is also key to the ability to retrieve and relocate data to protect it from intruders. But with a cloud architecture, data location changes dynamically according to the current workload of the cloud system. This means that at any one time a given user's data can move from one virtual server to another across different sections of a server park or even between different storage facilities possibly located in different countries. Most likely, the cloud architecture will make use of redundancy and store data in several different locations at once.

All in all, the complexity (or impossibility) of establishing data location adds up the impossibility for cloud users of upholding a second cornerstone of data security, namely controlling, or even verifying, who gains access to the data in question. This constitutes the technical basis upon which a number of governance issues arise having to do with 3rd party access to data and the retention of data beyond the control of the user. By constructing an opaque system of data storage, cloud technology lends itself to being misused as a tool for mass surveillance by governments as well as data mining by private corporations. While data retention legislation was necessary before traditional e-mail messaging and phone communications would store by ISPs and Telecoms, cloud computing services in many case store all information flows by default, making them prime tools for subsequent data analysis by 3rd parties.

The in-built data retention in cloud computing makes it technically possible for governments to access ever larger and more complete sets of personal data and communication along with the meta-data describing connections of communication between individuals. One document, leaked by Edward Snowden to the Guardian dating April 2013, seemingly documents that the NSA with its PRISM program had created a system for gaining direct access to e-mails, chats, videos, photos, stored data, file transfers, phone-calls via the Internet (VoIP), video conferences, and social networking activities from users of cloud services provided by Microsoft, Google, Yahoo!, Facebook, YouTube, Skype, AOL and Apple with more providers to "come online". What this last phrase meant was initially unclear as providers denied all knowledge of the system, implying that PRISM enables access without consent (Greenwald and MacAskill 2013). However, a group of the cloud providers involved have later revealed that they were in fact acting under a so-called FISA order (described below) and compelled by a "gag order" to keep silent about their involvement (Ashford 2013a, 2013b). Another leaked document seems to reveal practices by the British intelligence agency, GCHQ, of tapping and storing for up to 30 days the total flow of data through fibre-optic cables connecting the North America and Europe, including phone calls, e-mails, Facebook postings and more. (MacAskill et. al. 2013) Although such practices are do not directly make use of weaknesses in cloud architectures, it is very likely that storing and sifting through such enormous amounts of data relies on cloud computing solutions. And a third leak to der Spiegel shows how a collaboration program between

national intelligence services, who are each in themselves legally prohibited from spying on their own nationals, nevertheless enables the creation a matrix system of information gathering ('Boundless Informant'), which makes information available to any of the involved agencies about citizens in any country (Poitras et. al. 2013). The general tendency in these revelations is illustrated by a quote, brought both in the Guardian and Spiegel of U.S. Chief of Cyber Command, Keith Alexander, who supposedly asked rhetorically: "Why can't we collect all the signals all the time" during a visit to his British counter-part in 2008. The emergence of such thinking coincides precisely with the advent of cloud computing as a technical space of possibility. And it indicates a clear intention on the part of intelligence agencies to make full use of those possibilities.

The first question to be asked in the wake of the Snowden leaks has to do with the legality of such total surveillance practices. Especially pertinent is the underlying issue of legality within different jurisdictions. Within the articles referred to above, the impression is given that the Tempora program – although controversial – may in fact be setup in compliance with U.K. regulations and that the Boundless Information system seems simply to make clever use of legal provision use for transnational cooperation. These provisions are typically included in Mutual Legal Assistance Treaties (MLATs) between individual countries. One example of such a treaty is the German-US Mutual Legal Assistance Treaty in Criminal Matters with the United States (2003) and the subsequent Supplementary Treaty to the Mutual Legal Assistance Treaty in Legal Matters with the United States, both of which entered into force in 2009 (Maxwell and Wolf 2012). In the case of PRISM, the matter of legality is disputed. Some hold that the U.S. Foreign Intelligence Surveillance Act provides a legal basis for a broad range of surveillance of citizens from outside the U.S. by U.S. government agencies and therefore puts PRISM within the boundaries of U.S. law (e.g. Rauhofer and Bowden 2013). Others, however, argue that while PRISM may only "target" foreigners, the practices of dragnet surveillance involved will necessarily lead investigators to "acquire incidentally" an extraordinary mass of personal data belonging to U.S. citizens putting the program at odds with the U.S. constitution (Kaminiski 2013).

In Europe, the question of legality goes even deeper. European cloud providers were quick to see a silver lining in the PRISM revelations, profiling themselves as "privacy friendly" over against U.S. based cloud providers with reference to the differences in U.S. and E.U. data protection legislation (Abboud and Sandle 2013). The U.S. Patriot Act with its provisions for data retention and access by law enforcement has especially been singled out as putting U.S. data protection in a class lower than that enjoyed by European citizens. But this view in fact does not provide a faithful picture of the state of legislation in the E.U. versus that in the U.S. For while it may be argued that the original Data Protection Directive of 1995 went further in some crucial respects than contemporary U.S. data protection legislation, the European Data Retention Directive may very well have levelled out those differences. On white paper (Maxwell and Wolf 2012)compares government access to data across a number of different jurisdictions (see figure below) and shows that the U.S. government in fact does not have wider allowances than European governments. In a European country a citizen – according to the white paper – is less likely to be notified of privacy breaches by government than in the US. The co-existence of the Data Protection Directive and the Data Retention Directive along with national provisions for government

authorities' access to retained data seems therefore to present a legal paradox, which the Irish High Court and Austrian Constitutional Court recently sought to unravel by testing the Data Retention Directive's legality at the European Court of Justice. A decision is expected toward the end of the year (EDRI 2013).

Table 2: Governmental authorities' access to data in the cloud. Source: Maxwell and Wold, 2012.

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the Cloud provider notify the customer?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
Australia	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Canada	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Denmark	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
France	Yes	Yes, except for personal data without a legal purpose, electronic communications	No	Yes	Yes	Yes
Germany	Yes	Yes, except for personal data without a legal purpose, electronic communications	Yes, except may delay until disclosure no longer would compromise the investigation	Yes	Yes	No, not without cooperation from the other country's government, except for telecommunications customer non-content data
Ireland	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Japan	Yes	No – must request data through legal process	No	Yes	Yes	No, not without cooperation from the other country's government
Spain	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United Kingdom	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes	Yes

Key to the discussion about "privacy-friendly" jurisdictions is an understanding of the powers bestowed – or not bestowed – on government agencies by the U.S. Patriot Act of 2001. It is erroneously believed by many that the Patriot Act created new, invasive powers for such agencies to gather personal and secret information. The reality is, however, that most of these powers existed already and that they were – and remain – limited by the U.S. Constitution (Maxwelll and Wolf, op. cit.). So just as in the case of Europe, there is an underlying legal paradox, which hopefully the lawsuits mentioned above will help to clear

up. Even within the confines of the Patriot Act itself, however, government agencies are still bound by burden of proof and not legally empowered to gain access to cloud data (or any other kind of personal data). Specific provisions outside the Patriot Act for gaining access to data include provisions within the 1978 Foreign Intelligence Surveillance Act for so-called FISA orders, which must be issued by a judge. These orders give access to content data in cases where there is reason to believe that access to the data will help unveil international terrorism or spying. FISA orders could be given before the Patriot Act, but the Patriot Act added a "gag order" disallowing telecoms and ISPs served with such an order from disclosing the existence or content of the order. As already mentioned, this "gag order" was the reason behind initial denials by major cloud providers of having had knowledge of the PRISM program,This illustrates the opaqueness created by legislation in this area. Government investigators may themselves issue National Security Letters (NSL's) directly to telecoms and ISPs in order to gain access to meta-data, which is most likely to the mechanism used in the Verizon-scandal. The possibility of issuing such letters had also been part of the arsenal of investigative mechanisms before the Patriot Act, but its use seems to have been expanded after the passing of the Patriot Act which also here added a "gag order" as well as allowing agencies other than the FBI – including the CIA and the NSA – to issue such orders. FISA orders and NSL letters, the range of their use and their constitutional legality, are at the heart of the on-going controversy regarding U.S. data access in telecoms, internet services and clouds. The question is whether these powers of investigation in fact go much further than those used by the European law enforcement and intelligence communities?

Comparing the powers of investigation granted to U.S. investigators with similar provisions in the E.U. must firstly take place at national level, since national level implementations of the European data protection directive have taken various courses in the different member states (Korff and Brown 2010). In Denmark, for instance, it is legal for cloud providers to voluntarily provide customer data to government investigators or a police investigation, which counts as a valid reason to break the obligation to protect personal data (Maxwell and Wold, op. cit.). Even though provisions for forcing such data sharing are bound to classical search warrants issued by a judge, which could create the image of much stricter data protection legislation, the legality of voluntary sharing (which remains illegal in the U.S.) creates a highly opaque juridical situation in which we can only guess what would produce such volition on the part of cloud providers, ISPs and telecoms. In France, efforts have been made since the 1980's to coordinate at central, national level efforts to counter terrorism. Overcoming the institutional disparities, which in the U.S. still acts as a brake on domestically based investigation efforts, the Unité de coordination de la lutte anti-terroriste (the coordination unit of fight against terrorists) was founded in 1984 coordinate domestic and foreign intelligence gathering, and in 2008 the Central Directorate of Domestic Intelligence was created in which the state police and the anti-terrorism and counterespionage units of the Ministry of the Interior were merged (Erlanger 2012). This higher level of coordination is necessary in order to utilize the relatively limited resources of French investigative agencies, which traditionally rely more on manpower and physical actions than computing analysis. In order to obtain data stored in clouds, government investigators can either obtain classical search warrants or they can under certain circumstances directly issue request letters to the cloud provider requiring that the provider

produce customer data relating to a criminal investigation (Maxwell and Wolf, op. cit.). French law also does not prohibit voluntary sharing of information by cloud providers, nor does it oblige cloud providers to inform customers if information is shared. It should be obvious from these examples that data stored in clouds on European soil are not necessarily safer than in the U.S. on juridical grounds. The real difference lies in the concrete practices of the intelligence communities in each country.

The second question to be addressed, then, is the issue of the desirability of the practices revealed. While many have been quick to speak out against revelations that communications in and out of the European Parliament have been recorded (Hecking and Schulz 2013) and to decry the spying practices of NSA and GCHQ, the underlying issue of balancing trade-offs between privacy and security remains. The arguments here are classical and not specific to cloud computing. From a law enforcement point-of-view, access to more data gives a higher likelihood of prevention of crime and terrorism. From a privacy point-of-view, the mechanisms and laws put in place to allow for such access are seen as dangerous in themselves given the risk of mission-creep, which it is feared can lead to the on-going escalation of surveillance far beyond what would be politically acceptable. This discussion goes to the very core of the open society and the nature of democracy and will likely be intensified on the basis of the Snowden leaks and subsequent political reactions.

The third question to be asked, which one might fear being overlooked, is whether or not it is technically possible to prevent such massive surveillance practices given the interconnected nature of the information society and the rise of cloud computing and big data. Proponents of "privacy by design" (PbD) hold that true privacy protection can only be upheld through conceptions of information processing and data security fundamentally different from those which structure ICT development today. The Information and Privacy Commissioner of Ontario, Canada, has put forth a list of PbD principles among which is to keep ICT design user centric and to allow for strong online identity protection. Section 3.3. of this report covers some of the technical options for achieving such protection. The point of raising these issues here is to underscore the difficulty of establishing actually trustworthy cloud services by setting up legal boundaries to organizations' behaviour while at the same time allowing for the opaqueness of cloud providers' practices and the secrecy of intelligence agencies' behaviour. From this point of view, the real battle over the conditions for privacy lies not in privacy legislation, but in the standardization regimes covering cloud computing.

Without going too deeply into the conceptual questions underlying standardization of cloud services, it is worth noting here the existence of what may prove to be paradigmatic developments in the basic approaches of the data security research community. These basic developments can be of direct relevance to the political strategies There are those who argue that the basic objectives of data security – to prevent access to data from outsiders or, if this fails, to prevent data from becoming comprehensible through encoding or encryption – has become outdated with the digital interconnection of the world. From a system design point of view, we should assume instead that all data – once given over to interconnected databases – is already lost. What matters, then, is to make the data worthless to the unwelcomed reader. Most relevant to solving this issue is still the

protection approach covered in section 3.3. But there are those who argue instead for a fundamental change in how we handle online identities and for the empowerment of users in this respect. Instead of centralized identity management and authorization systems which users need to trust in order to access online resources, a societally wiser approach might be to place users' identify management with themselves, outside the systems they wish to access, thereby creating a radically de-centralized information society. Again, such debates fall outside the scope of this report. The European research projects FIDIS and HYDRA are recommendable sources of learning on the subject. The point here is simply to outline the oppositional forces drawing policy either in the direction of more centralized solutions with trust in providers as the core component for fluent system behaviour or in the direction of decentralized, user-centric solutions based on an inherent distrust of centralized systems and a greater trust in the judgment of individual users. The forces pushing for the former approach are strong, while the latter draws only limited attention in spite of its greater resonance with ideals of open society. Political decision-makers need to be clear about which direction they want to draw governance developments.

3.5.3. Safe Harbour and international harmonization

With the legal and practical complexities surrounding the twin questions of data retention and 3rd party access to data, the issues of extending the EU-US Safe Harbour data protection collaboration and further effort towards international harmonization of legal frameworks must be viewed in the light of reality rather than in the glow of idealist readings of European data protection policy interpreting a priori as "better". Collaboration on data sharing in support of law enforcement has shown repeatedly that the U.S. and European governments speak very different languages when it comes to defining such core terms as "law enforcement", "law enforcement authority", "intelligence" and "intelligence agency" (De Busser 2010). From the point of view of the European Commission, law enforcement and intelligence operations are clearly separated, but this is not the case for the U.S. We might add that also European member states, as shown above, do not necessarily make the same sharp distinction as the EC. The reason for this might simply be that the E.C. – unlike national governments – is not involved at the same time involved in police activity and international intelligence gathering and thus does has not been forced to deal with the overlap of interests and competencies that arise for national governments. This interpretation at least would make sense of the increasingly entrenched difference in approach to bi-lateral data exchange and data protection collaboration where the EC on its part pursues a universal understanding and governance of core terms, preferably through the intermediation of international bodies like the Council of Europe or the United Nations, while the U.S. government pursues the *real-political* goal of gaining trouble-free access to foreign law enforcement and intelligence data.

As there are good reasons for national-level European intelligence agencies to pursue similar interests, it is important to notice the difference between the total sums of interests on the two sides of the Atlantic. In the U.S., the law enforcement and intelligence communities have interests in the establishment of international legal frameworks allowing for the unhindered flow of data between countries which overlap directly with the interests of U.S. based cloud providers and their European daughter companies. With the business models of some cloud providers being based largely on the unhindered mining of the

personal data of users for commercial purposes, this overlap in interests extends also to the legal frameworks regulating 3rd party access to data. In Europe, the absence of large, home-grown cloud providers means that this overlap in interests is not directly duplicated. Outside of the EC, national intelligence and law enforcement agencies will most likely pursue legal solutions similar to those of their U.S. counterparts. But without the simultaneous existence of similar interests from cloud providers, European policy makers cannot at national nor at European level pursue with the same confidence the logic of boundless information as the U.S. government. The extreme valuations of U.S. cloud giants on the stock market has very little to do with their physical assets or the value they derive from end-users as many of them derive none. What drives these valuations is rather the understanding that the immense amount of personal data turned over to these providers will in some way or other always be commercially exploitable and that, given the weakness of current governance regimes, these values are readily available for any company able to deliver immediate utility and gratification to users (Lanier 2013). From an industrial policy point-of-view, it is nonsensical to hand over such values harvested from European citizens. From this point of view, it would be recommendable for European decision-makers to work actively for a regime of strong data protection centred around European jurisdiction in order to foster a lively European cloud industry bound to uphold real-world data protection practices and with a more healthy long-term contribution to the real economy (see also Bigo et. al. 2012).

Applying these reflections to the issue of extending the Safe Harbour agreement with the U.S., one must first and foremost focus on the enforceability of any collaborative data protection regime. As we have seen above, 3rd party access to personal data is of great value to the entity accessing that data – that entity being public or private. Since such access takes place in a legal grey zone, it is unwise to leave the matter of compliance to Safe Harbour principles up to trust in the cloud provider.

The original Safe Harbour agreement between the EU and the U.S. was made in order for U.S. businesses to gain access to European markets without having to go through the same processes of registration with national data protection agencies as Europe-based businesses and to circumvent the fragmented data protection policy implementations made by individual member states. Once deemed to uphold "adequate" standards of data protection, U.S. providers of internet services would have access on equal footing to markets in all member states. Such adequacy means to uphold the basic principles of data protection of the European directive, for instance the obligation to inform users about access granted to 3rd parties or data processing done for other purposes than those originally agreed to by the user. In effect, these principles would most likely prevent the legality of many uses of personal data by providers of advertising-driven services delivered. Critics have, however, have long maintained that the enforcement regime around the Safe Harbour agreement is much too weak to guarantee real-world compliance (EDRi 2012). Safe Harbour is a self-certification scheme through which companies certify the own compliance with the scheme's principles. Investigations based on user complaints take place under the jurisdiction of the company's home country and is first and foremost carried out by private-sector dispute resolution organisations. Ultimately, of course, such self-compliance mechanisms are subject to enforcement by government authorities, primarily the Federal

Trade Commission. But in the light of the recent Snowden revelations, a general trust in this mode of layered enforcement becomes difficult to maintain, and there are serious indications that the Safe Harbour principles are not enforced in substance (Nielsen 2013).
The proposed Data Protection Regulation in its original form aims squarely at mending the combined deficiencies of enforceability of the Data Protection Directive and the Safe Harbour agreement. In parallel with recent and upcoming legislation on the same topic in other countries such as Australia and Singapore, the EC proposal includes the notion of extraterritorial reach of the legislation, i.e. the automatic applicability of the Regulation to any organisation processing data as part of the provision of products or services to citizens or organisations within the EU. At the same time, the proposal aiming at the creation of a Regulation rather than a Directive means that the proposed rules would apply uniformly across Europe without having to be implemented at national level. The proposal thus aims to kill two birds with one stone, achieving at once a unified European digital market and more serious measures to ensure the protection of the personal data of European citizens. One important detail with regard to the enforceability of the proposed rules is the inclusion of a sliding scale of fines for data protection and privacy breaches of up to 2% of yearly turnover. Such enforcement measures, along with more detailed demands for documentation of data protection practices, seem to represent a step forward in comparison with the Directive (Brodies 2012).

