ETAG

European Technology Assessment Group

ITAS · DBT · FCRI · ISI · IST · ITA · TC · Rathenau

Final Report

Report

Deliverable No.5 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 Daniel Bachlechner (Fraunhofer ISI)
Dr. Arnd Weber (ITAS)
Mrs Maggie Jaglo (ITAS)
Dr Leonhard Hennen (ITAS)
Mr Rasmus Nielsen (DBT)
Dr Michael Nentwich (ITA)
Mr Stefan Strauß (ITA)

December 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 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/SC8

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 Daniel Bachlechner (Fraunhofer ISI)
Dr. Arnd Weber (ITAS)
Mrs Maggie Jaglo (ITAS)
Dr Leonhard Hennen (ITAS)
Mr Rasmus Nielsen (DBT)
Dr Michael Nentwich (ITA)
Mr Stefan Strauß (ITA)

With contributions from:
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:

December 15th, 2013

CONTENTS

EXECUTIVE SUMMARY

Cloud Computing and Social Network Sites (SNS) are among the most controversially discussed developments in recent years. They are both part of the same societal transformation referring to a paradigm shift stating that "the network is the computer". The opportunities of using powerful computing resources on demand via the web are considered as a possible driver for the growth of the European economy. Especially cost savings as well as increased productivity and mobility are seen as key elements by many experts. However, there are also critics arguing that economic, social and technical risks prevail or even dismiss the potentials of Cloud Computing and SNS. This project sheds light on these aspects and analyses the potentials and impacts of these developments. This includes a review of the technological and economic developments Cloud Computing is based on, an identification of driving factors and barriers for Cloud Computing in Europe as well as of main actors and their interests; and an analysis of impacts on citizens, business (including the IT industry itself) and public administration including a broad range of technical, economic, cultural, legal, regulatory issues and the impacts on society and economy as a whole. Cloud Computing not least includes a variety of technical concepts that alter computing infrastructures. SNS represent a prominent phenomenon grounding on Cloud Computing with a wide array of services and applications mainly focussed on end-users. Particular interrelations are given in terms of privacy and security challenges which are main issues addressed by the analysis of SNS related impacts.

Foundations of Cloud Computing

Cloud Computing is still an evolving concept and technology. This is underlined by the fact that many different types of definition and characteristics exist. The analysis of different definitions shows that there is a core set of functionalities and characteristics including on-demand services, network access, resource sharing and measured services but also that the exact definitions of these aspects and the focus setting vary depending on the viewpoint of the authors. There is no universally accepted definition, but the definition of NIST has prevailed in practice. It defines Cloud Computing as *"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."* Similar to the plethora of definitions, there is also a growing number of service, delivery and revenue models. In particular the service and delivery models have become an object of marketing. Beside the three classical service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as Service (SaaS), which are reflected in the NIST definition, there is growing number of brandings for new service models. These are used to differentiate specific segments or services, but make it hard to keep an overview because the borders to other technologies or services are not always well defined. The same situation can be found in case of the delivery models, where besides the typical delivery models of public, private or hybrid clouds many new terms emerged. Within this project, we focus on the main types of delivery and service models to avoid the resulting definition-related problems. In case of the revenue models, there are no stable definitions yet. Typically, different models are based on subscription or usage (pay-as-you-go) and advertisements. The hybrid model of freemium services is currently the main revenue

model for consumer-oriented offers. Apart from that there are new approaches like dynamic pricing. Given this blurry situation, the project focuses on service and delivery models to classify and analyse cloud services and providers. Finally it should be noted that the overall focus for the analysis of challenges and opportunities lies on public and hybrid cloud services.

A more detailed review of the evolution of the Cloud Computing concept reveals that it is not a disruptive or totally new concept. It can be traced back to ideas from the 1960s and there are predecessors and related concepts like Application Service Provision, Utility Computing and Grid Computing that appeared in the last decades. Many basic ideas of Cloud Computing like location independence or pay-per-use have already been introduced above, though some of these concepts failed to succeed on the market. Basically, the underlying technology of Cloud Computing is based on two concepts: multi-tenancy and service orientation. Typically, these concepts are implemented in form of virtualisation systems and web services. This is also reflected in the three-layered basic architecture. In addition, Cloud Computing demands several requirements such as the availability of sufficient network capacity ensuring access to data, reliable and fault tolerant service offers and a well-functioning technical infrastructure for proper functioning. Although the basic concepts seem to be clear, the concept and technology still bears potential for further advances in areas like scalability and flexibility. Beyond that it is necessary to address several technical challenges like interoperability to facilitate compelling reasons to use Cloud Computing.