With regard to international harmonization, the EC regulation proposal intends for Europe to "take the lead" for global data protection standards (EC 2012), which is more readily possible through the proposed construction of European legislation with extraterritorial reach than similar positions have been in earlier negotiations in which EU leadership has relied more on the construction of international legal frameworks. With the construction of legislation with extraterritorial reach, there is the possibility of making principles similar to those of international conventions count in those internet interactions, which involves European citizens and business. However, there is of course a balance to be struck concerning the possible conflicts with other national legal frameworks, not only in the U.S. (Kuner et. al., 2013). Nevertheless, going down the path of legislation with extraterritorial reach means that the EC has in effect found a way to speak a foreign policy language much more akin to those of the U.S. and other major powers without compromising the core ethical stance of European data legislation from the beginning. Given the importance of maintaining these principles from both a human rights and a European industrial policy perspective, it becomes important in the parallel negotiations of a free trade agreement with the U.S. not to fall into the trap of trading off ethics on the one hand against potential growth on the other. In the case of cloud computing it seems quite clear that these often opposing interests overlap.

3.5.4. Discussion and conclusions

The difficulty of governing cloud computing due to the plurality of jurisdictions involved is well-known and has been at the basis of discussions about the revision of data protection legislation both in Europe and internationally. Over the past year, however, the world has gained insight into trans-legal (if not illegal) practices of 3rd party access to data for the purposes of data mining by both private actors and government agencies. This insight has shown that cloud governance is not only about legal frameworks, but also about their

enforceability. With the extraterritorial reach of the proposed European data protection regulation, the European Commission has taken one step away from its previous reliance on international agreements in this area towards a more unilateral approach to upholding European standards of data security and privacy in a globalized economy.

This approach has both benefits and drawbacks. On the one hand, more active means of enforcement become available to Europe while providers under the proposed Regulation will be forced to provide greater transparency. As such, the proposed legislation relies less on trust in individual actors than previous frameworks such as the Safe Harbour agreement. On the other hand, with this approach Europe moves on step closer to the strong-arm style of diplomacy, which have otherwise been associated with other major world powers, especially the U.S. Taking this step puts negotiations about international data protection legislation on the same table as other international relations issues such as the proposed free trade agreement between the EU and the U.S.

It is important in this context to ask difficult questions about the relationship between vested interests and viewpoints being put forth in the debate. The US cloud industry, for instance, may share an interest with the US government in weakening European cloud governance and/or its international applicability. Such an interest might be shared by some member state intelligence agencies, although they do not make up a strong voice in the public debate about these issues. But European citizens, SME cloud users and government agencies, all of which are at a disadvantage in negotiating terms of service and security practices with major cloud providers, may in fact need exactly the strong leadership of Europe. Such leadership may additionally help further home-grown European providers of primary cloud services. It might, however, also stifle the growth of secondary providers of app-based services. Striking the necessary balance between these concerns is no simple matter. Simple answers should therefore be viewed with some suspicion.

On the basis of these observations, decision-makers may wish to:

- Scrutinize viewpoints put forth in the debate to see whose interests they serve.
- Be especially wary of exclusively trust-based solutions to cloud governance issues.
- Look further into ways of promoting cloud architectures designed from the beginning to secure data security and privacy through design rather than trust or legislation.

4. CONTRACTUAL ISSUES AND CHALLENGES OF THE MARKET COMPETITIVENESS

4.1. Introduction

The first section of this chapter will analyse the regulatory environment in a wider sense, i.e. in particular the questions of jurisdiction, customer rights and the contractual relationship as whole including for example Service Level Agreements (SLA), which was identified by the initial analysis of drivers and barriers as another focal point (Leimbach et al. 2012, 83-84). Strongly related to these issues are the question of vendor lock-in, where legal and technical aspects like interoperability work together.

While the first is of importance for both, business users as well as consumers, the latter one is in particular of importance for business in general. Because vendor lock-in can create a barrier for competitiveness of the market for users as well as competitors by establishing barriers to change and market entrance. Therefore the second part of the chapter will examine this as well as more general challenges issues for the competitiveness of European suppliers like the fragmented markets or the lack of fast growing enterprises.

4.2. Contractual issues of Cloud Computing

This section provides a high level overview of contractual issues relating to cloud service provision and a discussion of some of the possible consequences of such issues. Where applicable, the relevant European legislation is discussed, however national legislation is not. It should be noted that this section does not discuss the treatment of data, and specifically the handling of personal data, in detail as this is dealt with separately in a separate section (see chapter 3.4). Rather this section provides a general overview of a wide range of commonly found contractual clauses between cloud service providers and their clients including choice of law, IP issues, terms of service, and acceptable use. While the issue of data protection attracts much attention and debate, other contractual issues also impact the adoption of cloud computing and are discussed herein. It should be noted that no view on the enforceability of specific contractual provisions is provided.

The remainder of the paper is laid out as follows. The first part provides an overview of the general documents that make up contracts for cloud service provision. The second part discusses common features and related issues in Cloud service contracts. It ends with a discussion of some of the business consequences of cloud service contracts and resulting policy options on the European level.

4.2.1. The contract

The contractual relationship between cloud service providers and their clients is laid out in one or more documents typically comprising:

- A Terms of Service ("TOS") - the TOS contains provisions concerning the overall relationship between a cloud service provider and a client. Section 4.3 will discuss these provisions in greater detail.

- A Service Level Agreement ("SLA") – details the level of service to be provided and typically includes mechanisms for auditing service delivery and compensating clients for underperformance. Common features of SLAs are discussed briefly in section 4.3.

- An Acceptable Use Policy ("AUP") – a policy designed to protect cloud service providers from the actions of clients typically detailing uses of the service that are prohibited. AUPs are discussed in greater details section 4.3.

- A Privacy Policy – a policy detailing the cloud service provider's policy for handling and protecting personal data typically in line with the data protection law requirements.

Recent research notes three distinctions in terms and conditions governing cloud service provision (Bradshaw et al, 2010):

1) Free v Paid Services: The obligations of the cloud service provider are likely to be in proportion to the consideration by a customer. Within paid services, terms and conditions typically fall in to those offering standard-form contracts and those subject to negotiation. The latter typically are limited to those prospective customers with sufficient bargaining power e.g. public sector organisations and large corporations, typically multinational corporations.
2) US v EU Legal Jurisdiction: Those service providers asserting their terms and conditions under the US had more extensive disclaimers of warranty or limitations of liability that those asserting governance under an EU member state.
3) IaaS v SaaS: There is less variance in the terms and conditions offered by IaaS than SaaS; IaaS services are more similar than SaaS.

4.2.2. Common features and issues in Cloud Computing Contracts

Choice of Law

The nature of cloud computing assumes that data will be stored across multiple data centres used by a cloud service provider. This can introduce a degree of jurisdictional uncertainty unless (and even if) stated in the TOS. Data may be transmitted, stored and processed across multiple jurisdictions so seamless that the end user, and indeed the cloud service provider (due to the chain of service provision) may not know where data resides at any given point in time.

Of 31 terms and conditions analysed, Bradshaw et al (2010) noted that 15 mandate the law of a particular US state, most commonly California, as the jurisdiction of choice. A further 11 explicitly stated the law of an EU member state and five the either the customer's local law or no choice of law. The jurisdiction for settling disputes is typically similar to the applicable law. The choice of US State law provides certain advantages to cloud service provider. For example, US courts are more likely to recognise disclaimers and limit liabilities as stated in Terms of Service. In addition, legal costs are much higher in the US thus providing a disincentive to EU firm, and particular consumers and SMEs, in taking legal action.

The applicable legal rules to establishing applicable law to contractual obligations in the EU can be found in the Rome I Regulations (Regulation 593/2008/EC).[6] Article 3 recognises that a contract shall be governed by the law chosen by the Parties subject to the existence and validity of the consent of the parties. Where the applicable law to the contract has not been chosen in accordance with Article 3, Article 4 of the Regulations provides a means of determination of choice of law. Article 4(1)(b) states: *"a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence"*

Article 4(1) also provides for the franchisors and distributors in a similar manner. Where the contract is not covered by Article 4(1) or where the elements of the contract would be covered by more than one.

Article 4(2) provides that the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence. Notwithstanding these provisions, Article 4(3) states:*"Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply."*

Similarly, Article 4(4) states: *"Where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected."*

Establishing a real and substantial connection between the jurisdiction and the parties involved can be interpreted widely. Some considerations in choice of law for cloud service provision may include:

- What is the nature and quality of their commercial activity in the jurisdiction?
- Is the sale of services passive or active e.g. is the cloud service provider actively aware that they are making sales to resident of a particular jurisdiction?
- What jurisdiction are the paying customers or end users resident or domiciled in?
- Where is the cloud service consumed?
- Where is the data located? Where are the data centres located?
- Where is the cloud service provider located? Does the cloud service provider have any business presence in the jurisdiction?
- Does the cloud service provider advertise, market or solicit business in the jurisdiction?

Article 6 of the Regulations provide specifically for consumer contracts and would generally apply the country in which the consumer has their habitual residence. Bradshaw et al (2010) note that a number of cloud service providers seek relatively short limitation periods

[6] For legal rules relating to the choice of court having jurisdiction in civil or commercial disputes within the EU, the so-called 'Brussels Regime" recast in 2012 applies (REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters). While the original Brussels Regime only applied to individuals domiciled in the European Economic Area (EEA) or Switzerland. However, the 2012 Regulation also sets out rules applicable to suing individuals domiciled elsewhere.

in which a customer must bring a claim in respect of a service. Consumers are likely to be protected from such limitations EU consumer protection legislation[7].

Data Location and Transfer to Countries outside of the EEA

To achieve operational efficiencies and other technical and business objectives, cloud service providers will transfer data to different data centres. These locations may be located in different jurisdictions including outside of the EEA. Depending on the complexity of the chain of service provision, the identification and maintenance of an exact location on data may be difficult. Concerns are multi-fold and include the location of the data in storage, when processed and in transit.

The applicable legal rules on data protection in the EU can be found in the Data Protection Directive (Directive 95/46/EC). This Directive was introduced in 1995 to harmonise the laws on data protection across the EU member states. On 25 January 2012, the European Commission unveiled a draft European General Data Protection Regulation that will supersede the Data Protection Directive however this is out-of-scope for this paper. Currently, Article 25(1) states: *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."*

Article 26(1) provides for a number of derogations including where:

"(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."

Even where the Article 26(1) derogations are not met, Cloud service providers may still be able to transfer data to a third country. The Council and the European Parliament have given the European Commission the power to determine, on the basis of Article 25(6) of Data Protection Directive whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. To

[7] Annex to Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts

date, the European Commission has so far recognised the following for inclusion on the so-called 'White List': Andorra, Argentina, Australia, Canada, Switzerland, the Faeroe Islands, Guernsey, the State of Israel, the Isle of Man, and Jersey as providing adequate protection. In addition, the Commission has also recognised the US Department of Commerce's Safe Harbour international privacy principles, and the transfer of Air Passenger Name Record data to the United States' Bureau of Customs and Border Protection as providing adequate protection. The former includes the transfer of personal data to US organisations that have signed up to the Safe Harbour international privacy principles agreed between the US and the EU.

Under Article 26(4) of the Data Protection Directive the European Commission can decide that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2). By incorporating the standard contractual clauses into a contract, cloud service providers (acting as Data Controllers) established in the EEA can legally transfer personal data to a Data Controller or to data processors established in a country not ensuring an adequate level of data protection[8].

A third mechanism, Binding Corporate Rules (BCRs), is available to transfer data to countries not ensuring an adequate level of data protection. Unlike the White List or Model Clauses, the BCRs are not decided upon by the European Commission. The BCRs are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.[9] They were designed by the Article 29 Working Party to complement the Safe Harbour international privacy principles, which only apply to US organisations and the EU Model Contract Clauses. BCRs are required to be approved by the data protection authority in the EU Member States in which the organisation will rely on the BCRs. Organisations intending to adopt a BCR will appoint a lead authority, typically where their European headquarters is located or where their data protection responsibilities lie however this is not always the case. A mutual recognition procedure has been agreed whereby once the lead authority considers that a BCR meets the requirements as set out in the working papers, the data protection authorities under mutual recognition accept this opinion as sufficient basis for providing their own national permit or authorisation for the BCR, or for giving positive advice to the body that provides that authorisation. To date, 21 countries are part of the mutual recognition procedure: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain, and the United Kingdom.

In their review of terms and conditions, Bradshaw et al (2010) noted that the majority of service providers studied did not address the location of data storage, processing and transit adequately. Furthermore, unless the service provider is operating its own secure infrastructure, this may not be possible or economically feasible. While the Data Protection

[8]http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

[9]http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/

Directive and specifically Articles 25 and 26, provide a strong legal basis for controlling the export of data outside of the EU, commentators have noted that this may not be an adequate disincentive to non-EU government authorities.

Data Integrity and Availability

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle (Boritz 2005). Many clients consider using the cloud as they perceive the cloud to be a safe method of backing up data. With this in mind, data integrity and availability go to the core of consumer expectations.

Bradshaw et al (2010) found that the majority of cloud service providers surveyed included clauses in their terms and conditions, which placed the responsibility for preserving data integrity with the client. While a number of service providers surveyed stated that they would use 'best efforts' but nonetheless disclaimed responsibility for data integrity.

Article 17 of the Data Protection Directive (Directive 95/46/EC) requires that Member States provide that:*"…data controllers to implement appropriate technical organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."*

Article 17(2) requires data controllers to choose data processors with sufficient guarantees in respect of the technical security and organisational measures governing the processing and compliance those measures. Any such processing must be governed by a contract stipulating that the processor shall act only on instructions from the controller. At least, for personal data it would seem that cloud service providers have obligations however this is not clear for business data which may be contractually disclaimed. This is consistent with recent findings by Hon et al (2012) in negotiated cloud service contracts.

Data availability is the extent to which an organization's full set of computational resources is accessible and usable (Jansen/Grance, 2011). Availability can be impacted by both temporary and prolonged outages; denial of service attacks and scheduled maintenance (Jansen/Grance, 2011). Availability is typically dealt with in SLAs however is typically disclaimed and remedies limited to service credits.

Security of Data

McDonagh (2012) identifies two areas of law with respect to the security of data in the cloud:

- Obligations under data protection legislation
- Access to date for law enforcement purposes

For the purpose of the Data Protection Directive, the cloud client can typically be considered the 'data controller' and the cloud service provider the 'data processor'. Article 17 of the Data Protection Directive requires the data controller to: *"…implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."*

The data controller must ensure a level of security appropriate to the risks represented by the processing and the nature of the data taking in to account the state of the art and the cost of implementation. While no guidance is given on specific security measures, it is clearly expected to be proportionate to the sensitivity of the data being processed. Article 17 (2) requires the data controller to choose a processor: *"…providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures."*

The contract between the data controller and data processor must stipulate that the processor shall act only on instructions from the controller and that the obligations on the data controller under the Directive are also incumbent on the processor. Clients of cloud service providers may wish to consider the security of data not only in storage but while being processed and in transit and specifically require the cloud service provider to encrypt the data in such instances. The Article 29 Working Group provide a detailed list of 14 safeguards relating to the controller-processor relationship.[10]

There are significant practical issues with compliance with these requirements in a multi-tenant cloud environment. While the data controller is responsible for the security measures, it would be extremely difficult for a cloud service provider to accommodate multiple discrete security policies from clients on a shared service. Hon et al (2012) note that cloud service providers in negotiated contracts generally refused to adopt client policies or adapt their own. Rather, they specifically based on the security policy on industry best practices while reserving rights to change their own policy unilaterally. The use of industry certifications including PCI-DSS, ISO27001, SAS70 and COBIT5 are common assurances for security in IT and increasingly cloud computing and clients may contractually require cloud service providers to maintain these certifications. While these certifications are gaining greater traction in cloud computing and involve regular audits by third parties, cloud service providers are unlikely to contractually agree to audits by clients or third party auditors nominated by clients. This area is further complicated depending on the complexity of the chain of service provision and the use of the Internet as a transport mechanism in cloud computing.

Hon et al (2012) note that many standard terms of cloud service providers did not require security incidents to be reported to clients or end users however noted that providers were typically agreeable to negotiating such service provision.

[10] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, European Commission

Access to data may be provided for law enforcement purposes in a number of ways. Contractually, Bradshaw et al (2010) noted that the overwhelming majority of cloud service providers state that they will disclose data in response to a valid court order. Others may provide procedural safeguard by providing advance notice, if possible. It should be noted that Bradshaw et al (2010) do note other cases with lower disclosure thresholds. Cloud service providers, particularly in negotiated contracts, may address the issue by providing that they will not provide access unless instructed by the client however any such contractual arrangements must operate against the backdrop of the applicable legislative framework for access to data for law enforcement purposes and such a provision would therefore carry little weight (McDonagh 2012).

The Council of Europe Cybercrime Convention is an international treaty on crimes committed via the Internet and other computer networks. The objective of the treaty is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The treaty deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also sets out such procedural law issues including expedited preservation of stored data (Article 16), expedited preservation and partial disclosure of traffic data (Article 17), production order (Article 18), search and seizure of computer data (Article 19), real-time collection of traffic data (Article 20), and interception of content data (Article 21). Chapter III outlines details on international co-operation. While the treaty has been ratified by the majority of the Member States of the Council of Europe, 12 have not including the Czech Republic, Greece, Ireland, Luxembourg and Sweden. Notwithstanding the Council of Europe Cybercrime Convention, the actions of law enforcement officials must interpreted against the backdrop of the European Convention on Human Rights protections such as those concerning the right to privacy and the right to fair procedures.

Law enforcement official may also be able to access data for law enforcement purposes under the Data Retention Directive (Directive 2006/24/EC). While originally drafted against a telecommunications backdrop certain envisaged services are now delivered by cloud service providers. As such the Directive may impose requirements on the cloud service provider to store citizens' telecommunications data for six to 24 months. Under the directive the police and security agencies will be able to request access data relating to communications provided a court has granted permission. In the context of the Data Retention Directive, a 'service provider' is: *"..a person who is engaged in the provision of a publicly available communications service or a public communications network by means of a fixed line or mobile telephones or the internet."*

Services such as email clearly fall within this definition. 'Data' refers to traffic data or location data but not the content of the communications.

Law enforcement agencies may also be able to gain access to data through a variety of legal mechanisms including Mutual Legal Assistance Treaties (MLATs) – bilateral agreements between EU member states and the US to exchange information required for lawful investigative purposes – and a variety of US mechanisms. The latter have been the

subject of some controversy and while beyond the scope of this paper include provisions under the US Patriot Act, the US Electronic Communications Privacy Act, Foreign Intelligence Surveillance Orders, National Security Letters as well as traditional mechanisms.

IP Issues

Cloud services will typically include the storage, processing and transport of data. Much of this data will be protected by copyright, known in copyright law as "works", which may be owned by the client, third parties, or the service provider. Central to any IP infringement claim will be the claimant's ability to establish:

- That IP rights exists in the works at issue;
- That the claimant owns the IP;
- That the IP has been infringed; and,
- That none of the defences for infringement apply.

Cloud service providers typically provide non-public resources for use by customers which are distributed, seamless and invisible to end users. These resources are typically provided under agreements to ensure security and privacy. Thus investigating the processes, software and physical infrastructure of a cloud service provider is significantly more difficult than traditional on-premise software.