Market development of Cloud Computing

A review of the different market research reports shows that Cloud Computing services are one of the fastest growing segments within the market for software and IT services. Only Mobile Computing or Big Data seem to have comparable growth rates but their segments are smaller. Moreover, they are also drivers for the cloud market because they often build upon cloud technologies. At the moment the market for public Cloud offers grew by nearly 20% per year. For example IDC states that the market grew from 40 bn. $ in 2012 to 47.7 bn. $ in 2013. Also other market segments like Cloud-related IT services or markets for private Clouds show a strong growth. Therefore Cloud Computing will become an essential part of the overall market. This will lead to an overall growth of the software and IT services as well as the IT hardware market, but it will also lead to a decrease of existing market segments, in particular, the segment of software products based on licenses and maintenance contracts as well as IT service segments like outsourcing. However, it is presumed that cloud-related services like integration consulting (e.g. in case of hybrid cloud solutions) will grow and maybe compensate for the loss in the IT service market.

The common view is that in respect of the different services models the market for the SaaS model (including BPaaS) will stay the biggest one in the future. Nevertheless, it is presumed that IaaS, which is with a clear margin the second biggest market, will grow at an even higher rate. Moreover, some experts believe that PaaS will also gain in importance. Though this will lead to an increasing share of both models within the Cloud Computing market, SaaS will remain in absolute value the main market in the future. One reason for this is the difference in the adoption and usage patterns. This relates to consumers using

cloud services for private purposes as well as for their work life, but also the growing number of SMEs adopting cloud services are more used to standardised product offers. Finally, there is a clear trend towards more diversity on the cloud market, i.e. more and more complex services and revenue models.

Regarding the regional development the US is the biggest market for Cloud Computing at the moment. According to all forecasts, it will show in terms of absolute value the greatest growth. However in terms of growth rate emerging markets like China or India are growing in importance. At the moment, Europe is the second biggest market behind the US and followed by Japan, but it is characterized by smaller growth rates than many other regions. As reasons for this researchers name two issues: Firstly, the lower adoption rate in general caused by a greater reluctance against Cloud Computing that is also reflected in the adoption patterns, and secondly, the economic crisis of the Euro zone. The strongest players in the market are well known. On the one hand there are early movers like Amazon and Google with a strong background in Internet-based services as well as for example Salesforce, which was an early proponent of SaaS and its predecessors. On the other hand, there are the IT service providers like IBM, HP or Deutsche Telekom (T-Systems) and others who capitalize on their technology and customer base. Another group is formed of specialist like VMWare or Terremark, which were engaged in virtualisation and data center operation. There is also the group of more product-oriented companies like Microsoft, Oracle or SAP, which all started at a later stage but rely on their experience, strong profile as well as their existing market position. Finally, there is the group of "cloud born" companies like Dropbox or Evernote, which build their offers on cloud services of others and address consumers and SMEs in the first place. However, the question will be which of these companies are able to turn their revenues into profit while growing further. It is probable that one or a few of them will become global players and many of them will not survive in the long run. The growing number of acquisitions of promising start-ups and medium-sized companies is a first sign of market consolidation.

Adoption and usage patterns of Cloud

Although there is little information available, it seems obvious that European companies are generally less engaged in using cloud services as compared to their US counterparts. The difference is most obvious in the SME segment, where US companies are more likely to adopt cloud services. Most European companies only started to adopt cloud services in the last two years, which might be an explanation for the differences in the adoption patterns. With regard to the different types of usage, it is not possible to determine bigger differences between the US and Europe. Most often, simple applications are the first ones in both regions, while with more experience the complexity of the services used increases. There are also uncertainties to which extent European companies tend to use private Cloud instead of public Cloud offers. Given this and taking the positive development in recent years into account, it might be that the lagging behind of Europe is not as big as some predictions state or discussants fear.

In case of the consumers' adoption and usage patterns the situation is more complicated due to the different definitions of consumer cloud services. Therefore comparisons between the different studies and analyses are only possible to a very limited extent. Overall, the

results show that the adoption of cloud services by consumers varies between the different European countries. Characteristics such as geographical location or size do not seem to affect the adoption of cloud services significantly, but it seems likely that different national approaches towards privacy and trust, which were addressed by some studies, form a good indication. In regard to what kind of services are used two trends are recognizable. Firstly, most consumers prefer to use free services over paid ones. Secondly, the studies show that services with less involvement of personal data are more frequently used than others. Based on the information available on the situation in the US, it seems clear that US consumers also clearly prefer free service offers. As for the second point, the relation between personal information/data and adoption, it is not possible to find relevant information. In total, the adoption level in the US is likely higher than the one in Europe.

At a first glance the adoption level of Cloud services by governments and public services does not seem to differ much between the US and Europe. However, there are some differences with respect to the overall attitude and the resulting course of action. The US federal government already started in 2009 to implement projects and meanwhile adopted a federal Cloud strategy foreseeing a Cloud First policy, which often leads to the use of existing public cloud services. In contrast, many European states just started to develop plans for national cloud platforms with varying coverage, which will take time to develop and implement. Often, part of these plans is to support the national IT industry. Until these platforms work, many smaller efforts were made that led to the introduction of private clouds within the existing structures. However, there are also European countries following different approaches. At the moment it is obvious that more pragmatically approaches gain more attention.

The growing maturity of Cloud Computing will lead to a transformation in usage and offers. While the last years were shaped by the fact that most services where transferred from existing offers into the Cloud, the future development will enable more services building upon other services. The question is if and when this "Cloud innovation" will occur and how it will impact, i.e. it will be a revolution or more an evolution or even something in between. Nevertheless some trends for the next years are already observable. The first one is that, in particular for innovative Cloud offers, consumer will play an important role ("Consumerization of IT"). In the market for business oriented Cloud services the trend of more and more complex services is recognizable, which will lead to a growing hybridization of the existing IT landscape in companies. This requires high levels of integration, but it also governance strategies to comply to existing regulations and to assure the security of own data and applications, in particular if critical processes are involved.

Identification and assessment of drivers and barriers

In order to determine the challenges for Cloud Computing in Europe that needs to be addressed, the first step was an initial identification of barriers and drivers. It served two purposes: Firstly, it supported the identification of impacts, positive as well as negative ones; secondly, it helped to determine the importance of them. Together with the results of the impact analysis this was a major input for the selection of challenges. It showed that there is currently a strong research focus on the barriers for adoption and use in Europe that strongly focus on the barriers and drivers for demand side, in particular on the

business usage and less on the consumer usage. This is also reflected by the fact that the number of barriers outnumbers the one of drivers. The analysis underpins that cost savings and resulting competitive advantages are seen as the major drivers for the business adoption, but that in a long-term other drivers like flexibility and innovation will gain of importance. Concerning the barriers five group of barriers can be identified: 1. technical barriers, e.g. technical security, network availability and reliability, interoperability/standards; 2. business and operational barriers, e.g. compliance, regulation, vendor lock-in, lack of skilled developers and users, service reliability/access to data; 3. regulatory-legal barriers, e.g. privacy/data protection, contractual arrangements, legal jurisdiction, service levels, consumer rights; 4. governance barriers, e.g. third party access/data retention, data location; and, 5. socio-cultural barriers like loss of control, lack of trust/ lack of transparency. All of them are strongly interrelated and need to be reflected in the analysis of impacts. Regarding the situation off Cloud service providers the review shows that the spectrum of identified barriers covers a broad spectrum, of which many are not specific for Cloud Computing. However, some of them still have a high importance for the take up of the Cloud providers in Europe. Finally, it should be noted that there are interrelations between the barriers and drivers for the demand side as well as the supply side.

Impacts of Cloud Computing services

The review and analysis of the existing literature on socio-economic impacts reveals a fundamental challenge. Most of the literature is based on assumptions and estimations, in particular the one on impacts on the economy as a whole. Even on the micro-level of companies there is only little literature based on real cases, which makes it difficult to evaluate the estimations made. Therefore, the results of the different studies have to be interpreted with caution.

Direct impacts on businesses, public administrations and consumers are widely discussed. In particular for businesses and public administrations cost savings of IT services are seen as the main impact. The span of estimated cost savings reaches from 10 to 30%, but as already mentioned there is only little literature that deals with real cases. Some examples suggest that cost savings can only be realized if certain conditions are given. Additionally, the question of the total cost of ownership (TCO), which also includes costs for migration and termination, has not yet been answered. In case of consumers, cost savings are seen as less important. Most often the convenience of using services is seen as the main positive impact. This also counts for employees using Cloud services for work purposes (IT consumerization, Buy/bring your own device (BYOD)) or for small companies. Beyond that other positive impacts are growing mobility and flexibility. In the medium to long term, productivity gains are seen as positive impacts, in particular for businesses and public administrations. Apart from that, another often controversially discussed impact is the professionalization of security management (back up, security, etc.) which comes along with cloud offers and could be a benefit for consumers and SMEs.