This sub-section provides a brief overview of some of the applicable legal rules in the EU that impact cloud computing with an emphasis on copyright, patents and trade secrets.

Copyright
Copyright law in the European Union comprises a number of directives, which while the member states are obliged to enact into their national laws allowed for significant derogations, and by the judgments of the Court of Justice of the European Union, that is the European Court of Justice and the General Court. A detailed consideration of copyright law is beyond the scope of this report however the main features will be discussed. The applicable legal rules on copyright protection in the EU can be found in a number of directives including:

- Council Decision of 16 March 2000, on the approval on behalf of the European Community of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society)
- Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access

- Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version).
- Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs
- 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

Various types of material are recognised in EU law in which copyright can subsist including literary works (including computer programs[11]), film, sound recordings, artistic works, and original databases,[12] all of which can be stored, processed and transported in the cloud. Copyright will subsist in works of the kind listed only if they are original and copyright is acquired automatically on generation. The author of a copyright work is the first owner of copyright in that work (unless the work is created in the course of employment, in which case the owner of the copyright is the employer) but he or she can assign that ownership to another person. Articles 1 and 2 of the 2006 Copyright Directive sets the term of protection of copyright for a literary, artistic, cinematographic or audio-visual works at 70 years from the death of the author of the work or the death of the last surviving author in the case of a work of joint ownership or the date on which the work was lawfully made available to the public if it is anonymous or was produced under a pseudonym. The term of protection for related rights (e.g. those of performers) is set at 50 years.[13] Copyright gives the owner certain exclusive rights to do certain things in relation to the work, including reproduction, communication and distribution[14]. Anyone else who does any of these things (known as the acts restricted by copyright) without the permission of the owner, infringes copyright and may be subject to legal proceedings taken by the owner for that infringement. Article 5 of the Copyright Directive provides certain exceptions and limitations in respect of alleged infringement of copyright including the temporary reproduction of a work for transmission in a network between third parties by an intermediary or for a lawful use of no economic consequence, reproduction for the purposes of research or private study, review or the reporting of current events, criticism, public security, educational use, library use and use for the purposes of public administration.[15] A person sued for copyright infringement may claim that copyright does not subsist in the work in question, or that the act complained of does not fall within the scope of the restricted acts, or that the act complained of was not carried out in relation to a substantial part of the work.

The liability of cloud service providers for illegal content uploaded by their clients is dealt with by the Copyright Directive and the Electronic Commerce Directive (Directive

[11] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

[12] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs

[13] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights

[14] Article 2,3 and 4

[15] Article 5

2000/31/EC). The Copyright Directive requires Member States to provide adequate legal protection against services which (a) are promoted, advertised or marketed for the purpose of circumvention of, or (b) have only a limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures. Similar protection is required against services that remove or alter electronic rights-management information.

The Electronic Commerce Directive (Directive 2000/31/EC) sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike. It establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. Central to the E-commerce Directive is the definition of information society services: *"…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."*

The majority of cloud services clearly fall within this definition however one might argue that free services are not depending on one's view of remuneration and "*individual requests of a recipient of a service*".

Articles 12-14 of the E-commerce Directive (Directive 2000/31/EC) establish precisely defined limitations on the liability of internet intermediaries providing services consisting of mere conduit, caching and hosting. The conditions under which a hosting provider is exempted from liability, as set out at Article 14(1)(b) constitute the basis for the development of notice and take down procedures for illegal and harmful information by stakeholders. It should be noted that these exemptions apply only in respect of liability for damages, leaving open the possibility that an injunction can be secured to stop the activity in question.

The capacity of a cloud service provider to avail of the exemptions under the E-commerce Directive will depend on the nature of cloud service being provided and it is certainly far from clear. Paragraph 43 provides: *"A service provider can benefit from the exemptions for 'mere conduit' and for 'caching' when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission."*

Article 12 is clear, the service provider must not have initiated the transmission, it must not have selected the recipient of the transmission, and it must not have selected or modified the transferred information. Similarly to avail of the exemption for caching, the service provider will be exempt if the sole purpose of the service is to make more efficient the information's onward transmission to other recipients of the service upon their request, on condition that (a) the provider does not modify the information; (b) the provider complies

with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Article 14 requires that to attract protection under the exemption relating to hosting that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. In each of these exemptions, the conceptualisation of the service being provided would seem to be more simplistic than the typical cloud service, and specifically SaaS services. The hosting exemption as outlined in Article 14 is likely to have greater application in cloud service provision however this depends on the extent of 'authority' and 'control' reserved by the cloud service provider.

An emerging issue relates to the ownership of metadata and other information generated from the interaction of the clients and their end users with the cloud service. Reed (2010) posits that information generated by the cloud service provider for its own internal purposes will belong to the provider[16]. However, if the metadata or information contains client data protected under copyright, the client may have an infringement claim – if the client is aware of such use at all. Reed (2010) suggests that cloud service providers need to pay careful attention that they do not take unfair advantage of clients nor infringe copyrighted works. Contracts should state clearly whether such data is being collected and for what use.

Patents and Trade Secrets

A patent is a legal title that can be granted for any invention having a technical character provided that it is new, involves an inventive step and is susceptible of industrial application. A patent gives the owner the right to prevent others from making, using or selling the invention without permission.

European patent law is comparatively fragmented compared to European copyright law. It includes national patent laws, the Strasbourg Convention of 1963, the European Patent Convention of 1973, and a number of European Union directives and regulations in countries which are party to the European Patent Convention. Unlike copyright, you must apply for a patent. An application for a patent can be submitted in discrete Member states or can be examined centrally at the European Patent Office. Applicants must then have that patent validated in each European country and in some instances, translated in to the local language. As such, each patent is subject to legal interpretation and determination for validity and infringement in each discrete country. In December 2012, 25 EU Member

[16] Reed, C. (2010) Information Ownership in the Cloud. Queen Mary School of Law Legal Studies Research Paper No. 45/2010.

States (except Spain and Italy) agreed to participate to create unitary patent protection. In February 2012, 25 countries (except Poland and Spain) agreed to establish a Unitary Patent Court across the EU territory. As yet, these initiatives have not been ratified. It is noteworthy that the European Parliament rejected a common position relating to the patentability of computer-implemented inventions in 2005.

A number of contractual issues regarding patents are pertinent to cloud computing. It is possible that cloud service provider either infringes or enables infringement of a patent through its service. As much of the technical workflow processes are hidden from clients in a cloud service, such infringement may be difficult for a patent holder to prove. While cloud service provider AUPs often include infringement of intellectual property as an unauthorised use, one might equally posit that the cloud service provider should warrant they do not infringe third party patents and indemnify their clients (and their customers) against any liabilities associated with such infringement.

A trade secret means information that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Cloud service provision often involves the subcontracting of multiple layers of IT infrastructure by both customers and services providers. Where the primary cloud service provider sub-contracts IT infrastructure to one or more sub-contracting third parties not privy to the initial agreement with the client, issues may be raised in relation to trade secrets and confidential information generally. In addition to civil (and indeed in some instances criminal) liabilities in the event of disclosure, distribution of confidential information relating to an alleged invention may constitute a form of public knowledge of prior art; such disclosure even to a small group of third parties, in the absence of affirmative steps to conceal, may invalidate a patent.

Hon et al (2012) identify a number of IP areas where care should be taken by parties entering in to contracts relating to cloud service provision. Standard terms may not address IP ownership for applications developed by clients or end users on a cloud service provider's IaaS or PaaS platform and using a cloud service provider's integration tools. Similarly, where clients or end users suggest or actually implement improvements or bug fixes, it may not be clear where IP ownership lies. Hon et al (2012) also identifies the issue of license entitlement as potentially inadequately covered area. Clients may wish to clarify whether services that include application licenses are addressed in the contract and similarly cloud service providers may wish to clarify that clients are entitled to install, configure and use third party applications.

Liability and Indemnities

The IT industry has a long tradition of attempting to minimise the provider's liability for any loss, direct, indirect or consequential, that may arise from the provision of the service. A number of common features of such contracts include exclusions of indirect and consequential losses, setting low liability caps and excluding all liability. In some instances, IT providers will not exclude key types of general liability e.g. personal injury, damage to physical property, IP infringement or unlawful acts. While relevant, the key concerns of organisations entering in to contracts for cloud services relate to losses associated with

misuse of data including personal data, service interruptions or failure, and data integrity or loss.

As discussed in section 2, cloud service provider choosing a US state as the applicable law may do so to limit exposure for direct liability for damage cause to the client or their end users by the cloud service provider. Bradshaw et al (2010) noted that all US-based providers surveyed sought to deny liability for damage as far as possible whereas EU-based providers excluded such liability only for *force majeure* and similar instances. With regards to indirect liability such as indirect, consequential or economic breaches by the provider, disclaimers are more common across both sets of providers (Bradshaw et al, 2010). Bradshaw et al (2010) also identified that the majority of service providers sought to limit the extent of any damages that the service provider might be found liable and in many cases limit compensation to service credits. The majority of cloud service providers also seek indemnifications from clients against any claim against the provider arising from the client's use of the service. Hon et al (2012) note that for negotiated contracts, those clients who were in a position to negotiate their contracts, sought (and in some cases succeeded) to avoid such clauses relating to liability and indemnification. Hon et al (2012) noted that a compromise was that cloud service providers could terminate or suspend the service with sufficient prior notice for clients to investigate and terminate the relevant account if necessary.

Despite service provider attempts to disclaim liability, EU law typically does not allow service providers to contractually avoid liability in the same way the US legal system might. Under Article 23 of the Data Protection Directive addresses the issue of compensation for persons suffering damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive. Persons suffering such damage are entitled to compensation from the data controller unless the data controller can provide that they are no responsible for the event giving rise to the damage. Under the current Data Protection Directive, the data controller is responsible for the processing carried out by the data processor. The proposed revisions to the Data Protection Directive will apply obligations directly to the data processor and such obligations shall be governed by a contract that shall address technical or organisational measures, impact assessment, records relating to processing activities and notification of breaches. Article 26 of the proposed revisions also explicitly states that a data processor who processes personal data other than instructed by the data controller shall be considered as the data controller and become fully liable as if he had acted on his own behalf.

With regard to failures to meet performance levels in cloud service agreements can result in significant losses for clients. UK case law has found that attempts to exclude defined losses consequential on failure may not insulate the service provider from wider liability for such losses.[17]

[17] GB Gas Holdings v Accenture [2009] EWHC 2966 (Comm)

Acceptable Use Requirements

Acceptable use policies (AUPs) are a widely used deterrence mechanism used by cloud service providers to protect them in the event of misconduct by their clients or customers of clients. Typically, the AUP specifies uses of the service that are prohibited. Common prohibited activities listed in AUPs include use of the service for:

- bulk unsolicited commercial email, fraud, gambling, hacking into other systems, hosting or distributing viruses;
- hosting content that is obscene, defamatory or such as to promote discrimination or incite hatred; and,
- any illegal or unauthorised activity including infringement of intellectual property of others.

Bradshaw et al (2010) note that AUPs for cloud service providers are largely homogenous in the set of activities and behaviours prohibited.

Many AUPs use language that may not be feasible for clients to meet. For example, some AUPs require the client to 'ensure', 'use best efforts' or 'commercially reasonable efforts' to ensure that end users comply with service providers AUPs and TOS'. Where clients, such as higher education institutions, have multiple customer constituents, some of whom are employees (e.g. administrative staff and faculty) and some are not (e.g. students), alternative language or process may be more appropriate e.g. that the client should inform customers or customers of clients should be required to accept AUPs and TOS before using the service. Where AUPs (and indeed TOS) require clients to affirmatively preventing 'all' 'unauthorised' or 'inappropriate' use as per the examples cited previously, again it is possibly more reasonable to expect clients to seek to prevent those 'unauthorised' or 'inappropriate' activities that are 'material' and of which the client is aware of.

Unfair Terms and Distance Selling

The EU Unfair Term Directive (Directive 93/13/EC) requires that contracts must be drafted in such a way to prevent the imposition of unfair terms that are likely to deprive consumer rights. The Unfair Contract Terms Directive introduces a notion of "good faith" in order to prevent significant imbalances in the rights and obligations of consumers on the one hand and sellers and suppliers on the other hand. Terms that are found unfair under the Directive are not binding for consumers. Article 5 of the Directive also requires contract terms to be drafted in plain and intelligible language and states that ambiguities will be interpreted in favour of consumers. It should be noted that while the Unfair Contract Term Directive focuses on consumers, national courts have also found contractual terms to be unfair for small businesses.

Similarly the Distance Selling Directive mandates the provision of certain information to the consumer including the identity of the supplier, the supplier's address, the main characteristics of the goods and services, and the price of the goods or services including taxes. Article 4(2) of the Directive specifically highlights the requirement for the supplier to

provide such information in a *"…clear and comprehensible manner in any way appropriate to the means of distance communication used."*

Service Levels and Performance

The SLA details the level of service to be provided and typically includes mechanisms for auditing service delivery and compensating clients for underperformance. SLAs typically contain the following however certain elements may be addressed elsewhere in the TOS:

- a list of services to be delivered including a definition of each service;
- service performance targets which specify the standard of service to be provided under the agreement;
- an auditing mechanism with respect to service delivery; and,
- a compensatory mechanism for compensating clients in the event of underperformance.

The service levels will vary by service, negotiation and often by price. Common exclusions in the calculation of service performance (and compensation) included downtime for scheduled maintenance and any factor outside the cloud service provider's immediate control. SLAs are often provided by reference to the cloud service provider's website and are subject to change this requiring monitoring by the client. While clients can monitor service performance, this is often not the case and thus they rely on the monitoring of the cloud service provider.

Variation of Contract Terms

Bradshaw et al (2010) found that many cloud service providers typically reserved the right to change certain or all contract terms unilaterally in their standard form contracts. This is unsurprising in commoditised services and particularly SaaS contracts. Such variation may be communicated by reference to an updated version on the cloud service provider's website, particularly if in relation to a free service. In such an instance, continued use is considered tantamount to acceptance. Hon et al (2012) note that in negotiated contracts, clients may negotiate that cloud service providers cannot make changes to core aspects without notification and have included a break clause if changes were deemed materially detrimental to their service.

Monitoring

The cloud service provider may include provisions to monitor client cloud services and data although non-inclusion does not signal that they do not monitor. Some client service providers may monitor customer's use in terms of nature and pattern of use for performance purposes. Others may declare that they monitor customer uploads and use both for performance purposes but also for enforcement of the AUP.

Backup

As can be seen from the discussion elsewhere in this paper, cloud service providers may not warrant data integrity and may attempt to limit liability in the case of service failure including data loss or corruption. While cloud service providers may indeed back-up their systems and the their client's data regularly, many will not warrant to do so particularly free services. In some instances, Bradshaw et al (2010) and Hon et al (2012) cite situations where cloud service providers emphasise that the client or both the client and the service provider are responsible for backups.

Dispute Settlement

Contracts for cloud service provision will typically include a provision for dispute settlement. As discussed in section 2, the jurisdiction for dispute settlement or arbitration will typically be the same as that selected under the choice of law provisions. Cloud service providers that include clauses imposing arbitration would seem to be in the minority in standard cloud service contracts (Bradshaw et al. 2010). Where such clauses are imposed, they may be region-specific, either targeting specific regions where disputes are judged to be more likely or seek to conduct the arbitration under rules of an arbitration association in the jurisdiction stated under the choice of law.

It should be noted that in March 2013, the European Parliament voted to support new legislation on Alternative Dispute Resolution (ADR) and Online Dispute Resolution (ODR). The Directive is expected to give all EU consumers the chance to resolve their disputes without going to court, regardless of product or service type or place of purchase. In order to address the particular needs of online consumers, the Regulation on Consumer ODR will create an EU-monitored online platform which will allow disputes to be resolved online and within a set period of time. These new initiatives are particularly relevant to consumer-focussed cloud services.

Termination

Contractual issues on termination fall into a number of categories depending on whether the contract comes to a natural and expected conclusion or is terminated due to some breach of contract. The contractual documents will set out the term of the service and will typically make provision for termination events and the handling of the client's data after the contract with the service provider ends. Key considerations include:

- Setting the term of service and (non-) renewal of service
- Defining termination events
- Data preservation following termination
- Data deletion following termination
- Data transfer on termination

The length of an initial term depends on cloud service with negotiated agreements typically having longer terms. Use of auto-renewal clauses are common and typically involve an

advance notification system. Some negotiated contracts may seek longer terms with guaranteed renewals for reasons including continuity of service and guaranteed pricing.

In addition to expiry, cloud service contracts usually specify a number of termination events. Material breach including breach arising from the activities outlined in the AUP and non-payment are common. Other events of specific relevance to organisation contracting cloud services are insolvency, acquisition or compliance with regulator requests. Insolvency is a specific termination event that is typically addressed however the cloud service providers may not necessarily provide adequate detail on how client service continuity or treatment of data will be addressed. In the event of insolvency, clients should consider whether provisions for the return of data in the event of the winding up of the provider. It is unclear whether these provisions could be enforceable as against a receiver (McDonagh 2012). The acquisition of the cloud service provider or even change of control is typically not addressed. Some clients may seek to include such a term particularly where the acquirer or new shareholder is a competitor although this may reduce the attractiveness of the cloud service provider. Finally, in heavily regulated sectors, clients may require the option of termination where such termination is requested by a regulator, government agency or such similar third party.

The treatment of data on termination is a key issue and is often cited as primary factor in vendor lock-in concerns. There are three main issues:

- data / application preservation following termination – the client will want to ensure that they have a reasonable amount of time to gain access to their data / applications and transfer this data / application to a new service, if appropriate;
- data transfer - the client may want support transferring their data or applications to a new service; and,
- data deletion following termination – the client will want to ensure that their data or application has been deleted from the cloud service following termination.

Bradshaw et al. (2010) note that cloud service providers deal with data preservation following termination in three ways namely, by provision of a grace period at the end of a service contract, immediate deletion at the end of service agreement or through a hybrid approach neither obligating to preserve data but not undertaking to delete data and offering a grace period at their discretion. For negotiated contracts, agreement on data preservation is essential. It should be noted that Bradshaw et al. (2010) also identified other approaches, primarily relating to free services, including Facebook's preservation of deceased member accounts and Zoho's reservation of rights to terminate 'inactive' accounts. The requirements under the Data Retention Directive, as discussed earlier, may also apply here.

A commonly cited issue by clients of cloud computing services is support for data, and indeed application, transfer in the event of termination. Whilst many cloud service providers provide tools and processes for on-boarding clients, the transfer of data and applications on termination is a different matter altogether. Whilst Hon et al. (2012) note that in negotiated cloud service contracts, some cloud service providers will commit to

return users' data in a standard format (and some routinely do so during the contract e.g. Salesforce.com), most providers do not provide assistance in transfer and if so require payment. Migration out of one cloud to another or elsewhere is stifled by a number of migration and interoperability issues and serves to exacerbate concerns regarding vendor lock-in. It should be noted that not all portability issues are initiated by the service provider. In some instances, clients require customisation that results in migration and portability issues.