The review also revealed several direct negative impacts and concerns. They mostly relate to security and control. There is the risk to lose control over data or that the confidentiality of data is breached as well as the risk that the data is not available when needed. These

risks concern all user types from businesses via public administrations through to consumers. For consumers in particular, there is the risk of sacrificing privacy because many advertisement-based or freemium services like web-based mail services rely on the analysis and reuse of user data. Moreover, the mobile use bears further risks like the cost of mobile connections and in particular roaming fees for usage outside of the provider's network. Further risks can arise if a transfer of data is problematic either because data cannot be deleted or technical problems make it difficult. The problem of data portability and beyond that of migration or usage of different providers is even a bigger challenge for businesses and public administrations, because in the worst case vendor lock-in can eventually lead to higher instead of lower costs. Additionally, many large corporations already used outsourcing and/or virtualisation in the last years, which is quite close to private clouds. Therefore, it is an open question to what extent they can reap additional benefits. It can be stated that there is a widespread fear that Cloud Computing providers and foreign government's abuse data, 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 can be overcome, Cloud Computing is expected to have a bright future.

Regarding the impacts on the IT markets and the IT industry itself, it can be stated that Cloud Computing represents a fast growing segment and will gain in importance in the future. According to different market researchers, it can be stated that the share of Cloud Computing in the overall market for software and IT services will grew from 3 to 5% at the moment to a range of 10 to 20% in the next 5 to 10 years. Though it might be that in some years Cloud Computing as a segment will merge into new or other market segments, 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 today, i.e. the dominance of US-based providers will continue. Nevertheless, the current challenges may provide an opportunity that European providers with a strong focus on reliability and confidentiality gain in importance, in particular if they are supported by the European policy.

Based on the positive direct impacts, several studies conclude that Cloud Computing enables significant productivity growth that will impact overall growth and employment positively. Another argument, which is often brought up in discussions on the impact of Cloud Computing on the society and the economy as a whole, is that Cloud Computing, due to the flexibility and low costs, supports the creation of innovation and in particular that new businesses can easily enter the market and scale their operations. However, only a very limited number of the analyses tried to determine the size of these effects for Europe or at least for some of the EU member states. In these cases, all studies forecast a significant positive impact on employment and the creation of new business opportunities, which goes along with an overall economic growth. But for two reasons these results have to be interpreted with caution beside the normal challenges of all types of forecasts. Firstly, the underlying calculations are based on estimated cost savings. This is fair due to the lack of empirical values, but normally such estimations tend to be quite optimistic, particularly in early stages of a technology. Secondly, the analyses partly neglect input-output relations

and effects, i.e. the fact that job creation in one sector may lead to job destruction in another. The relevance of these points is underlined by some recent literature on the impact of IT in general on employment and growth. This research shows that even realised productivity gains do not automatically lead to the creation of highly-skilled employment. In the worst case, it could even have the opposite effect.

This review is not aimed at dismissing the positive expectations and potentials associated with Cloud Computing as a whole, but it is aimed at raising awareness for the fact that these potentials are not exploited automatically. Exploiting them requires that all obstacles are removed as well as that the estimated cost savings can be realized to a certain extent. Moreover, the analysis also showed that beyond addressing obstacles and challenges specific framework conditions like education or infrastructure are required to turn productivity gains into growth of employment. Additionally, the aim of changing the structure of the industry poses some further challenges. Based on this consideration, the main barriers and challenges that need to be addressed are analysed in the following sections.

Technological challenges

Though there are only a few technological challenges named in the analysis of barriers and impacts, there are reasons two have a more detailed look for two reasons. The first one is that related to technological capabilities like flexibility which demands efficient and highly scalable infrastructures. The second reason is that some challenges are reinforced by technological issues. The most prominent example is the vendor lock-in, which can be reinforced by a lack of standards. Consequently these challenges will be shortly analysed in the following. Finally it should be noted that information security is also a technological challenge, but due to its importance and its non-technical aspect it is treated separately. The analysis shows that standards and interoperability are important for two reasons. Firstly, because only interoperable cloud services enable users to fully exploit potentials of cloud computing such as dynamic usage and flexible payment. Secondly, standards and interoperability prevents vendor lock-in, which is a concern representing a major barrier for cloud adoption. Howwever, the IT industry is shaped by market driven de facto standards either set market leaders or driven by industryal bodies. In both cases the European influence is small. Therefore this challenge needs to be addressed. Considerations with respect to scalable data management are important in the context of cloud computing as the amount of data being processed is growing constantly and as the majority of Web applications are designed to be driven by traditional database software and porting them to utilize alternative data stores is often not feasible. In particular other emerging technologies such as Big Data are relying on Cloud Computing and require addressing this to unfold their potentials.

Data security

The most important security issue is confidentiality. After the Snowden revelations it has become known that the NSA is attempting to "(i)nsert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets." (Guardian 2013c) This not only means that it can Internet traffic and data stored on Cloud servers, it has also access to online company computers. The US government

even has access to encrypted information, e.g. through manipulated random number generators and even "encryption chips" (Guardian 2013d). It turned out that the concerns of businesses to put confidential data to Cloud servers, widely reported in surveys, were rather justified.

As identified in the STOA project on eGovernment security, Europe would benefit from having a reliable, highly secure or even proven computing base, without any scope for zero-day exploits or Trojan horses. This is the only way in which a solid base for future computing can be achieved. Such a secure computing base would have to comprise both hard- and software. It is also an aim of the US DARPA Crash program. Based on this, high quality applications could be used, and attacks on servers be reduced, either because of less vulnerabilities, or because of using isolation.

While Cloud services can be used to backup encrypted data, with or without a secure base, the challenge to process confidential data remotely without any insiders having access remains. Homomorphic encryption is an approach to solve this, but it is unclear if it will ever be economic. An alternative would be to explore the costs of using large, mass-manufactured devices using tamper-detecting membranes.

Regarding confidentiality, "privacy by design" would help consumers in particular, e.g. by the use of pseudonyms or attribute-based credentials (which reveal only, e.g., the age, but not the identity).

As to availability, there is the general risk that Cloud servers might be down, that a denial-of-service attack is taking place, that no network is available or that a provider goes out of business. While aspects of this can be addressed with various means, in general Cloud users will need to consider a backup solution such as local storage and processing.

Cloud computing, privacy and the EU data protection regime

Data protection law is applicable currently elaborated by Directive 95/46. This Directive is designed to protect fundamental rights which might be harmed by data processing and is applicable to all cloud computing in which personal data is processed.

There are four core problems created by the specificities of Cloud Computing for data protection law.

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, however, 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 and the applicability of the Directive can be difficult to establish.
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 between cloud provider and cloud client, call into question the delineation of roles and responsibilities imagined in the Directive.
3. The problem of worldwide and continuous data transfer: Cloud Computing service provision can utilize 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 without further protecting individuals' rights.
4. The lack of a binding European interpretation mechanism: The above issues remained problematic, as the Directive provided no mechanisms to adapt to them.

In 2012, the Commission released a draft Data Protection Regulation aimed at replacing Directive 95/46. There may be changes to the text before the Regulation becomes law – a revised text was voted on in the European Parliament in October – however, the general framework outlined in the Regulation looks likely to remain.
There are several changes with varying significance made by the Regulation to address the problems identified in relation to the Directive.
1. The Regulation offers a clarification and expansion of scope: This is aimed at ensuring that the application of data protection law is clear and that EU citizens' data is protected regardless 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 trans-border 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.

There are also several novel features introduced by the Regulation which may affect the provision of cloud services. Of particular importance are; 1. The right to be forgotten; 2. The right to data portability; 3. Data protection by design and default. It remains to be seen, however, precisely what the effect of these innovations will be.

Governance issues related to data retention and enforcement outside the EU

The difficulty of governing Cloud Computing, which arises from the plurality of jurisdictions involved, is well-known. But over the past year the world has gained insight into trans-legal (if not illegal) practices of third-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. The proposed regulation seeks to provide means for the enforcement of European privacy policy in international markets. Currently, it seems that this approach has support in the European Parliament.

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 Safe Harbour. The benefits of greater enforceability are obvious. 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. Strong European leadership may alleviate this disadvantage. 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. 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. And while "Europeanisation" of cloud governance may be preferable to other tendencies of Member State actions, which point towards nationalisation, there are real risks of a global polarization that may spill from matters of ICT governance into areas of economic, strategic and perhaps even military collaboration.

One pathway forward, which may meaningfully supplement the proposed strengthening of Europe's position, may be a true internationalisation of governance structures underlying the functioning of the Internet. So far, the world has relied on an Internet governance regime largely founded on U.S. hegemony. But now, we see calls for the severance of historical ties between core Internet infrastructure and the U.S. military-industrial complex. If Europe is ready to answer this call, it may contribute to a sea change in ICT governance and a global step forward towards the realization of the liberating potentials of a neutral, open Internet.