Clients typically wish to ensure that their data has been deleted following the termination of an agreement. This may include, but often is not explicitly stated, replicated data for the purpose of system performance (incl. caching) and metadata.

4.2.3. Discussion and conclusions

The legal framework for the provision of cloud services is at an early stage of conceptualisation and current heavily favours the cloud service provider. It covers a wide remit of scenarios and is complicated by the multi-tenant nature, underlying chain of service provision (and the nexus of contracts that this represents) and the reliance on the Internet.

The applicability of EU law is of concern to both consumers and businesses. Greater legal certainty is required for determining when a non-EU provider can be considered 'established in the EU.' The choice of law is critical. The stipulation of US law by many cloud service providers impacts cloud service contracts disproportionately impacting exclusions and limitations on liability, and indemnifications. While current plans for reform on data protection regulation will address many issues, awareness campaigns would help businesses understand the implications of choice of law on their rights. Similarly the location of data in storage, transit and processing has been identified as a concern by numerous studies and most recently the IDC study for the Commission. While some providers, notably Amazon.com and Microsoft, will provide assurance on storage and processing, this is far from the norm.

- Support of proposals for the provision and funding of standardised technical approaches and tools to support the provision of greater transparency on the location of data within the cloud.

The reservation of rights to vary the provisions of agreements introduces uncertainty. The use of updates via websites without notification exacerbates this uncertainty.

- Support of proposals to stipulate minimum requirements regarding changes to the provisions of contracts, the notification of such changes and remedies for those clients for whom the changes are material.

The use of Acceptable Use Policies requires greater scrutiny. The language used may not be feasible for clients to meet depending on where they are situated along the chain of service provision and particularly where the clients are at arms-length from end users.

- Encourage standardisation in this area and support proposals for model clauses and language for Acceptable Use Policies.

There is uncertainty over IP ownership in a number of cloud computing instances. These include ownership of IP where applications are developed by clients or end users on a cloud provider's IaaS or PaaS platform using the cloud service provider's tools and ownership of improvements or bug fixes on cloud services. There is a degree of incompatibility between the current IP frameworks and cloud computing; the former is largely based on geographic location whereas the latter is not. Legislation needs to consider whether a more proactive role in addressing IP issues in and of the cloud is needed and also advisable. The extent of change introduced by cloud computing should not be underestimated and one might argue that cloud computing highlights the need for systemic revision of the IP system. While discussions are ongoing in relation to the Copyright Directive, cloud computing impacts a wider set of IP.

- Consider a comprehensive review of IP law across the EU and support proposals for model clauses addressing the issues outlined.

The Commission has identified that trustworthiness, or rather the lack thereof, is a major barrier to the adoption of cloud computing. Many of the contractual provisions considered standard in cloud services contracts lack transparency, which is recognised as a key element in the fair and legitimate processing of personal data. These include lack of transparency in relation to the security of data, performance levels and metrics, audit rights, use of metadata, the identity of data processors and subcontractors along the chain of service provision and indeed the location of data in storage, in transit and while being processed.

- Support of optional proposals for measures that might be taken to provide greater transparency for businesses. These may include the development of technical tools for assurance and accountability, for use by various stakeholders including end users, regulators and the service providers.

Many consumers and businesses make use of cloud computing services due to the perceived redundancy and resilience provided by the cloud. The uncertainty regarding backups is of concern and goes to the core of trust in cloud services.

- Encourage stipulating minimum requirements for provisions relating to backups of cloud services, which introduce certainty.
- Support of proposals for soft actions including awareness campaigns to address this issue.

Many cloud service providers will not provide full disclosure on their security arrangements. Those providing enterprise cloud services relay on third party certification of their security and IT governance policies. Conventional information system assurance (and associated trustmarks) have been subject to criticism for being (i) largely reliant on human

intervention (with limited capacity), (ii) limited in scope, (iii) passive, periodical and retrospective, (iv) lacking transparency due to reliance on internal monitoring, (v) lacking warranties and (vi) subject to co-optation risk (Schouten 2012, Endeshaw 2012).

- Support of proposals for the development of EU cloud-specific certification and the adoption by public sector organisations within the EU.

Policymakers, academia and industry have called for research on trustmarks in the cloud computing context (Lynn et al. 2013, IAMCP 2011, Global Access Partners 2011, Robinson et al. 2010). Research suggests that trustmarks have the greatest effect on perceived trustworthiness in an Internet context (when compared to objective-source third-party ratings and advertising-derived implications), influencing respondents' beliefs about security and privacy, general beliefs about firm trustworthiness, and willingness to provide personal information (Aiken/Boush 2006). Next generation trustmark systems address the failings in traditional assurance based systems and trustmarks by providing an active dynamic trustmark that could provide continuous machine-based evidence that cloud services meet the trustmark requirements consistently and repeatedly (Lynn et al. 2013).

- Support for proposals for technical tools and funding for the development of an EU-wide trustmark for cloud computing. In addition to increasing transparency on service quality, this may serve to distinguish EU cloud computing services from those offered in third countries.

There is uncertainty regarding the provision of access of data to law enforcement agencies. Existing legislation is not uniformly applied across the EU and was not drafted with cloud computing in mind e.g. the Data Retention Directive. There is considerable perceived legal uncertainty with regards to the disclosure of personal data to a third country. This would seem to be particularly the case with regards to the US and specifically the use of National Security Letters, which limits the ability of service providers to reveal that they have received a disclosure order. Uncertainty is further exacerbated by the complexity and lack of transparency in the chain of service provision in cloud computing. It may be difficult to determine which legal jurisdiction applies in any given circumstance.

- Consider support of proposals that address issues relating to jurisdictional uncertainty. This may include supporting initiatives to stipulate compliance with EU law where the client (and the end users) are based in the EU, minimum requirements regarding the disclosures to a third country and obligatory use of MLATs. In addition, the Parliament may wish to consider supporting awareness campaigns to address uncertainty in relation to US measures.

Finally, it should be stated that the Cloud Computing landscape is complex, fragmented and at an early stage of conceptualisation. Therefore, policy intervention in the contractual relationship between parties and particularly organisations is limited and needs to be taken with care.

4.3. Issues in market competitiveness

The competitiveness of markets is a crucial point for the further development of Cloud Computing in Europe. In a first line it is crucial for users, who would benefit from competitive markets in terms of price and variety of offers, but also for service or product providers who would benefit from a broad set of applications. But as shown in the previous sections the situation of the market today is ambiguous. On the one hand there are many small and medium sized companies offering services based on Cloud technologies. On the other hand there is a handful of global players, mostly of US origin, which already gained important share of the market. Based on the fact that that Cloud is like other markets for software and IT services a two-sided market shaped by network effects, this situation bears some risks for the competitiveness of the market. Because in such markets there is due to the networks effects the tendency that only a few players will establish strong platforms, which create their own closed ecosystems consisting of a strong user base on the one side and a broad numbers of other service providers offering further solutions and applications for the platform (Veugelers et al. 2012, 18-19). Though such a system can have advantages for both sides, the problem is that the platform owner can misuse its power. That in particular in the IT sector such a tendency exist is shown by the historical cases of IBM in the 1970s, Microsoft in the 1990s or the current discussion on the dominance of Google in the search engine and advertising market.

The first direct issue is that a platform owner could create barriers, technical and legal, that makes it hard to migrate easily to offers of other providers. This problem of vendor lock-in will be dealt in the first part of the section. While parts of legal problems were already addressed in the previous section (see 4.2), we will here based on this results supplement it with the related technical issues of standardisation and interoperability. Beside the direct customer impact the vendor lock-in would also impact other competitors by creating additional market entry barriers. From an overall point of view this situation could also implicates some issues. A first point is that that such a situation of few dominating platform owners could lead to the fact that positive economic and societal impacts could diminish or even turned into the opposite. From a European perspective this is especially critical since many of the big players at the moment are not of European origin. One way to answer this would be the creation of regulatory framework mitigating the risk of such a behaviour. As shown in the previous sections some steps towards this situation are already undertaken, for example the question of data portability (see 3.4 and 4.2). However another way is to create a vivid and competitive market environment as well as the creation and support of a competitive landscape of European providers.

However, since the raise of the software and IT industry, there is the challenge that the European IT industry is underrepresented. Though Europe is the second biggest market for IT worldwide, the number of European companies among the biggest one hundred is low, depending on the definition and scope between a few to a maximum around 15 (Aumasson et al. 2010, 208-210). Over the last decades many initiatives were started on national or the European level to change this situation, but none of them changed the situation significantly. In particular since first internet boom around 2000 the question, why in particular no new fast-grown players like Google, Amazon etc., which used the potential of disruptive innovations in the industry, emerged in Europe, was placed in the focus of the

discussion (Veugelers 2009, Aumasson et al. 2010, Veugelers et al. 2012). There are two reasons to focus on the lack of fast-growing companies in the second part of this section. On the one hand Cloud is still an emerging segment with a potential for disruptive innovations in technology and business, so that especially here is chance left to improve the competitiveness. On the other hand the topic refers as recent analysis has shown (Veugelers et al. 2012) many of the most often named challenges in the past. The following section will deal with a topic which is also strongly related to these issues, namely the fragmentation of markets in Europe. But given the fact that it encompasses also other issues and that it has also an importance for the creation of competitive market, we will deal with in the third part.

Finally there are two issues that were mentioned already in previous sections, the provisioning of infrastructure and the creation of human capital. At a first glance both are not directly competitiveness issues, but in longer perspective these two factors will have a strong impact on the competitiveness. Skilled and trained employees are fundamental for both, provider of cloud solutions as well as their users. Especially the ability of users to exploit the potentials of Cloud and related other emerging technologies like Big Data will enable to realise the positive societal and economic benefits of it. Consequently the availability of human capital is strongly impacting the competitiveness, especially since there is already a discussion on the lack of skilled workforce. Similar to that the availability of network infrastructure, mobile as well as flat wired connections, will impact in the long run the competitiveness of the market. The reason is that Cloud Computing will enable more and more digital business, which will lead to a strong increase in the demand of network. There it is necessary to develop these infrastructures further in order to realise the benefits. The resulting challenges in both areas, human capital as well as infrastructure provision will be addressed in the two last parts of section. It will conclude with a discussion including the description of possible policy options.

4.3.1. Standards. interoperability, and vendor lock-in

The issue of standards, interoperability and vendor lock-in exist since the early days of the computer business. Nevertheless many studies in the recent years underline that this complex of topics is still of high relevance and may even gain more importance due to Cloud Computing (f.e. Aumasson et al. 2010, 191-198, Ecorys 2010, ESA 2009). The reason is that one way to exploit the full potential of Cloud is either to change providers according to needs and priorities like price and service offers or to combine different solutions to get the best combination of different applications. To do so it would require that standards and interoperability is given by all providers, but as shown this is often not the case. Moreover some providers try to control their own proprietary software world by restrictive IPR use or non-disclosure of specifications. This might have negative consequences for users, who experience a vendor lock-in, as well as for other providers, who are not able to offer interoperability of their own solutions.

Vendor Lock-in refers to a situation in which a customer is dependent on a vendor for products and services such that he or she cannot switch to another provider without suffering substantial costs and thus are locked in to continuing the relationship with that vendor (Zhu/Zhou 2011). Software vendors can lock-in customers by designing software

incompatible with those of other vendors, using closed architectures or proprietary standards that lack interoperability with other software vendors, and by licensing the software under exclusive conditions (Kucharik 2003). Lock-in may be a deliberate strategy of the software vendor as it reduces the bargaining power of the customer by increasing switching costs thus providing the software vendor with a possible competitive advantage. Similarly, customer-driven customisation may result in lock-in as the customisation impacts interoperability. It is clear from our review of literature in this area and the legal landscape that a number of factors contribute to vendor lock-in in the cloud computing context and specifically in the case of data and application transfer on termination. Here the client may be at a disadvantage as a result of contractual terms - the threat of immediate deletion, short grace periods or lack of migration assistance – or for technical reasons. The former has been discussed earlier in section 3.14. A number of technical factors may contribute to exacerbating the impact of these contractual provisions including data lock-in and application lock-in.

Data lock-in can arise where cloud service providers do not provide export tools or support the export of data in a non-proprietary format. While many SaaS providers provide tools for common data formats, this is typically not the case with PaaS providers where the onus is more likely to be on the customer to develop and create appropriate export routines. Application lock-in typically occurs where an application has been designed for or customised for a specific customer. In PaaS environments, the runtime environment may be customised to meet the service provider requirements. The customer software developers may customise their applications to address these customisations. In IaaS environments, lock-in complexity is exacerbated. IaaS providers using hypervisor-based virtual machines often bundle the software and VM metadata together for portability within the IaaS provider's cloud. Furthermore, depending on the IaaS offering, the data stores may vary widely. Application-level dependence on specific policy features would further limit migration. These factors, combined with discrete data portability issues, can result in increased complexity for migration to other IaaS providers.

Vendor lock-in introduces higher costs associated with software and data migration and in some instances end user training. While using a full-service provider reduces the risk associated with the chain of service provision, often inherent in the cloud service provision, it also may have the effect of compounding lock-in and increasing switching costs. Open standards for data (including metadata) portability, data stores (including policies), applications and API calls would reduce the impact of lock-in. However, cloud service providers may not have sufficient incentives to support such open standards and in fact, may have as already indicated incentives to do the opposite.

Changing this situation is quite difficult. The point is that standardization processes from a European perspective are difficult, because normally international and national standardisation bodies are often far behind the dynamic development within the IT industry. As a consequence a few global players, mostly of US origin, are able to introduce their own de facto standards. For European companies the only choice left is to follow these developments, but which is particular very difficult in the early stage of a development because the choice is exacerbated by multiple proposals for standards. Additionally many

institutions that deal with standardisation beside the official national bodies like the different IEEE WG are also dominated by American companies. Only a few Europeans are able to participate in these bodies, which led to a difficult development. On the one hand the influence of the few Europeans is limited. On the other hand they also pursue different, contradictory strategies, i.e. either promoting market and proprietary standards or open standards. Overall this creates a situation where standards for data or software migration are hard to achieve.

Similar to the situation regarding standards the situation for interoperability, i.e. the ability to communicate and interact with other systems is also problematic. This topic is in particular an important issue for Cloud providers, because to offer their specific solutions it is required that it can be used in cooperation with different other solutions. An example for this problem would be an industry-specific extension for an enterprise application. Given the fact that this market is dominated by a few players, which only offer limited insight, the company would need to develop several specific programming interfaces (if even possible), which would either increase their costs by doing so or limit their potential by focusing maybe on one platform owner. Overall this is limitation of competition and hinders the creation of new products and services based on such solutions (Nessi 2008, ESA 2009).

4.3.2. Market fragmentation

The fragmentation of the European market is in general an issue for both, users as well as providers of Cloud Computing. Nevertheless, in the past the discussion on the fragmentation with respect to IT often focussed on the disadvantages resulting from it for the competitiveness of the European providers (Aumasson et al. 2010, 218-226, Mowery 1996, Steinmueller 2004). Despite of that it is also an issue for users, business user as well as consumer, because it also relate to issues like the fragmentation of the regulatory framework. During the time many problems were discussed including socio-cultural aspects such as language barriers or mentality. However since parts of this broad spectrum are already addressed for example by the discussion of the draft regulation on data protection, we focus here on challenges of cross-border operations between the different member states beyond that. It includes in particular cross-border payments and transactions as well the harmonization of the regulatory framework.

The problems within cross-border transactions and payments comprise a range of issues. Many of them were already addressed by the Commerce directive (Directive 2000/31). Though some points are already addressed and other like the single payment area (SEPA) are on their way, there are two issues left. Firstly there are a few challenges that are specifically posed by Cloud Computing. Secondly there are other points where due to different implementations by the member states, problems can occur. A good example for the first is the case of the VAT regulations in case of European provider and European customer situated in different countries, while the data processing and delivery may take place in further countries. In such cases the different regulations and the complexity of the system can lead to difficulties, in particular for small or medium sized companies with low experiences and formal structure, i.e. legal department. Some argue that this seems to be no problem for US companies entering the European markets, which is at least partly true. However as long as they only operate from the US, which most small firms do, the sales

taxes, the counterpart to VAT, are raised and cannot be reclaimed. In case of other US firms that also open operations in Europe like Amazon or Google, it must be stated that they often mange to achieve a certain size before they do that. This includes also legal and tax departments, which are as shown by recent discussions, very firm with the specific characteristics of the European tax system and its loop holes. Overall it shows that there are things left that need to be clarified, though the Commission decided against an update of the directive (EC COM 200/942). It might be sensefull to review this and address in a further process specific points with relevance for Cloud Computing.The letter point relates to further harmonisation of the regulatory background. A first step regarding this is the planned regulation on data protection, which will create a harmonisation within the member states. Other parts relate to the consumer protection and consumer rights, where the new directive was recently adopted (Directive 2011/83/EU). Here strong collaboration and further harmonisation in the implementation process of the member states would help to increase legal certainty for both, users as well as providers. Finally there are further activities planned that would support the further harmonisation such as the Common European Sales Law (COM 2011/635/EC). Also here the particular needs of a single market for digital services need to be addressed.

Beyond this it should maybe also noted in this context that cultural diversity in terms of languages or mentality should be not only considered as problem for several reasons. Though the US may have a common language the culture varies strongly between the northern and southern parts as well as the western and eastern parts. Moreover diversity can also create innovation as shown by the example of Skype, which was invented to circumvent the diversity of the European telecommunication system. Overall it shows that diversity is also a chance, if it is perceived in the right way.

4.3.3. Lack of fast-growing companies

The lack of innovative, fast-growing enterprises refers to "overaging" of European companies even in high tech sectors, i.e. the fact that the majority of European companies are in average older than in the US. This is considered to be another reason for the lagging behind of Europe in the productivity growth (Phillipon/Veron 2009).Similar to the market fragmentation it addresses a broad set of issues, but in opposite to it they mainly deal with challenges and issues for providers, less for customers. Nevertheless, both are strongly intertwined. However, the set of issues and challenges addressed in th is discussion includes the lack of entrepreneurial activities in Europe, the role of the state in supporting companies, in particular by public R&D spending and procurement, as well as the lack of capital for financing growth and innovation, especially the lack of venture capital. Additionally the discussion is also often enlarged by a general discussion on the entrepreneurial culture, which summarise these aspects, but also includes other points like the regulatory framework and the resulting market fragmentation as a barrier.

Regarding the lack of entrepreneurial activities the many analysis show that the level in Europe is not as high as in the US or other world regions (Aumasson et al. 184-185). Detailed analyses even show that the differences between the member states vary strongly (Eurobarometer 2010), which cannot easily be explained. But as other research shows the number varies lso strongly in time, depending on the development of the overall economy

and other factors. Finally there is also the argument that the difference is not big enough to explain the overall lack and may not address the right problems with regard to the share of fast growing companies (Veugelers/Cincera 2010). Beside market fragmentation they identify further reasons like the missing link between the actors in the European innovation system, in particular science and business, the lacking role of the state as intermediary between actors, the lack of competition between young and old companies as well as the lack of financial capital (Veugelers et al. 2012, 9-12). These are considered as main reasons why promising companies either fail to grow beyond a certain size, that they fail or that they are taken over either older European or US companies.

A first point that is often discussed with regard to the missing link of actors is the low level of R&D spending, in particular the business R&D spending, where Europe significantly lags behind the US. In particular the software and IT service as well as the internet sector, which are fundamental for Cloud Computing, are affected by it (Turlea et al. 2010, 75; Turlea et al. 2011, 55). The other point discussed is the role the state as an intermediary between the actors. This discussion refers in particular to its ability as one of the main procures in the field, becaus the state, governments and public bodies, are responsible for round about 20% of the market volume in IT services and software within the EU member states (Aumasson et al. 2010, 231-240). This resulting market power could be used to reinforce technological and economic developments desired. This is clearly done in the US, where the Cloud first policy implemented by the current government sets a clear sign for Cloud Computing. Overall there are two measures, normal procurement and pre-commercial procurement, which could be used in this context. In particular pre-commercial procurement is seen as a possibility to create a link between science and business. Moreover some describe it also as mean to bridge what is identified as the "valley of death" between innovation and market success for innovative companies (Wessner 2008). In many cases the literature refers here to the SBIR program in the US, where the state as procurer offers small companies the chance to develop innovative solutions desired by public agencies. Beside the the financial R&D support the program is also directed at helping the companies to find further funding in a later stage by a close integration of venture capital companies (Wessner 2008). Though this is a very successful example, the question if and how such pre-commercial procurement could be used in Europe is still point of discussions (Edler 2011, OECD 2011). Normal procurement processes are more likely to be used for other other purposes. As already indicated with the example of the Cloud first principle it can be especially used to reinforce technological and economic developments desired. This plays in particular in the field of standardisation and interoperability, as mentioned in the related section before. In Europe this possibility is recognized and for example the recently launched European Cloud Platform which is aimed at a joint procurement of Cloud Computing solutions in the public Sector (COM 2012/529/EC), addresses this topic. Additionally there are also activities with regard to the promotion of pre-commercial procurement. A first step was the adoption of a communication (COM 2007/799/EC) in 2007, which recommend the implementation of such mechanism in the EU member states. But since the use of it is still low and many legal aspects were mentioned two new proposals (COM 2011/896/EC and COM 2011/895/EC) where launched, which are aimed at replacing the existing public procurement directives in order to ease the implementation of pre-commercial procurement schemes within the member states. Both

are still under negotiations. Moreover also further activities are announced with respect to the coming Horizon 2020 program. Already in the currently closing 7th framework program some initiatives such as the introduction of public-private partnerships were started, which are aimed to raise the company level R&D spending.

The second one is the lack of financial capital, which refers the founding and growth of companies. In most cases it refers to at least two points: Firstly the restrictions to receive external financing from banks or other sources, and secondly to the lack of venture capital. While the first one is at the moment even more problematic, the latter one exists as topic in the European innovation policy for a long time. Analysis show that the level of VC spending in Europe is in total as well as per employee in the lower in the IT sector than in the US (Schleife et al. 2012, 32-33). Moreover there are analyses arguing that European VC was often invested in wrong directions (Weber et al. 2011), only focus on later stage investments as well as the argument that Europe lacks of promising investments (Fransman 2011). Most recently Veugelers et al. (2012, 25-35) showed empirical evidences that the lack of particular venture capital impacts the performance of the ICT sector in Europe. However, based on earlier studies it also addresses the point that not only companies in the early stage suffer from it, but also in particular that fast growing companies also faces problems to finance their growth Cincera/Veugelers 2010). Given the importance and attention, which is paid to the topic, it is not surprising that there are already several efforts to boost the European market for venture capital in the making. Recently the Commission addressed the problem in three communications (Small Business Act (COM (2008/349/EC), Innovation Union (COM 2010/546/EC), Single Market (COM 2010/648/EC) announcing activities towards a single European venture capital market, increase the access to finance for innovators or the continuation of the risk-sharing financial facilities. Parts like the RSFF (risk sharing financial facilities) are already implemented or on their way as the proposal for new regulatory regime for venture capital shows, but mostly only in early stages.

However, since the topic exist for a long time and also many initiatives were undertook before, but the situation did not really improve, one could raise the question if there are factors influencing this. Some research indicate that beside legislative and financial support, further aspects like the entrepreneurial culture including a venture capital and business angel culture also play an important role (Fransmann 2011). With regard to this the example of Israel might show that more is needed to establish such a culture. This process began back in the late 1960s and 1970s, when Israel started a programme for high-tech industries, especially in the defence sector. Subsequently, policies were implemented which targeted a larger human capital base, improved scientific quality and strengthened science-industry relations. While at this time it was focused on defense related activities, the focus shifted to other industries after the economic crisis of the 1980s. The activities were then steered by the newly founded Office of the Chief Scientist (OCS), which aimed at supporting high-tech companies throughout the whole life cycle. This office launched several programmes of which the YOZMA programme, which was aimed at creating a venture capital market, turned out to be a huge success. But also other programs aimed for example at pre-commercial procurement and increasing science-industry relations, were successful (Breznitz 2006; Breznitz 2007). This shows that the

problem can be only addressed by a holistic approach taking into account the whole life cycle of a company as well as the whole value chain of the industry and innovation system.

4.3.4. Broadband coverage

As already outlined in section 2.2 and 2.4 availability is a crucial precondition for the success of Cloud Computing. One major aspect of availability is the existence of enough bandwidth capacity. Since the broadband penetration is one major pillar of activities of the EU and its member states in the recent years, it is not surprising that Europe overall has made some progress in the overall penetration with fixed and mobile broadband. However a closer look reveals some critical details. First of all the penetration varies strongly between the different member states in Europe as well as in the member states itself. In particular rural areas clearly less well connected than cities (EC 2013, 46). This creates an imbalance in leveraging the benefits of Cloud between the different regions in Europe. Maybe even more critical is another. Though the number of so called Next generation Access, which are capable of 30 Mbps and more raised in the last years up to 20,3% of all fixed line access, the share of FTTB/H (Fiber to the building/home) only amounts for 25,8% within the NGA lines, i.e. only 5,1% of all. In that regard Europe lags behind other world regions (Japan 42%, South Korea 58%, US 9%). The critical issue here is that other NGA technologies like vDSL or Docsis 3.0 only have limited perspective in further grow of bandwidth behind 100 Mbps, but in the long run the vision of broad adoption and heavy utilization of Cloud Computing as needed to realise the positive benefits pose the questions if the current bandwidth development will be sufficient for these future requirements. Though the coverage in high speed mobile access is little better with 26,2% coverage of LTE in Europe (EC 2013, 72), the question remains if it will be sufficient for future requirements.

Overall there is no clear answer to that in the current literature in terms of clear forecasts, which bandwidth for fixed and mobile networks is needed, but there is the tendency to state that the current bandwidth is not sufficient for a heavy and foremost data-intensive utilisation of Cloud Computing as foreseen in many use cases like Big Data applications. Therefore the question is raised how to continue with the further broadband deployment. In particular the further deployment of FTTB/H technologies would require a high amount of further investments, which might be the reason why some telecommunication providers try to exploit the existing infrastructures such as DSL as much as possible. But if they are forced to proceed this shift towards new technologies, it might be that questions arises how to finance this. One solution could be either to increase prices for customers or they could try to claim usage fees from provider of services using the infrastructure. Both is from an overall view not desirable. The first way would maybe lead into digital divide within the society and presumably thereby led into a lower utilisation of Cloud Computing. The consequences of the latter approach are discussed quite controversial within the debate on net neutrality (EFI 2011, Heng 2011). Though in particular the effects on emerging and innovate service offers are one major point of this controversial, which could not be totally solved until now, the effects of such approach could also negative effects on the competitiveness of the market and thereby on the overall potentials and impacts of Cloud Computing. Nevertheless, there is also the legitimate question how the telecommunication

providers should finance the further development. All these points need to be addressed in the future planning for broadband infrastructure in Europe.

4.3.5. Lack of skilled workforce

Similar to the case of network infrastructure the development of the human capital base is a factor, which is in a mid and long term perspective a necessary framework condition that influences strongly the competitiveness of Europe in Cloud Computing. As shown in previous sections (see 2.6) a sufficient level of skilled workforce is essential to realize the positive impacts of it, because only a continuously skilled workforce will ensure that the IT industry itself is capable to develop new solutions in the emerging field of Cloud Computing and related areas like Big Data, which could work as one driver for the utilization of it. Moreover these new solutions do not only require skilled developers, they also require skilled and literate IT users, which is able to fully exploit the potentials offered (Aumasson et al. 2010, 263-272).

Due to the fact that the shortage of literate professionals, IT developers as well as skilled users, is not only a recurring claim of the different industry associations, but also well researched by many studies on the member state or EU level (Korte et al. 2009), there is not a need for more awareness regarding the general problem. Moreover many initiatives are already aimed at addressing the problems. This includes the e-skills program of DG Enterprise, which exists since the mid 2000, addressing the increase of skilled IT labour force. Above that the pillar six of the Digital Agenda is also dedicated to fight computer illiteracy and labour shortage, including increasing the share of women in IT labour force and consumer education. Though this is already a broad spectrum, there is a need for a further increase of workforce, which may require new approaches how to enlarge the the skilled workforce in alternative ways. Consequently there is need to evaluate how other countries and regions deal with this problem. Another point is that the Digital Agenda addresses the need to include more women, but there might be also other groups that could be better included. Examples are the growing number of elderly people, which are often considered as “too old” (digital emigrants), or young students, that stopped formal IT education at a university or similar institution. While the potential of first could be for example addressed by increased measures for lifelong learning especially in IT, the latter one could be addressed by special programs that offer the chance to receive another formal degree of education related to IT. Finally there is also still a group of less formal educated, young people, which may have an affinity to IT that could be addressed.

Another final point is that there is lack of knowledge how the requirements for skills will change in the next years. It refers to two points. The first is the change of requirements caused by Cloud Computing and other technologies such as Big Data. A first approach was done by a study commissioned by the European Commission in 2011, which clearly underlines the changing requirements due to Cloud Computing and the resulting need for more support in the creation of such skills, in particular for SME using Cloud Computing (Laugesen et al. 2011). Though this is partly reflected in the current IT literacy programs like e-skills program, there is a need for further research due to the fast moving character of Cloud Computing. The second point is the possible change of skills requirements caused by a growing number of young people that are familiar with all kinds of digital technologies.

This may also impact skills requirement in future, in particular for example regarding data protection or similar challenges related to Cloud.

4.3.6. Discussion and conclusions

Concluding we can state that the market competitiveness for Cloud Computing in Europe shows some significant issues that need to be addressed. But as also outlined we focused on the most important one's from our perspective, but there are others, which are partly interrelated to the issues discussed here. In the following we will shortly summarize and discuss the results of the analysis and present options how the identified challenges could be addressed.

The issues analysed can be differentiated according to their way of impacting the competitiveness. It is obvious that vendor lock-in, standards and interoperability have clear direct impact on the competitiveness for both, users as well as suppliers. In case of the fragmented market have a direct impact, but as outlined in the analysis it also touches points that have a more indirect impact on the market. Nevertheless, all points also are relevant for users/customers as well as provider. In this perspective the lack of fast-growing companies, which similar to market fragmentation refers to broader set of challenges like the level of R&D or procurement policies, is mostly related to the providers and their competitiveness, in particular European providers. The impact for users/customers is clearly indirect, because the increased competitiveness could lead to better offers, but it is not necessarily the case. Finally the infrastructure and human capital only have an indirect impact and can be considered as foundations for the overall competitiveness in the digital world. But as shown by the analysis there are clear links underlining their particular importance for the further uptake and thereby competitiveness in Cloud Computing for Europe.

In case of vendor lock-in, standards and interoperability the reduction of choice for customers and the resulting decrease of competition among providers are obvious negative impacts. Though concentration processes are not fully avoidable, especially in markets shaped by network effects and also reduces for example search costs, it is necessary to limit the possible negative aspects by addressing the related issues. One possibility is the contractual question of data portability and the time the provider needs to keep the data (retention) if a customer wants to change. Though it is addressed for personal data within the draft regulation (see 3.4), but there is need also for other business data. Another way to do so is to support standardisation and interoperability. In particular the problem of the low speed of official standardisation in ICT was also addressed with the new regulation on standardisation adopted in 2012 (Regulation 2012/1052/EC). However the implementation in particular in the area of ICT will require further efforts, in particular the inclusion of the industry driven bodies. Further important steps are the introduction of an European Interoperability Framework and Strategy (COM 2010/744/EC). But this also needs to be implemented. From that point of view the following policy options can be considered:

- Support of proposals to stipulate minimum requirements regarding data portability and retention periods to support migration.

- Support of proposals for soft actions including awareness campaigns, technical support tools and funding thereof.
- Support for the implementation of the EIIF by implementation in public procurement processes
- Support of participation of European member, in particular from SME, in industry driven standard bodies

Market fragmentation includes many aspects ranging from the regulatory framework to socio-cultural aspects. As outlined are some already addressed in other sections of this report, while others like cultural diversity, beside the fact that is unclear how to address them directly, maybe should be not only considered as problem, but also a chance for Europe. Nevertheless there are a still many points left where the analysis showed the need and possibilities of actions. Among others there are many things like for example the VAT system, payment systems or others that still can form a barrier for cross-border activities. Though there are addressed by the eCommerce directive and the Commission decided after a review not to update, there a still issues left as indicated by the Commission (COM 2011/942/EC). Other areas that need to be addressed are the harmonisation of the regulatory framework. This is partly ongoing via the planned draft regulation on data protection. Above that the recently adopted consumer rights directive should help to harmonize this area, though it will require efforts to implement it in the Memeber states. Finally further aspects are the support of further ongoing activities aimed at the creation of a real single market such as the Common Sales Law is necessary. The resulting policy options are:

- Address the issue of Cloud specific aspects within the eCommerce directive.
- Support the harmonization of data protection rules through the establishment of a common regulation.
- Support of the implementation of the consumer rights directive.
- Explore and support further options to create a single market for digital services, e.g. the Common European Sales Law.

Similar to the market fragmentation the lack of fast-growing enterprises refers to a broad set of issues, but in opposite to it they mainly deal with challenges and issues for providers, less for customers. Nevertheless, both are strongly intertwined. The spectrum in that case reaches from the lack of entrepreneurial activities in Europe, the role of the state, i.e. public R&D spending and procurement and aspects like the lack of capital for financing growth and innovation. Overall this is seen often as lack of entrepreneurial culture, which then often includes aspects like the regulatory framework, which are here covered in the section of market fragmentation. Regarding the lack of entrepreneurial activities the analysis has shown that the level might be lower as in other world regions, but that overall the difference is not as significant as sometimes described. However there are considerable differences between the member states, which cannot easily be explained. But as further shown it might be not only a problem of founding new enterprises and or the innovation of new products and services. However, there are some enterprises that may have the potential, but that they do not grow big enough for different reasons. The result is that the majority of European companies are in average older than in the US. Reasons are that the

promising companies either fail to grow beyond a certain size, that they fail or that they are taken over either older European or US companies. Market fragmentation is, as outlined before, seen as one reason, but there might be also other points. But also the lack of a sufficient capital for growth is also considered to be another reason for this development, because many of these companies are either not able to finance the so called "valley of death" between innovation and market success or they are not able to finance the continuous fast growth. This refers to two points. The first one is the role of state, which can use public R&D funding, which is particular in the software and internet sector very low, as one mean to bridge this gap. But in recent discussions the role of the state as procurer, i.e. in form of innovative procurement as well as normal procurement, has gained more significance (Veugelers et al. 2012). The second one is the lack of venture capital in Europe, which is similar to the market fragmentation one of the most often mentioned problems. In the case of the procurement the Commission launched several initiatives, but there is still a great variety in Europe left. In the latter case there were many new initiatives in the recent years, including the RSFF as well as regulatory measures to improve the European VC markets, but the effect until now is not obvious. It might be that beside legislative and financial support, further aspects like the entrepreneurial culture including a venture capital and business angel culture also play an important role (Fransmann 2011). Examples are other countries like Israel, which showed that in particular that a strategic use of measures was a key success factor. Based on that possible policy options are

- Support the further integration of single European venture capital market.
- Explore possibilities to support young companies to grow rapidly beyond national borders.
- Support soft measures to increase entrepreneurial activities, including such measures as promotion of "second chance".
- Support soft measures to stimulate the growth of a European culture for entrepreneurship.
- Address the issue of a coherent policy framework combining measures in support of the Cloud and other digital industries (strategic industrial policy).
- Address the issues of a missing link between public R&D funding and public procurement, in particular innovative procurement on the EU and member state level.

In case of the infrastructure provision the analysis has clearly shown that though there are many progresses made regarding the broadband coverage and penetration in the EU, there is still a need for more. The vision of a society utilizing Cloud Computing will raise future requirements regarding coverage and penetration that in mid and long term perspective cannot be solved with the development as it is shown today. Consequently, there is need to address the identified issues in different ways. The first issue is the problem of imbalanced development in Europe, where the differences between and within member states vary partly strongly. The second issue is the question how to develop the NGA technologies in a manner that it will fit to the needs arising from Cloud Computing and related or similar trends. Finally there is the challenge how to finance the costs of a further development of network infrastructures under a fair balance between the needs of the telecommunication

providers on the one side and user, end users as well as service providers, on thither side. Options addressing these points are:

- Address the issue of imbalance in broadband coverage and penetration in between and within the member states, in particular the problem of rural areas.
- Support the review of the current broadband strategy beyond 2020 against the background of the needs resulting from a growing utilization of Cloud Computing.
- Support the review of best practice in other countries to establish an FTTB/H infrastructure.
- explore the problem of financing future infrastructures ensuring a fair balance of interests for all stakeholders.

Finally the case of human capital also underlines the need that achieving and maintaining a leading role in a mid and long term perspective requires adequate framework conditions. In particular for Cloud and related technologies like Big Data, which could work as one driver for the utilization of it, require more and more literate professionals. But as shown this requirement is limited to developers, it also exist on the side of users. This raises the risk that there will be an increasing race for qualified persons between the both sides, which in the long run may impact the overall competitiveness of the economy as a whole. Given the fact that there is already a lack of qualified personnel identified in Europe, there is strong need for further actions in future. Possible options are:

- Support the integration of skills requirements of emerging segments like Cloud Computing or big Data within the existing literacy programs.
- Address the need of further measures to increase the number of qualified persons.
- Support the implementation of programs dealing with the inclusion of groups less represented in the IT workforce such as women, elderly people or young people with less formal education.