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 contexts. 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 couple of other aspects. Besides 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 an 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 interventions, if possible at all, needs to be made 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 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. This is reinforced by issue of the location of data in storage, transit and processing, which was identified as one major concern. Though many of these issues for consumers are addressed by the current draft regulation on data protection, the situation in business differs and needs 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 AUPs and TOS. Especially the end users are often affected by this, which needs to be addressed by standardizations and simplifications. 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 Computing. 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 Computing by consumers 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 consumers and businesses can only rely on third party certification of security and IT governance policies used by Cloud providers. The currently most used information system assurance and related trust marks, however, 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, the analysis of IP issues 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 refer to a general set of issues in the current IP scheme and raises the questions if and how these issues should 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 and 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 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 to offers of other providers (vendor lock in). This includes 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 a vivid and competitive market by supporting a competitive landscape of European providers. They are underrepresented in the worldwide IT industry, which contradicts Europes position as the second largest market, is subject of research for a long time. Regarding Cloud Computing there are two major points. The first one is the fragmentation of the market. It refers to a broad set of issues all dealing with challenges to cross-border activities in Europe. There are still issues that need to be addressed to enforce the creation of a single market for digital services. The second point related to a 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 a 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 the focus of the discussion. The latter point relates in particular to the role of the state as procurer as well as to the level of public R&D funding. Apart from specific challenges in all these areas, the lack of coordinated strategies combining funding and procurement is an issue that needs to be addressed. While there are many activities to increase the level of venture capital or stipulate founding activities there is also some point in the question why it did not succeed until now. Some research argues that this is caused by the fact that European investments were often directed to local invention, instead of exploiting the potentials of the open internet. Some analysis indicates that similar to the lack of a coordinated approach to R&D funding and procurement, there is 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 competitiveness due to their character as framework conditions for it. Skilled personnel is fundamental for both providers of cloud services as well as their users. Especially the ability of users to exploit the potentials of Cloud Computing and related other emerging technologies like Big Data is fundamental to realize the positive societal and economic benefits of it. Based on the 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 and 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 for a suitable network infrastructure. 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 concern 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 appropriate balance for all relevant stakeholders, including customers, service providers (incumbents as well as emerging players) and content provider.

SNS and major privacy challenges

The history of contemporary SNS is relatively short but turbulent. In practically no time, the variety of applications available and accordingly the user rates increased enormously: big players such as Facebook today count almost one billion users. In their very beginnings, SNS started as niche applications, already in the late 1980s and early 1990s with a first impetus from early web communities and interest groups. The first messaging services appearing during the 1990s created options to connect with other Web users and create contact lists. Few years later, sixdegrees.com, the first profile-based SNS combined different features for self-presentation, managing contacts, and messaging. The user profile today is standard in contemporary SNS and part of their core architecture as profiles are the main entry points to access all functionalities of SNS. The profile-based SNS expedited further developments and facilitated the occurrence of different community-focussed SNS. With increasing usage rates, business-related SNS and SNS devoted to particular interest groups appeared (e.g. the music-focussed MySpace was the most popular site during the early 2000s). After Facebook entered the global stage (in 2003), a broad spectrum of social media services (such as YouTube, Twitter, etc.) became available and SNS became part of the mainstream. Entailed is an on-going trend towards the integration of services and applications, transforming SNS into platforms for a broad spectrum of different features expanding also to the outside Web. Major drivers in this regard are social plugins and social graphs that link SNS and other web environments. This can affect the shape of the World Wide Web in general. Thus, the societal impacts of SNS are considerable, which not least reflects in the wide diffusion of SNS and the manifold different user groups. For most users, the main motivation is to continuously maintain and establish relations with friends, contacts, etc. The networking structure of SNS provides a variety of new modes of interactions to support this. The basic functionality of SNS to some extent grounds on classical theories in the field of network analysis: for instance Milgram's (1967) "small world problem", addressing the "six degrees of separation", i.e. that every person globally can be related over six degrees to any other, and Granovetter's (1973) hypothesis of the "strength of weak ties", claiming that loose connections have a strong impact on network expansion as they function as bridges across different network nodes. The growth of SNS environments is coined by these concepts and the variety of types of content available across SNS environments. Users' interactions are often related to dealing with content (e.g. consuming, sharing, creating, etc.). By enabling and stimulating one-to-many and many-to-many interactions among personal as well as non-personal entities (i.e. content) these new modalities contribute to the self-amplifying dynamic of SNS. A core aspect in this regard is the instant distribution of information among extensive numbers of users, groups or communities on local and global scale. This entails a broad spectrum of positive effects, such as social learning; new options for participation; strengthening community building; developing social capital; and enhancing political empowerment. A democratic potential of SNS has been highlighted for instance by the Arab Spring Revolutions, although in an ambivalent manner. While social media channels were supportive and catalysing means for activists and democratic movements to transform the governing regimes towards

democratic systems, the same channels have been used by authoritarian regimes for control and repression. Hence, social media can make a democratic difference, but only if people use it in that sense. The participatory capacity of social media is fed by the many different interactive features, which also stimulate the production of new knowledge. The variety of new possibilities for information exchange, mutual learning and collaboration is particularly relevant in scientific contexts. The increasing relevance of user-generated content also provides valuable source for various kinds of business models.