5. CONCLUSIONS AND OUTLOOK

5.1. Conclusions

Concluding it can be stated that the report shows the potentials of Cloud Computing for Europe. In particular regarding employment, creation of new businesses and economic growth there are indications that Cloud Computing and related developments like the trend towards mobile usage, consumerization or Big Data can create positive impacts for Europe. But like most developments in IT the story also has two sides. Because as shown in the further analysis there is the risk that these impacts cannot be realised or even worse turn into the other direction, if it is not possible to provide sufficient environment for the uptake of Cloud Computing.

The quest for such an environment leads directly to analysis of barriers and issues, but already the discussion of the direct impacts on consumer as well as business on administrative users and the overall impacts on economy and society already indicate first issues, which can be derived from the different expected impacts and that need to be addressed. This includes general topics like the availability of broadband up to specific measures suited to address specific negative impacts like a loss of privacy by measures such as a right to deletion and others. Based on this initial analysis and taken into account the work of the previous deliverable as well as further research (literature review, interviews, workshops etc.) the analysis focussed in the following on a set of issues identified as main barriers. The first broad complex dealt with questions of security, privacy and data governance. The analysis of all specific fields shows clear issues that need to be addressed. Regarding the data security it shows a clear need for further research on the technical security for Cloud Computing as well as the need to improve certification of it. Furthermore the support of providers aligning to that could be an option. In opposite to that the question of the data protection regime is already addressed by a new draft regulation. It addresses main points, but due to the ongoing status final could not be made, but several options were identified dealing with important aspects of it. Also in the case of data retention data and third party access the uncertainties create a need for further actions, because otherwise the current concerns cannot be resolved. Similar to this is the enforcement of EU standards outside the EU another major issue, where the current measures are not suited to address the existing concerns. Consequently international harmonisations as well as a review of existing agreements are possible policy options. Beyond the e measures of the draft regulation many other contractual issues exist, mainly caused by the early stage of development of the contractual relationships and the resulting favourable conditions for provider. As shown by the analysis this refers to issues ranging from the choice of law or IP rights to service and quality issues or the termination of the contracts, which can be addressed by different policy options such as standardisation of contracts, certification process or trust marks. Related to that is the issue of the competitiveness of the markets. Here the analysis showed that legal aspects on data portability and contract termination as well as technical aspects like lack of standards and interoperability can create a vendor lock-in, which can be addressed by policy options such as awareness raising or supporting interoperability in public procurement. Another point to

improve the competitiveness is the market fragmentation, which could be addressed as shown by the analysis by a harmonization of regulations such as data protection, the review of the eCommerce directive and other measures directed towards the creation of single market for digital services. From the perspective of the competitiveness of the European Cloud provider one major issue is the lack of global player in Cloud, in particular fast-growing, innovative companies. As the analysis showed this has different, partly interrelated reasons, which can be addressed in several ways. Possible options are the connection of R&D funding and procurement, the support of entrepreneurial culture or coherent policy industry policy framework. Beside these more specific issues, the analysis also showed that with broadband coverage as well as the shortage of skilled workforce two more general framework conditions will in the long run impact the realisation of the potentials of Cloud Computing. In case of the broadband coverage the analysis showed the need to address the imbalance of regions, in particular in rural areas, as well as the exploration and adjustment to future requirements are main points. Regarding the lack of skilled workforce the needs of the IT industry as well as the user industries needs to be addressed by measures for the enhanced education and a further expansion of the workforce itself. Overall this leads to broad list of policy options, in total nearly 60, which can help to improve the current state of Cloud Computing in Europe.

5.2. List of policy options

It is obvious that due to the strong interrelation of the identified issues some identified options emerge from more than one field. Consequently there is a need to consolidate the list of options. In course of this process we also reordered according to the approach of a functional analysis in the framework of a technological innovation system, which was introduced in the initial analysis of the previous deliverable. Though this also bears some challenges, the integrated approach allows a better understanding of problems and resulting options. Within the process we identified five clusters of issues split into the following functionalities:

- provisioning of infrastructures, which addresses the availability of secure and reliable technical network infrastructures;
- mobilizing resource, which addresses the need for human capital base, i.e. extension of total number as well as enhanced education of developer and user, as well as the need to improve the financial capital situation, i.e. the access to financial capital for innovation and growth;
- legitimation and creation of markets, which addresses the need for acceptance of new technologies such as Cloud as well as the support for the creation of a working and competitive market for Cloud;
- adapting the regulatory environment, which addresses the needs to adjust and harmonize the legal framework, in particular contractual issues and data protection regime, according to the challenges of Cloud Computing;
- encourage entrepreneurship and competition, which addresses the support of entrepreneurial culture and activities as well as a fair competition environment.

5.2.1. Provisioning of infrastructures

Sufficient infrastructures

This section comprises options based on the results of section 2 and 4.3 dealing with current and future needs arising from a growing utilisation of Cloud Computing.

- Address the issue of imbalance in broadband coverage and penetration in-between and within the member states, in particular the problem of rural areas, e.g. through licensing "light", unlicensed communications with higher reach, or mandatory coverage.
- Support the review of the current broadband strategy beyond 2020 against the background of the needs resulting from a growing utilization of Cloud Computing.
- Support the review of best practice in other countries to establish an FTTB/H infrastructure.
- Explore the problem of financing future infrastructures ensuring a fair balance of interests for all stakeholders.

Secure infrastructures

Beside the question of sufficient infrastructures the need for technical secure infrastructures is another important aspect. Section 3, especially section 3.3, and parts of section 4 underline the importance of the topic for the acceptance of Cloud Computing.

- Support measures to provide awareness of the problem of insider reading and of the technical approaches towards solutions, e.g. by producing communications or conducting workshops.
- Support the development of secure servers, reliably protected against attacks.
- Support research on technical measures against insider reading and their cost efficiency.
- Consider taking steps towards incentives for use of those new approaches, provide recommendations or even request mandatory use, to trigger the emergence of products as well as to encourage their use once they will be available.
- Support measures to achieve certification at a lower level, certifying, e.g. that a provider complies with European legislation, that processing takes place only in the EU, that a provider has a certain level of auditing, or that a provider takes responsibility for breaches.
- Support steps to achieve that Cloud Computing providers which operate solely under European jurisdiction play an increasing role.

5.2.2. Mobilizing resources

Developing human capital

As outlined in the report the development of the human capital base is in the long term one essential framework condition to ensure that the positive impacts of Cloud Computing will realize for Europe. Given the already existing constraints, but also the current measures to address it, possible policy options should be directed into two dimensions: Firstly, increase the size of the workforce, and secondly, to improve the quality of education, i.e. adjusting it to the future needs.

- Address the need of further measures to increase the number of qualified persons, in particular by exploring best practices in other regions.
- Support the implementation of programs dealing with the inclusion of groups less represented in the IT workforce such as women, elderly people or young people with less formal education.
- Support the further integration of skills requirements of emerging segments like Cloud Computing or Big Data within the existing literacy programs.

Improving financial capital situation

The financial capital situation is an important brick stone for the creation and growth of companies. As shown by the analysis in section 4.3 there exist a lack of it in Europe, which is one factor hindering the emergence of European based global players. Therefore policy option that addresses these issues will help the increase the competiveness of the European IT industry, which is also addressed in a later part of this section.

- Support the further integration of single European venture capital market.
- Explore possibilities to support young companies to grow rapidly beyond national borders.

5.2.3. Adapting the regulatory environment

Adjustment of the data protection regime

As shown there is a strong need to adjust the current data protection regime in the EU to requirements of the Cloud Computing. This adjustment is already ongoing; in particular the draft regulation on data protection addresses many issues. Since it is still under negotiation, it is not easy to make a final assessment, but resulting from the current state we see the following options.

- Support the current process of data protection law reform.
- Support the choice of a Regulation as the proposed legal instrument replacing the Directive.
- Support the strengthening of pre-existing individual rights in the proposed Regulation.
- Support the integration of the range of new rights offering further control to the data subject over their personal data – for example the 'right to be forgotten' and the 'right to data portability'.
- Support the novel obligations on the data controller in adhering to data protection law – for example, 'data protection by design and default' and the fact based approach to the concept of the 'co-controller'.
- Support further clarifications of principles related to data protection and cloud computing
- Support the accountability principle and be cautious with European level 'command and control' approaches.
- Support less rigorous consultation and notification requirements.
- Support the creation of European level consistency and interpretation mechanisms.
- Support the creation of the European Data Protection Board.

- Support increased cooperation and consistency between European DPAs.
- Support the fines mechanism proposed in the Regulation.
- Simultaneously, support the discretionary power of National DPAs in the fining process.
- Support proposals which allow justified international flows of data, whilst not risking the rights of citizens.
- Reconsider approaches which have perhaps not achieved all they promised up to now – for example Safe Harbour.
- Look into further possibilities to ensure the jurisdictional applicability of European data protection law, when European citizens or services are involved.
- Look into methods of oversight and enforcement when European data protection law should apply, but data is being processed abroad.

Creating a balanced framework for contractual relations

The analysis of contractual issues showed that the current state in contractual relations between user and provider is unbalanced. Though some parts especially for consumers are addressed in the current draft regulation on data protection, there are other issues that in particular for small and medium businesses are of importance. As analysed by section 4.2 this results in the following policy options.

- Support of proposals for the provision and funding of standardised technical approaches and tools to support the provision of greater transparency on the location of data within the cloud.
- Support of proposals to stipulate minimum requirements regarding changes to the provisions of contracts, the notification of such changes and remedies for those clients for whom the changes are material.
- Encourage standardisation in this area and support proposals for model clauses and language for Acceptable Use Policies.
- Consider a comprehensive review of IP law across the EU and support proposals for model clauses addressing the issues outlined.
- Support of optional proposals for measures that might be taken to provide greater transparency for businesses. These may include the development of technical tools for assurance and accountability, for use by various stakeholders including end users, regulators and the service providers.
- Encourage stipulating minimum requirements for provisions relating to backups of cloud services, which introduce certainty.
- Support of proposals for soft actions including awareness campaigns to address this issue.

5.2.4. Legitimation and creation of markets

Creation of trust

Trust is a major issue regarding the acceptance and adoption of Cloud Computing by all stakeholders. Therefore the lack of it can create an important barrier for the legitimation and thereby to the creation of a market for Cloud Computing in Europe. As shown throughout several sections including 2.6 and 4.2 there is a need to address issues in order

to increase the trust into Cloud Computing. Many of these identified actions have clear interrelations to the data protection and data governance.

- Support of proposals for the development of EU cloud-specific certification and the adoption by public sector organisations within the EU.
- Support for proposals for technical tools and funding for the development of an EU-wide trust mark for cloud computing. In addition to increasing transparency on service quality, this may serve to distinguish EU cloud computing services from those offered in third countries.
- Make it mandatory to notify consumers when a law enforcement request has been made.
- Review the Safe Harbour principle, negotiate conditions for government access,
- Consider encouraging the use of provider certification which shows compliance with European regulations.
- Organise a portal for addressing problems with Cloud Computing services.
- Scrutinize viewpoints put forth in the debate to see whose interests they serve.
- Be especially wary of exclusively trust-based solutions to cloud governance issues.
- Look further into ways of promoting cloud architectures designed from the beginning to secure data security and privacy through design rather than trust or legislation.

Foster the creation of a market for Cloud Computing

Another major issue for the adoption of Cloud Computing and the realisation of its positive impacts in terms of cost savings or flexibility is the existing of working and moreover also competitive market. As outline in section 2.6 and 4.3 this is essential, but also difficult endeavour. The analysis showed that there is set of policy options, which can be divided into two areas. The first one deals with reduction of barriers for cross-border operations in Europe. The second set of options is aimed at ensuring and increasing the overall competition. Both should help to create a vivid and competitive market for Cloud Computing in Europe.

- Address the issue of Cloud specific aspects within the eCommerce directive.
- Support the harmonization of data protection rules through the establishment of a common regulation.
- Support of the implementation of the consumer rights directive.
- Explore and support further options to create a single market for digital services, e.g. the Common European Sales Law.
- Address costs for network access, such as an abolishment of mobile data roaming fees.
- Support of proposals to stipulate minimum requirements regarding data portability, e.g. by enforcing providers to provide interfaces and data formats, and retention periods to support migration.
- Support of proposals for soft actions including awareness campaigns, technical support tools and funding thereof for data portability and vendor lock-in.
- Support for the implementation of the EIIF by implementation in public procurement processes to increase the diffusion of interoperable solutions.

5.2.5. Encouraging entrepreneurship and competitiveness

Encouraging entrepreneurial activities

Entrepreneurial activities are at the core of an industry. Therefore it is essential to encourage and support entrepreneurial activities, in particular ones aimed at innovative and disruptive developments. As outlined in sections 2.4, 2.6 and 4.3 the following options are possible to achieve this.

- Support soft measures to increase entrepreneurial activities, including such measures as promotion of "second chance".
- Support soft measures to stimulate the growth of a European culture for entrepreneurship.
- Encourage the emergence of European providers with high quality services.

Support the competitiveness of European Cloud industry

While addressing the entrepreneurial activities is a first step to achieve a lively European provider landscape, the other crucial part is the further support of it in order to gain a greater share of the market. As outlined in several sections the state can support this effort by taking an active role. Policy options for that are presented in the following.

- Address the issue of a coherent policy framework combining measures in support of the Cloud and other digital industries (strategic industrial policy).
- Support of participation of European member, in particular from SME, in industry driven standard bodies.
- Address the issues of a missing link between public R&D funding and public procurement, in particular innovative procurement on the EU and member state level.
- Encourage the use of provider certification which shows compliance with European regulations. Certifications could also cover quality of backups, quality of intrusion detection, etc.

5.3. Outlook

The overall aim of the forthcoming final phase is to produce a high quality final report that will be considered useful by European decision-makers. Based on this aim the work of the final phase is split up into two main areas.

The first part will focus on the compilation and consolidation of the results of the previous phases. This includes an internal review of all findings of the project as well as the integration of the results of the extra module on social networks sites. Above that we will also review the results of the policy workshop that will take place October, 2nd in Brussels as part of the European Innovation Summit as well as the integration of further comments by MEP's and the STOA secretary resulting from the presentations of results at the STOA panel on October, 10th in Strasbourg. Based on this exercise the consortia will deliver concise version of the previous deliverables as one of the two main parts of the final report.

The second part of the final report will take up the policy options identified here as well as further inputs from the policy workshop, presentation and further consultations with experts to derive a set of final policy recommendations for European-decision makers. For this purpose we will perform an internal review of all policy options derived from our in-depth analysis in this deliverable as well as of all further inputs from the policy workshop and other inputs, i.e. interviews or conference/workshop visits. The resulting list of policy options will be subject of a two-fold validation process.

In a first step we analyze to what extent current and announced policy actions overlap with our options in order to avoid duplications. Moreover this also serves the purpose concretize individual options. This will lead to a final set of concrete measures. In the second step identified will be clustered and prioritized according to their possible impacts on the uptake of Cloud Computing in Europe. This will result then in a concrete set of measures that can be undertaken to achieve this overall goal.

ANNEX: LIST OF RESPONDENTS AND EVENTS VISITED

Within the project and related activities a number of workshops and conferences were attended, respectively organised, by the contractors. This includes:

- Cloudzone, Karlsruhe 10.-11.05.2012
- Intel European Research and Innovation Conference, Barcelona 22. - 23.10.2012
- 19th ITS Biennial Conference, Bangkok 2012
- CloudConf, München 26.-27.11.2012
- KA-IT-Sicherheitsinitiative: „Cloud kommt von Klauen. Oder?", " Karlsruhe 5.10.2012
- ETTIS project: „Scenarios for the future cyber security in Europe", Frankfurt 27.-28.11.2012*
- The Computers, Privacy and Data Protection (CPDP): Data protection reloaded, Brussels, 23.-25-01.2013*
- KA-IT-Sicherheitsinitiative: "Cloud, aber sicher!! Karlsruhe 15.5.2013
- IFIP Summer School 2013: "Privacy and Identity Management for Emerging Services and Technologies, Nijmegen 17.-21.06.2013
- CAST Forum SOA und Cloud Security, Darmstadt 27.06.2013
- Roadmap for Cloud Computing for the Beijing Academy of Science and Technology, Karlsruhe, 22.-23.07.2013*

Workshop and conferences marked (*) were carried out by one of the contractors.

Individuals communicated with (f.e. explorative interviews, consultation via mail etc.) include:

- Eli Noam, Columbia University
- Philip Schmolling, Yunicon
- Matthias Schunter, Intel
- Tobias Voss, Viadee
- Gertjan Boulet, CEPS
- Michael Waidner, Fraunhofer SIT
- Stephan Engberg, Priway
- Søren Duus Østergaard, Duus Communications
- Henrik Hasselbach, IBM Denmark
- Nina Nørregaard, IBM Denmark
- Michael Friedewald, Fraunhofer ISI
- Bernd Carsten Stahl, De Montfort University *
- Gino Brunetti, Softwarespitzencluster
- Anna Fielder, Civic Consulting*
- Niels Madelung, Danish Standard / ISO-DK*
- Carsten Kestermann, Software AG
- Marnix Dekker, ENISA*
- Ken Ducatel, DG Connect*
- Henning Mortensen, The Danish Industry Association*
- Bernhard Löwe, KIT-IKS

- Li Ling, Beijing Academy of Science and Technology

Interviews marked (*) were carried out under the FP7-financed research project EST Frame, which researches Cloud Computing as case study for TA methodology.

Due to the cancellation of the originally intended workshop during the current phase further interviews and communications related to the policy options will take place in the advent or aftermath of the policy workshop scheduled for October, 2nd in Brussels.

REFERENCES

- Abboud/Sandle (2013): European cloud computing firms see silver lining in PRISM scandal. Retrieved from http://news.yahoo.com/analysis-european-cloud-computing-firms-see-silver-lining-125322771.html, Reuters 06/17/2013.
- Aiken, K., Boush, D. (2006): "Trustmarks, objective-source ratings, and implied investments in advertising: investigating online trust and the context-specific nature of internet signals." In *Journal of the Academy of Marketing Science*, vol. 34(3), pp 308-323.
- Alleweldt, F., Kara, S. (2011): Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods. Retrieved from http://ec.europa.eu/consumers/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf, 07/23/2013.
- Amazon (2013): AWS CloudHSM.http://aws.amazon.com/de/cloudhsm/07/14/2013
- Amazon (2013a): Price of external harddrive. http://www.amazon.de/gp/product/B0034G51XS/ref=noref?ie=UTF8&psc=1&s=computers, 07/23/2013.
- Amazon (2013b): Case Studies. Retrieved from https://aws.amazon.com/en/solutions/case-studies/, 07/23/2013.
- Arthur, C. (2012): Google privacy policy slammed by EU data protection chiefs, Guardian, 10/16/2012.
- Article 29 Data Protection Working Party (2007): Opinion 4/2007 on the concept of personal data: WP 136.
- Article 29 Data Protection Working Party (2012): Opinion 05/2012 on Cloud Computing: WP 196.
- Article 29 Data Protection Working Party (2013): Explanatory Document on the Processor Binding Corporate Rules: WP 204.
- Article 29 Data Protection Working Party: Opinion 05/2012 on Cloud Computing. 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, 07/23/2013.
- Ashford, W. (2013a): Technology companies call for more transparency over data requests. ComputerWeekly.com, Wednesday 12. June 2013
- Ashford, W. (2013b): Yahoo wants FISA objections revealed. ComputerWeekly.com, Thursday 11. July 2013.
- Aumasson, A., Bonneau, V., Leimbach, T., & Gödel, M. (2010): Economic and Social Impact of Software & Software-Based Services. D5–Final Report. Retrieved from http://www.cros-portal.eu/sites/default/files/25_Study%20on%20Economic%20and%20social%20impact%20of%20Software.pdf, 07/23/2013.
- Aumasson, Arnold/Bonneau, Vincent/Leimbach, Timo/Gödel, Moritz (2010): Economic and Social Impact of Software & Software-Based Services. D5 – Final Report, Paris (Smart 2009/0041) (http://cordis.europa.eu/fp7/ict/ssai/docs/study-sw-report-final.pdf).