Privacy is among the most controversial issues in SNS environments as relations, content and interactions are both explicitly and implicitly linkable to individual users. While a complex privacy "puzzle" stresses contemporary societies in general, SNS represent a significant part entailing many privacy challenges. A major problem is the lacking distinction between user information, interactions, and content. The combination of these issues enables SNS to gain deep and far-reaching insights into user behaviour and identity. Recent innovations such as the social graph aim at systematically mapping the variety of different relations and interactions and thus aggravate these problematic aspects. This results in multiplying the existing barriers for users to exercise their right to informational self-determination. Insufficient or lacking privacy protection mechanisms in SNS architecture reinforce this problem. This underlines the demand for privacy-by-design concepts as integral parts of SNS environments. Respective strategies need to deal with at least two core problems of contemporary privacy protection: a disclosure-by-default paradigm exemplified by SNS, i.e. the widespread availability of personal information as standard mode; and the related increase in personal identifiable information reinforced by a convergence of personal and non-personal data as one result of the multiple interactions, not least between personal and non-personal entities. Contemporary SNS affect several different types of privacy (such as communication, data and image, behaviour and action, location). Considering emerging trends related to SNS, privacy impacts might increase further with social plugins and graphs, biometrics and face recognition technologies, as well as mobile SNS usage and location-based services as fast growing markets.

In general, measures to address the major privacy challenges identified should not least trigger a shift of the prevailing disclosure-by-default paradigm towards a setting where privacy-by-design and privacy-by-default are the leading principles. More precisely, this shift might be stimulated by the following measures: Enforce content encryption as standard; foster anonymity and pseudonymity; strengthen freedom of information and transparency; raise awareness for privacy and transparency; stimulate innovation for privacy by design; strengthen the role of Data Protection Authorities to improve checks and balances. These measures are particularly salient in the face of the recent scandals revealing large-scale surveillance of individuals on a global level. While the collateral damage caused by these scandals is yet unpredictable, they highlight urgency for a revitalization of privacy – a concept that is strongly connected to the need to recover the individuals' trust in the system.

Conclusions

Overall these results underline that action is necessary to ensure that the positive potentials can be realized by all and for the society and economy at large. In particular the

recent developments such as NSA disclosures or cyber criminal activities have potential to undermine the trust of consumers and business and make them concerned about security and privacy. Normally, a situation like this is then often coined by the contradiction of interests, but also the IT and internet industry started to realize that trustworthiness is in the long run a critical factor for their business. This situation offers new opportunities for Europe and creates some reasons to take action in Europe now. The first one is the need for a holistic approach. The analysis shows that neither more technological solutions nor more regulations nor new governance structures will solve the problems alone. Only a combination of strong security, modern and appropriate privacy regime, fair legal environment and improved governance structures will assure that potentials for misuse can be minimized. The second reason to take action is that this would allow Europe to use the chance to gain more importance in the global discussion on digital society and economy. Finally, it also offers a chance to boost the European ICT and Internet industry.

Suggestions for policy options

The overall conclusions show that at the moment, there is a unique chance to achieve multiple Cloud Computing and SNS related goals simultaneously. There are no contradictions in assuring European citizens secure, privacy aware, legally certain and fair use of Cloud Computing and SNS and in increasing the competitiveness of European ICT industries. Moreover it is possible to exploit the potential of Cloud Computing and SNS to the benefit of both the European economy and society at large. Consequently the aim of the last step of the project was to prioritize the identified policy measures. For this we evaluated the options, analysed interrelations and complementarities, and, finally, derived a coherent and consistent set of options for European policy makers, which is grouped into four thematic blocks. The blocks and options are listed below. For a detailed description of each option please see section 6.2.

Make security a commodity

At the moment IT security is sometimes difficult. Solutions can be hacked, even if, e.g. a powerful crypto system is used, or sometimes they are inconvenient to use for normal users. Therefore it is necessary to support the development of highly secure IT solutions, which are easy to use and which can be adopted by all businesses, both big and small, as well as by all citizens.

1. **Support the development of open and secure software and hardware and encryption methods.**
2. **Encourage the use of checklists and certifications.**
3. **Assess the economic viability of hardware security modules.**
4. **Initiate a dialogue on the structure and governance of the Future Internet.**

Establish privacy as a location advantage

For a long time, European data protection standards were seen as a disadvantage for digital business. Recent developments, as well as changing requirements for emerging technologies and a growing digitalization of all spheres, underpin the necessity of modern privacy rules. By modernizing the data protection regime Europe could not only ensure a better protection of citizens, but also serve as a model for emerging markets, which could be attracted to increase their exchange with Europe. Moreover Europe could underpin this

function as an example for modern and appropriate privacy regime by addressing a fair and secure governance and proposing a structure of an open Internet at a global level.