- Babcock, C. (2013): Amazon's Cloud Revenues, Examined. Retrieved from http://www.informationweek.com/cloud-computing/infrastructure/amazons-cloud-revenues-examined/240145741, 07/23/2013.
- Barret, Victoria (2011): Dropbox: The Inside Story Of Tech's Hottest Startup, in: Forbes online, October 18,2011, (http://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/).
- Berry, R., & Reisman, M. (2012): Policy Challenges of Cross-Border Cloud Computing. Retrieved from http://serviceorientedarchitecturesoa.net/goto/http://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf, 07/23/2013.
- Berry, R., Reisman, M. (2012): Policy Challenges of Cross-Border Cloud Computing.http://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf, 07/23/2013.
- BGPmon (2010): Chinese IPS hijacks the Internet.http://bgpmon.net/?p=282, 07/23/2013.
- Bigo et. al. (2012): Fighting cybercrime and protecting privacy in the cloud. Study for the European Parliament's Policy Deparment C: Citizens' Rights and Constitutional Affairs. PE 462.509.
- Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J. and Scherrer, A. (2012): Fighting cyber crime and protecting privacy in the cloud: Report for the European Parliament.
- Bigo, Didier et al.(2012): Fighting cyber crime and protecting privacy in the cloud. Study on behalf of the European Parliament. http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050, Bruessels 07/23/2013.
- Blodget, H. (2011): Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data. Retrieved from http://articles.businessinsider.com/2011-04-28/tech/29958976_1_amazon-customer-customers-data-data-loss, 07/23/2013.
- Bloomberg (2012): Coke Gets Hacked And Doesn't Tell Anyone. http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html, 07/23/2013.
- Bloomberg (2013): Microsoft Azure Sales Top $1 Billion Challenging Amazon. April 30, 2013. http://www.bloomberg.com/news/2013-04-29/microsoft-azure-sales-top-1-billion-challenging-amazon.html, 07/23/2013.
- Bloomfield A. (2013): ACLU NSA Lawsuit: PRISM Violates the First and Fourth Amendments of the Constitution. Policymic. Retrieved from http://www.policymic.com/articles/48195/aclu-nsa-lawsuit-prism-violates-the-first-and-fourth-amendments-of-the-constitution, 07/30/2013.
- Borgmann, M., Hahn, T., Herfert, M., Kunz, T., Richter, M., Viebeg, U., & Vowé, S. (2012): On The Security of Cloud Storage Services. Retrieved from https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf, 07/23/2013.
- Borgmann, M., Hahn, T., Herfert, M., Kunz, T., Richter, M., Viebeg, U., Vowe, S. (2012): On the Security of Cloud Storage Services.

https://www.sit.fraunhofer.de/de/angebote/projekte/cloud-studie/, Darmstadt 07/23/2013.

- Boritz, J. (2005): "IS practitioners' views on core concepts of information integrity." In *International Journal of Accounting Information Systems*, vol. 6(4), pp 260-279.
- Bradshaw et. al. (2012): *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake*, IDC.
- Bradshaw, D., Folco, G., Cattaneo, G., & Kolding, M. (2012): Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up- take SMART 2011/0045 D4 – Final Report. EC. Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf, 07/23/2013.
- Bradshaw, S., Millard, C., Walden, I. (2011): "Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services." In *International Journal of Law and Information Technology*, vol. 19, pp 187-223.
- Breznitz, D. (2006): The Israeli Software Industry, in: Arora, A; Gambardella, A. (2006): From Underdogs to Tigers: The Rise and Grow of the Software Industry in Brazil, China, India, Ireland, and Israel. Oxford: OUP, 72-98.
- Breznitz, D. (2007): Innovation and the State, New Haven: Yale University Press.
- Brodies (2012): Data Protection: What price harmonization? Brodies.com, 07/30/2013.
- Brynjolfsson, E. Paul Hofmann, John Jordan(2010): Cloud Computing and Electricity: Beyond the Utility Model, Communications of the ACM, Vol. 53, No. 5, 32-34.
- Brynjolfsson, Erik, McAfee, Andrew (2011): Race against the machine, Lexington.
- Bugiel, S., Nürnberger, S., Sadeghi, A.-R., Schneider, T. (2011): "TwinClouds - Secure Cloud Computing with Low Latency". Communications and Multimedia Security (CMS'11). http://www.infsec.cs.uni-saarland.de/~bugiel/publications/pdfs/bugiel11-cms.pdf, 07/23/2013.
- Cachin, C., Schunter, M. (2011): A Cloud You Can Trust - How to ensure that cloud computing's problems—data breaches, leaks, service outages—don't obscure its virtues, IEEE Spectrum, pp 28-51. http://spectrum.ieee.org/computing/networks/a-cloud-you-can-trust/0, 07/23/2013.
- Carr, Nicolas G. (2003): IT doesn't matter, in: Harvard Business Review, 5 (2003), 41-49.
- Carr, Nicolas G. (2004): Does IT matter?, Boston.
- Carr, Nicolas G. (2009): The Big Switch: Our New Digital Destiny, New York.
- Cattaneo, G., Kolding, M., Bradshaw, D., & Folco, G. (2012): Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up SMART 2011/0045 D2 – Interim Report – Statistical Annex. EC. Retrieved from http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-statisticalannex.pdf, 07/23/2013.
- Cattedu (2011): Security and Resilience in Governmental Clouds. Making an informed decision. ENISA.
- Cattedu and Hogben (2009a): Cloud Computing. Benefits, risks and recommendations for information security. ENISA.
- Cattedu and Hogben (2009b): An SME perspective on Cloud Computing - Survey. ENISA
- Cattedu and Hogben (2009c): Cloud Computing. Information Assurance Framework. ENISA.

- Cellan-Jones, R. (2009): The Sidekick Cloud Disaster. Retrieved from http://www.bbc.co.uk/blogs/technology/2009/10/the_sidekick_cloud_disaster.html, 07/23/2013.
- Cincera, M./ Veugelers, R. (2010): Young leading innovators and the EU's R&D Intensity Gap (Breughel Policy Brief 2010/09), Brussels.
- Constine, J. (2012): Soleio, Veteran Facebook Designer Behind The Like Button, Joins Dropbox Team. Retrieved from http://techcrunch.com/2012/12/06/soleio-dropbox/, 07/23/2013.
- Cook, G., & Van Horn, J. (2010): How Dirty is your data? A Look at the Energy Choices That Power Cloud Computing. Retrieved from http://www.greenpeace.org/international/Global/international/publications/climate/2011/Cool%20IT/dirty-data-report-greenpeace.pdf, 07/23/2013.
- Cook, J. (2012): Outage at Amazon Web Services takes down Netflix on Christmas Eve. Retrieved from http://www.geekwire.com/2012/amazon-web-services-outage-takes-netflix-christmas-eve/, 07/23/2013.
- CSA (2013): The Notorious Nine. Cloud Computing Top Threats in 2013. Cloud Security Alliance, Top Threats Working Group.
- CSA: Quick Guide to the Reference Architecture. 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf
- Curry, Sam et al (2010): Infrastructure security: Getting to the bottom of compliance in the cloud. RSA Security Brief. http://www.rsa.com/innovation/docs/CCOM_BRF_0310.pdf, 07/23/2013.
- Cusumano, M. (2004): The business of software, Cambridge/Mass.
- DARPA (2013): Information Innovation Office. http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_%28CRASH%29.aspx, access 17.3.2013.
- De Busser, E. (2012): The Adequacy of an EU-US Partnership, in: Gurthwirth et. al. (Eds.): European Data Protection: In Good Health? Springer Science+Business Media 2012.
- De Hert, P. (2009): Citizens' Data and Technology: An optimistic perspective: Dutch Data Protection Authority, The Hague.
- Dekker, M.A.C. (2012): Critical Cloud Computing. A CIIP perspective on cloud computing services. Version 1.0, December 2012. ENISA
- Dignan, L. (2011): Cloud Computing’s real creative destruction may be the IT workforce. Retrieved from http://www.zdnet.com/blog/btl/cloud-computings-real-creative-destruction-may-be-the-it-workforce/61581, 07/23/2013.
- Duisberg, A. (2011): Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing, in: Picot, A. et al. (Eds.): Trust in IT, Heidelberg, 49-70.
- Ecorys (2010): The competiveness of EU SME’s in the ICT service sector. Rotterdam
- Ecorys. (2009): FWC Sector Competitiveness Studies - Competitiveness of the EU SMEs in the ICT services industry_final report. Retrieved from http://www.pedz.uni-mannheim.de/daten/edz-h/gdb/09/study_report_ict_services_en.pdf, 07/23/2013.
- Edler, J. (2010): Demand Oriented Innovation Policy, in: Smits, R./Kuhlmann, S/Shapira, P. (Eds.): The Co-Evolution of Innovation Policy – Innovation Policy Dynamics, Systems and Governance, Cheltenham.

- EDRI (2013): European Court of Justice Data Retention Cases To Be Heard On 9 July. http://www.edri.org/edrigram/number11.13/ecj-data-retention-case-9-july-2013, EDRi-gram newsletter, No. 11, 07/03/2013.
- EFI (2011): Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2011, Berlin.
- Endeshaw, A. (2001): "The Legal Significance of Trustmarks." In Information & Communications Technology Law, vol. 10(2), pp 203-230.
- EP (2013): ENISA: A new mandate to face the challenges of network and information security. European Parliament. Europarl.Europa.EU, REF: 20130416IPR07353.
- Erlanger, S. (2012): Fighting Terrorism, French-Style, New York Times, 03/30/2012.
- ESA (2009) European Software Industry: looking for a competitive advantage. European Software Association. Brussels. (Phillipon/Veron 2009)
- ESA (2009): European Software Industry: looking for a competitive advantage. European Software Association. Brussels.
- Etro, F. (2009): The economic impact of Cloud Computing on business creation, employment and output in Europe. Retrieved from http://www.uitgeverijacco.be/download/nl/23707917/file/rbe-2009-2-web-4-the_economic_impact_of_cloud_computing_on_business_creation__employment_and_output_in_europe.pdf, 07/23/2013.
- Etro, F. (2009): The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe. Draft version, May 2009.
- Etro, F. (2010): The economic consequences of the diffusion of Cloud Computing. the Global Information Technology Report, 2010, 107–112. Retrieve from http://networkedreadiness.com/gitr/main/fullreport/files/Chap1/1.9.pdf, 07/23/2013.
- Etro, F. (2011): The Economics of Cloud Computing. Paper presented at the Annual Conference on Anti-trust Law 2011: The Future of European Competition Law in High-tech Industries.
- Etro, Federico (2011): The Economics of Cloud Computing, IUP Journal of Managerial Economics, Vol. IX, 2, pp. 7-22, http://www.intertic.org/Policy%20Papers/Report.pdf, 07/23/2013.
- European Commission (2007): Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe : COM 2007/799/EC
- European Commission (2008): "Think Small First". A "Small Business Act" for Europe :COM 2008/349/EC
- European Commission (2010): A comprehensive approach on personal data protection in the European Union: COM (2010) 609 final.
- European Commission (2010): Europe 2020 Flagship Initiative Innovation Union: COM 2010/546/EC.
- European Commission (2010): Towards interoperability for European public services: COM 2010/744/EC.
- European Commission (2011): A coherent framework for building trust in the Digital Single Market for e-commerce and online services: COM 2011/942/EC.
- European Commission (2011): Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on public procurement: COM 2011/896/EC

- European Commission (2011): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Common European Sales Law: COM 2011/635/EC.
- European Commission (2011): Recommendations on the review of directive 95/46/EC. Annex 1. Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/annex-industryrecommendations-ccstrategy-nov2011.pdf, 07/23/2013.
- European Commission (2012): A European Consumer Agenda - Boosting confidence and growth. Retrieved from http://ec.europa.eu/consumers/strategy/docs/consumer_agenda_2012_en.pdf, 07/23/2013.
- European Commission (2012): Impact Assessment Accompanying the General Data Protection Regulation: SEC (2012) 72 final.
- European Commission (2012): 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 on the free movement of such data (General Data Protection Regulation): COM 2012/0011 (COD).
- European Commission (2012): Unleashing the Potential of Cloud Computing in Europe: COM(2012) 529 final.
- European Commission (2013): Digital Agenda Scoreboard 2013, Brussels.
- European Data Protection Supervisor (2012): Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe.
- European Parliament & European Council (1993): On unfair terms in consumer con-tracts: Directive 93/13/EEC.
- European Parliament & European Council (1995): On the Protection of individuals with regard to the processing of personal data and on the free movement of such data: Directive 95/46/EC.
- European Parliament & European Council (1995): On the protection of individuals with regard to the processing of personal data and on the free movement of such data: Directive 95/46/EC.
- European Parliament & European Council (1996): On the legal protection of data-bases: Directive 96/9/EC.
- European Parliament & European Council (2000): On certain legal aspects of infor-mation society services, in particular electronic commerce, in the Internal Market: Directive 2000/31/EC.
- European Parliament & European Council (2002): Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications): 2002/58/EC.
- European Parliament & European Council (2006): on the retention of data processed in connection with the provision of public electronic communication services: Di-rective 2006/24/EC.
- European Parliament & European Council (2006): On the term of protection of copy-right and certain related rights: Directive 2006/116/EC.
- European Parliament & European Council (2008): On the law ap-plicable to contractual obligations: Regulation 593/2008/EC.

- European Parliament & European Council (2009): On the legal protection of computer programs: Directive 2009/24/EC.
- European Parliament & European Council (2011): On consumer rights: Directive 2011/83/EC.
- European Parliament & European Council (2012): On European standardisation: Regulation 2012/1052/EC.
- European Parliament (2001): Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)). 07/11/2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN
- European Patent Office (1973): European Patent Convention (EPC 1973).
- European Union (2002): Charter of Fundamental Rights of the European Union: Official Journal of the European Communities: 2000/C 364/01.
- Falliere, Nicolas; O Murchu, Liam; and Chien, Eric (2011): W32.Stuxnet Dossier, Version 1.4, Symantec Security Response, available at http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 07/23/2013.
- Fenn and Raskino (2012): Gartner's Hype Cycle Special Report for 2012. Gartner Research.
- FI3P (2011): The European internet industry and market. Deliverable 2. Retrieved from http://www.fi3p.eu/assets/pdf/FI3P%20D2%20-%20EU%20Internet%20Industry%20and%20Market_Final.pdf, 07/23/2013.
- Fielder et al. (2012): Cloud Computing Study. For the European Parliament's Committee on Internal Market and Consumer Protection. IP/A/IMCO/ST/2011-18.
- Fielder, A., & Brown, I. (2012): Cloud Computing. Study. EC. Retrieved from http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411, 07/23/2013.
- Forbes (2012): NSA's New Data Center And Supercomputer Aim To Crack World's Strongest Encryption. http://www.forbes.com/sites/andygreenberg/2012/03/16/nsas-new-data-center-and-ultra-fast-supercomputer-aim-to-crack-worlds-strongest-crypto/, 07/23/2013.
- Fransman, M. (2011): The evolving ICT industry in Asia and the implications for Europe, Sevilla.
- Gartenberg and Ekholm (2012): Market insight: Consumer Apps and Services Will Become More Aware and Less Visible. Gartner.
- Gartner (2012): Gartner Says Worldwide Cloud Services Market to Surpass $109 Billion in 2012, Stamford (http://www.gartner.com/it/page.jsp?id=2163616).
- Gartner Inc. (2010): Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010. Retrieved from http://www.gartner.com/newsroom/id/1389313, 07/23/2013.
- Gentry, C. (2009): Fully homomorphic encryption using ideal lattices. Proceedings of the 41st annual ACM symposium on Theory of computing. http://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf, 07/30/2013.

- Giron, Frederic et al. (2009): The European Software and Software Based Services Industry, Brüssel.
- Global Access Partners (2011): Task Force on Cloud Computing Final Report: http://www.globalaccesspartners.org/Cloud-Computing-GAP-Task-Force-Report-May-2011.pdf, 07/23/2013.
- Goldsmith, B. (2013): Yahoo memo sparks debate on pros and cons of working at home. Reuters. London. Retrieved from http://www.reuters.com/article/2013/02/26/us-workplace-flexibility-idUSBRE91P0S720130226, 07/23/2013.
- Google 1 (2013): http://www.google.com/enterprise/apps/education/customers.html, 07/23/2013.
- Greenwald and MacAskill (2013): NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 07/07/2013.
- Greenwald, G (2013): NSA collecting phone records of millions of Verizon customers daily. The Guardian, 06/06/2013.
- Greif, B. (2012): Reporter ohne Grenzen stuft zwölf Staaten als Feinde des Internets ein.
- Gutwirth, S., Gellert, R., Bellanova, R., Friedewald, M., Schütz, P., Wright, D., Mordini, E. and Venier, S. (2011): Legal, social, economic and ethical conceptualisations of privacy and data protection: Prescient Project, Deliverable 1.
- Hecking and Schulz (2013): *Spying "Out of Control": EU Official Questions Trade Negotiations*. Spiegel International, 06/30/2013.
- Heiser, Gernot (2013): Protecting eGovernment Against Attacks. White Paper presented at STOA conference on eGovernment security. http://www.europarl.europa.eu/stoa/cms/home/events/workshops/egovernment, Brussels, 02/19/2013.
- Heng, S. (2011), " Netzneutralität. Innovation und Differenzierung keine Antipoden" Deutsche Bank Research Paper, Frankfurt.
- Henrich, Christian (2012): Statement at Karlsruher IT-Sicherheitsinitiative 5/10/2012.
- Hoffmann et. al. (2008): *Towards Semantic Resolution of Security in Ambient Environments* in: Mana and Rudolph (Eds.): Developing Ambient Intelligence. Proceedings of the International Conference on Ambient Intelligence Developments (AmI.d'07). Springer Verlag, Berlin, 2008.
- Hofmann, P., & Woods, D. (2010): Cloud Computing: The limits of public clouds for business applications. Internet Computing, IEEE, 14(6), 90–93.
- Hogan, O., Mohamed, S., McWilliams, D., & Greenwood, R. (2010): The Cloud Dividend Part One. The economic benefits of Cloud Computing to business and the wider EMEA economy. Retrieved from http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf, 07/23/2013.
- Hon, W., Millard, C., Walden, I. (2012): "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now." In *Stanford Law Review, vol. 16, pp 79-125.*
- IDC (2012): IDC Forecasts Public IT Cloud Services Spending Will Approach $100 Billion in 2016, Generating 41% of Growth in Five Key IT Categories, Framingham, (http://www.idc.com/getdoc.jsp?containerId=prUS23684912#.UPVtJ_IWnCc).
- International Association of Microsoft Channel Partners (2011): "*'Trustmark' Proposal for Cloud Service Providers*". Presentation at 5th Call for Proposals.

- ITTL (2011): Cloud audit & assurance. The Danish Internet and Telecommunication Agency (IT & Telestyrelsen). Retrieved January 2013 from: digitaliser.dk/resource/703330
- Jansen, W., Grance, T. (2011): "*Guidelines on Security and Privacy in Public Cloud Computing*. Special Publication." National Institute of Standards and Technology, U.S. Department of Commerce.
- Kalenda, F. (2013): Amazon Web Services macht 2013 etwa 3,8 Millarden Dollar Umsatz. Retrieved from http://www.zdnet.de/88138507/analyst-amazon-web-services-macht-2013-38-mrd-dollar-umsatz/, 07/23/2013.
- Kaminiski, M. (2013): PRISM's legal basis: How we got here, and what we can do to get back. The Atlantic, June 7th.
- Korff and Brown (2010): New Challenges To Data Protection. Study commissioned by the European Commission's DG JFS.
- Korte, Werner B. et al. (2009): Anticipating the development of the supply and demand for e-Skills in Europe 2010-2015, Brussels.
- KPMG (2012): Exploring the Cloud. A Global Study of Governments' Adoption of Cloud. KPMG International.
- KPMG (2013): The Cloud Takes Shape. Global Cloud Survey – The Implementation Challenge. KMPG International. Retrieved May 2012 from http://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDkQFjAB&url=http%3A%2F%2Fwww.kpmg.com%2FFR%2Ffr%2FIssuesAndInsights%2FArticlesPublications%2FDocuments%2Fthe-cloud-takes-shape.pdf&ei=DRb1UbTYNcSQ4gTWh4CgAQ&usg=AFQjCNEwrTqhruWts9hq0TeNYk0SYZA_5A&sig2=Rnr40bfxw9-DT-TRFuig6g&bvm=bv.49784469,d.bGE.
- Kraus, M. (2012): Cloud Computing und Consumerization of IT in Deutschland 2012. IDC. Retrieved from http://www.microsoft.com/germany/msdn/aktuell/news/show.mspx?id=msdn_de_45934, 07/23/2013.
- Kraus, M., & Zacher, M. (2012): Cloud Computing in Deutschland 2012. Deployment-Modelle und Management, Integration, Security und Compliance im Fokus. IDC. Retrieved from http://www.kaspersky.com/de/downloads/pdf/idc_executive_brief_mc_cloud_computing_2012_kaspersky.pdf, 07/23/2013.
- Kuan Hon, W., Millard, C., & Walden, I. (2012): Who is responsible for 'personal data' in cloud computing? - The cloud of unknowing, Part 2: International Data Privacy Law, vol. 2 no. 2, pp. 3-18.
- Kucharik, A. (2003): *Vendor lock-in, part 1 Proprietary and lock-in not necessarily synonymous*. Retrieved June 15, 2013, from Search Open Source: http://searchenterpriselinux.techtarget.com/news/913129/Vendor-lock-in-part-1Proprietary-and-lock-in-not-necessarily-synonymous, 07/23/2013.
- Kuner et. al. (2013): *The extraterritoriality of data privacy laws – an explisve issue yet to detonate* in: International Data Privacy Law, 2013, Vol. 3, No. 3.
- Lanier, J. (2013): *You are not a gadget… An interview with Jaron Lanier.* Jaronlanier.com/polecongadgetqa.html, 07/30/2013.
- Lardinois, F. (2012): Apple's iCloud Now Has Over 190M Users, Up From 150M Last Quarter And Seeing Steady Growth. Retrieved from

http://techcrunch.com/2012/10/25/apples-icloud-now-has-190-million-users/, 07/23/2013.

- Lardinois, F. (2012): Gmail Now Has 425 Million Users, Google Apps Used By 5 Million Businesses And 66 Of The Top 100 Universities. Retrieved from http://techcrunch.com/2012/06/28/gmail-now-has-425-million-users-google-apps-used-by-5-million-businesses-and-66-of-the-top-100-universities/, 07/23/2013.
- Laugesen, Nicolai S.(2011): Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements, Copenhagen.
- Leclerque, K. (2012): Public Cloud-Nutzung in Deutschland - Fallstudie Airport Nürmberg Infopark. PAC.
- Leimbach, T. et. al (2012): Foundations of Cloud Computing, Karlsruhe.
- Leimeister, S./Riedl, C./Böhm, M./ Krcmar, H. (2010): The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks, in: Proceedings of 18th European Conference on Information Systems (ECIS 2010) Paper 56. (http://aisel.aisnet.org/ecis2010/56).
- Liebenau et. al. (2012): *Modeling the Cloud. Employment effects in two exemplary sectors in the United States, the United Kingdom, Gemany and Italy*. LSE Enterprise.
- Lo, P. (2013): *Cloud computing is about to get personal* , Network World June 06, 2013 10:32 AM ET.
- Lynn, T., Healy, P., McClatchey, R., Morrison, J., Pahl, C., Lee, B. (2013): "The case for cloud service trustmarks and assurance-as-a-service". In: *International Conference on Cloud Computing and Services Science 8-10 May 2013*, Aachen, Germany: http://doras.dcu.ie/18357/1/CLOSER_2013_Paper_Case_for_Cloud_Service_Trustmarks_and_Assurance_as_a_service_115_10-03-13b.pdf, 07/23/2013.
- MacAskill et. al. (2013): GCHQ taps fibre-optic cables for secret access to world's communication. The Guardian, 07/21/2013.
- Marnau, N., Schirmer, N., Schlehahn, E., Schunter, M. (2011): TClouds. Herausforderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud. Datenschutz und Datensicherheit; Volume 35; Number 5; 333-337. http://www.springerlink.com/content/3664g67412449j52/fulltext.pdf, 07/23/2013.
- Maxwell and Wolf (2012): A Global Reality: Governmental Access to Data in the Cloud. A comparative study of ten international jurisdictions. A Hogan Loells White Paper.
- Maxwell, W., Wolf, W. (2012): A global reality: Governmental Access to Data in the Cloud. Maxwell_Revised Government Access to Cloud Data Paper. http://www.hoganlovells.com/hogan-lovells-revealing-study-about-governmental-access-to-data-in-the-cloud-detailed-in-white-paper-released-at-brussels-program-05-23-2012/ RP-online: Hackerangriff: Bayer hält stand (2011): http://www.rp-online.de/bergisches-land/leverkusen/nachrichten/hackerangriff-bayer-haelt-stand-1.1322513, 07/05/2013.
- Mayer-Schönberger, V. (1997): Generational Development of Data Protection in Europe in: Technology and Privacy, Agre, P. and Rotenberg, M. (eds.), MIT Press, Cambridge, MA, pp. 219-242.
- McDonagh, M. (2012): "Review of the Regulatory and Legal Environment for Cloud Computing in the EU" Irish Centre for Cloud Computing and Commerce.

- McGee, K. (2011): The 2011 Gartner Scenario: Current States and Future Directions of the IT Industry. Gartner Inc. Retrieved from https://noppa.tkk.fi/noppa/kurssi/t-128.5300/luennot/T-128_5300_gartner.pdf, 07/23/2013.
- Meyer, D. (2013): Privacy activists sue UK government over PRISM and Tempora. Gigaom. Retrieved from http://gigaom.com/2013/07/08/privacy-activists-sue-uk-government-over-prism-and-tempora/, 07/30/2013.
- Meyer, T., Simsek-Graf, C., & Sanna, D. (2012): Heiter statt wolkig. Softwaretest in der Cloud. Retrieved from http://www.sigs-datacom.de/fileadmin/user_upload/zeitschriften/os/2012/Testing/meyer_simsek_sanna_OS_Testing_2012_kj7r.pdf, 07/23/2013.
- Miller, C.C. (2013): Tech Companies Concede To Surveillance Program. New York Times, 07/07/2013.
- Morgan, T. P. (2012): Amazon's S3 object count kisses 1 trillion. Retrieved from http://www.theregister.co.uk/2012/04/09/amazon_aws_s3_objects/, 07/23/2013.
- Mowery, David (1996) (Hrsg.): The international Computer Software Industry, Oxford.
- Nessi (2008): A NESSI Position Paper: European Software Strategy. Brussels.
- Nielsen, N. (2013): *EU questions decade-old US data agreement*, EUObserver.com. http://euobserver.com/justice/120919, 07/22/2013.
- Nightlabs (2013): http://www.cumulus4j.org/latest-stable/de/, 06/21/2013.
- Nordic Council of Ministers (2011): Nordic Public Sector Cloud Computing - a discussion paper. TemaNord 2011:566.
- Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues: Towards Trusted Cloud Computing,Proceedings of the Workshop On Hot Topics in Cloud Computing (HotCloud), San Diego, CA, June 2009. http://www.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf
- OECD (2011): Demand Side Innovation Policy: Theory and Practice in OECD Countries", Paris.
- Open Hypervisor (2011): Isolating Spears. http://www.open-hypervisor.org/index.php/HPvisor/news/, 07/28/2011.
- Panettieri, J. (2013): Google Apps, Enterprise Cloud Revenues $1B In 2013. Retrieved from http://talkincloud.com/cloud-services-providers/google-apps-enterprise-cloud-revenues-1b-2013, 07/23/2013.
- Pepitone, J. (2012): Instagram can now sell your photos for ads. Retrieved from http://money.cnn.com/2012/12/18/technology/social/instagram-sell-photos/index.html?iid=s_mpm#comments, 07/23/2013.
- Poitras et. al. (2013): How the NSA Targets Germany and Europe. Spiegel International, July 1st 2013.
- Rader, D. (2012): *Case - How cloud computing maximizes growth opportunities for a firm challenging established rivals* in: Strategy and Leadership, Vol. 40, No. 3. pp. 36-43. Emerald Group Publishing Ltd.
- Rannenberg et al. (Eds.) (2009): The Future of Identity in the Information Society. Challenges and Opportunities. Springer Verlag, Berlin.
- Rauhofer and Bowden (2013): Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud. Paper presented at the Berkeley Center for Law and Technology Privacly Law Scholars Conference, 6-7 June 2013. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2283175

- Reed, C. (2010): "*Information 'Ownership' in the Cloud*." Queen Mary University of London, School of Law Legal Studies Research Paper No 45/2010.
- Reichmann, A. (2011): File Storage Costs Less In The Cloud Than In-House. Forrester.
- Ristenpart, T., Tromer, E., Shacham, H., Savage, S. (2009): Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. ACM Conference on Computer and Communications Security: 199-212.
- Robinson et. al. (2010): The Cloud. Understanding the Security, Privacy and Trust Challenges. RAND Europe for the European Commission, DG InfSo.
- Robinson, N., Valeri, L., Cave, J., Starkey, T. Graux, H., Creese, S., Hopkins, P. (2010): *"The Cloud: Understanding the Security, Privacy and Trust Challenges"* Report prepared for Unit F.5, Directorate-General Information Society and Media, European Commission: http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf, 07/23/2013.
- Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. (2010): The Cloud: understanding the security, privacy and trust challenges. Privacy and Trust Challenges. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2141970, 07/23/2013.
- Schleife, K. et al. et al. (2012): Wachstumshemmnisse für kleinere und mittlere Unternehmen am Beispiel der IT-Branche, Berlin.
- Schneier, B. (2013): Terms of Service as a Security Threat. Retrieved from http://sysinfosec.net/article.php/20130117081339726#4, 07/23/2013.
- Schneier, B. (2013b): Government Secrets and the Need for Whistleblowers. CRYPTO-GRAM Newsletter, June 15, 2013.
- Schneier, B. (2013c): Protecting E-Mail from Eavesdropping. CRYPTO-GRAM Newsletter, June 15, 2013.
- Schneier, Bruce (2013): Government Secrets and the Need for Whistleblowers. CRYPTO-GRAM Newsletter, 06/15/2013.
- Schonfeld, E. (2011): Netflix Now The Largest Single Source of Internet Traffic In North America TechCrunch. Retrieved from http://techcrunch.com/2011/05/17/netflix-largest-internet-traffic/, 07/23/2013.
- Schouten, E. (2012): "Auditable Cloud Services and Industry Compliance." In *Wired*, 11/2012.
- Schubert (2011): *The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010*, European Commission, Expert Group Study.
- Schubert, L., & Jeffery, K. (2012): Advances in clouds. Research in future Cloud Computingf. Retrieved from http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf, 07/23/2013.
- Schulzki-Haddouti, C. (2012): Wild Wild Cloud: Datenschutzkontrolle unmöglich. Retrieved from http://futurezone.at/netzpolitik/10436-wild-wild-cloud-datenschutzkontrolle-unmoeglich.php, 07/23/2013.
- Schwartz, M. J. (2013): Flickr Bug Revealed Private Photos To Public. Retrieved from http://www.informationweek.com/security/privacy/flickr-bug-revealed-private-photos-to-pu/240148386, 02/12/2013.
- Sealed Cloud (2013): http://www.sealedcloud.de/?page_id=8, 07/13/2013.
- Steinmueller (2004): The European Software sectoral system of innovations. In: Malerba, F. (ed.): Sectoral Systems of Innovations, Cambridge, 193-241.

- Streetinsider (2013): Salesforce. Retrieved from http://www.streetinsider.com/Earnings/Salesforce.com+%28CRM%29+Lower+Despite+Q2+Top+and+Bottom-Line+Beat%2C+Q3+EPS+Guidance+Falls+Short+But+FY+In-Line/7683268.html, 07/13/2013.
- Taft, D. K. (2012): Microsoft Sees Revenue Growth on Server and Tools as Xbox Drops. Retrieved from http://www.eweek.com/c/a/Windows/Microsoft-Sees-Revenue-Growth-on-Server-and-Tools-as-Xbox-Drops-686610/, 07/23/2013.
- Trevis (2013): Google: Number of Gmail Users. Retrieved from http://www.trefis.com/company?hm=GOOG.trefis&division=0781&driver=0883&from=pdf&scroll=1#/GOOG/n-0781/0875?c=top&from=rhs, 07/23/2013.
- Turlea, A. et al. (2010): The 2010 report on R&D in ICT in the European Union, Seville.
- Turlea, A. et al. (2011): The 2011 report on R&D in ICT in the European Union. Seville.
- United States (1986): Electronic Communications Privacy Act of 1986 (ECPA, Pub.L. 99-508, 100 Stat. 1848, enacted October 21, 1986, codified at 18 U.S.C. §§ 2510–2522).
- United States (2001): USA Patriot Act (U.S. H.R. 3162, Public Law 107-56), Title V, Sec 505. Amended 18 U.S.C. § 2709(b).
- van Ark, B. et al. (2003): ICT and productivity in Europe and the United States. Where do the differences come from? In: CESinfo 3(2003), 295-318.
- Vanson Bourne (2012): The Business Impact of the Cloud. According to 460 Senior Financial Decision-Makers. Vanson Bourne. Retrieved July 2013 from http://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEIQFjAC&url=http%3A%2F%2Fstatic.ziftsolutions.com%2Ffiles%2F8a57cb7d3e5aa0dd013e61c646bb1d58.pdf&ei=_BT1Ucy7NOOQ4AT_6YD4Dw&usg=AFQjCNEo3DLi66SynXZ5ehn40mWW08ou_Q&sig2=27v-Dt9A8Z2fagRrAf0_WQ&bvm=bv.49784469,d.bGE&cad=rja
- Vaughan-Nichols, S. J. (2013): Evernote hacked, forces password reset. Retrieved from http://www.zdnet.com/evernote-hacked-forces-password-reset-7000012045/, 07/23/2013.
- Vehlow, M. (2011): PwC study: Cloud Computing in the Middle Market. http://www.pwc.de/de/mittelstand/cloud-computing-im-mittelstand.jhtml, 07/23/2013.
- Venkataraman/McArthur (2011): Vimeo EC2 transcoding. Retrieved from http://de.slideshare.net/ptrmcrthr/vimeo-ec2, 07/23/2013.
- Veugelers, R. (2009): "A lifeline for Europe's young radical innovators". Bruegel Policy Brief, 2009/01.
- Veugelers, R. et al. (2012): Lessons for ICT Innovative Industries. Three Experts' Positions on Financing, IPR and Industrial Ecosystems, Seville.
- Waldmann, U. (2013): Comment at CAST Forum, 06/27/2013.
- Wauters, P., Declercq, K., Van der Peijl, S., Davies, P. (2011): Study on cloud and service oriented architectures for e-government. final report. Deloitte. Retrieved from https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/smart2010-0074finalreport.pdf, 07/23/2013.
- Weber, Arnd; Haas, Michael; Scuka, Daniel: Mobile Service Innovation: A European Failure. Telecommunications Policy, Volume 35, Issue 5, June 2011, 469-480
- WEF (2010): Exploring the Future of Cloud Computing. Riding the next wave of technology-driven transformation. World Economic Forum in partnership with Accenture.

- WEF (2011): Advancing Cloud Computing: What to do now? Priorities for Industry and Government. World Economic Forum in partnership with Accenture.
- Wessner, Charles (2008): Assessment of the Small Business Innovation Research Program, Washington, D.C.
- Wimmer, B. (2011): Uni Salzburg liegt in Googles Händen. Retrieved from http://futurezone.at/netzpolitik/69-uni-salzburg-liegt-in-googles-haenden.php, 07/23/2013.
- Wohlsen, M. (2013): Amazon Crash Could Cost A Lot More Than 400,000 Pairs of Unsold Underwear. Retrieved from http://www.wired.com/business/2013/02/amazon-crash-unsold-underwear/, 07/23/2013.
- Woloszynowicz, M. (2011): The Economics of Dropbox. http://www.w2lessons.com/2011/04/economics-of-dropbox.html, 07/23/2013.
- Yahoo Finance (2013): Rackspace Hosting, Inc. (RAX). Retrieved from http://finance.yahoo.com/q/ks?s=rax, 07/23/2013.
- Zhu, K., Zhou, Z. (2011): "Lock-In Strategy in Software Competition: Open-Source Software vs. Proprietary Software." In *Information Systems Research*, Article in Advance, pp 1-10.
- Zotero (2013): http://www.zotero.org/ Access June 14, 201, 07/23/2013.