1. **Proceed with the modernization of data protection.**
2. **Establish the principles of security and privacy by design.**
3. **Support the creation of a European Data Protection Board.**
4. **Ensure the extraterritorial application of European data protection law.**

Build a trustworthy environment for digital business and living

Digital life of citizens and business needs legal certainty to ensure new ideas are taken up. Since many emerging ICT create both new chances and new challenges, there is a need to continually review existing legislation and to adjust it if necessary. Only if people have trust in legal certainty, they will adopt and use new technologies and exploit their potential for the economy and society as a whole.

1. **Stipulate the setting of minimum requirements for contracts.**
2. **Support the standardization of Acceptable Use Policies and Service Level Agreements.**
3. **Eliminate jurisdictional uncertainty.**
4. **Support the development of certifications.**

Create an inspiring ecosystem for ICT industries

A crucial precondition for a competitive ICT industry is an inspiring ecosystem. This is illustrated by examples in other regions (Silicon Valley, Israel) or other industries (cars, machine equipment). Such ecosystems contain many components. Of particular importance is support for innovative and fast growing companies as well as the provision of sufficient framework conditions.

1. **Encourage the creation of European market players.**
2. **Support standardization and interoperability.**
3. **Empower people across all strata of society.**
4. **Reconsider current broadband strategies.**

1. INTRODUCTION

1.1. Impacts and challenges of Cloud Computing and Social Network Sites

In recent years, Cloud Computing and Social Network Sites have become major trends not only in business but also in various other fields of society. Although the introduction of more and more information and communication technology into all spheres of life has always raised discussions, there were only a few as controversial as the on-going discussions on these both technologies. These technologies are associated with high expectations and opportunities but also with a number of concerns and risks. Both, advocates and opponents, use many arguments, such as:

- *"With Cloud Computing, no one knows where the data is located."*
- *"Social Networks enable the easy connection of people."*
- *"Cloud Computing will change the way we use information."*
- *"Social Networks pose threats to children and young adults."*
- *"Cloud Computing is always less expensive than on–premises computing."*
- *"Social Networks increase the efficiency of collaboration."*
- *"Cloud Computing is only one more new hype in the IT industry."*
- *"Social Networks are the end of privacy."*
- *"Cloud Computing will help to create new employment and innovation."*
- *"Social Networks will will disrupt offline social relations."*

This list of arguments is only a random sample and can be easily extended and varied. However it already shows that the perception and the way on how Cloud Computing and Social Network Sites are perceived and discussed is characterized by a strong antagonism of arguments. On the one side there is a tendency to celebrate euphemistically the potentials and benefits for individuals, businesses and the society and economy as a whole, while on the other side there is strong perception of these technologies as threats.

This antagonism is very obvious in the case of Cloud Computing. There is the expectation that Cloud Computing offers significant opportunities for customers as it reduces the total cost of ownership of information systems and consequently lowers the barrier to acquisition respectively usage of IT systems for (especially smaller) enterprises. It is also expected that these new forms of usage and the underlying new business models will also impact the current European IT market structure, resulting in important value transfers and price reductions and impacting all segments. Beside the impact on the IT industry itself, the development of both is also seen as pivotal for the overall competitiveness of the European economy and society as a whole. It is considered as a chance to increase the low adoption of ICT technologies, in particular in SME, which is seen as one reason for the European productivity gap

However, Cloud Computing also pose a number of challenges for enterprises as well as for private citizens. There could be increasing virtualisation of the processing of personal and other sensitive data that is transmitted and stored by commercial providers on servers situated in a location unknown to the costumer. Therefore, data protection and security are

crucial issues, since it has always been a limiting factor for the trust that businesses and consumers have in cloud services (and its predecessors). Often it is not clear which of the different arguments are realities and which are myths. It also reveals that there is no clear understanding what Cloud Computing is and how it works. One reason for that is the practice of many providers to label all kind of internet-based services as Cloud Computing. At the same time different actors have different understandings of the terms, depending on their specific perspective and the technologies themselves, keep changing. Moreover, it also underlines that there is only little knowledge on how it is used, by whom it is used and which factors influence the further development. Therefore, the current picture we have of cloud computing and its impact is somewhat blurred.

However, it is also true that both technologies, Cloud Computing as well as Social Network Sites, have impacted modern societies. Even if their ideas are not realised swiftly or perhaps never completely, they will lead to discussions on possible impacts – in particular data protection and autonomy and sovereignty of users – on central topics of IT-related technology assessments. This can be exemplified using the example of Social Network Sites, which emerged before Cloud Computing. Although it is typically not associated with Cloud Computing, they already now pose similar challenges on a large scale. Companies such as the current global market leader Facebook provide a service which allows for uploading data and connecting its users. It became extremely popular among private citizens as well as among many companies who try to capitalise on the new ways of marketing. At the same time, issues connected to user´s privacy rights and data protection have led to heated debates. Consequently, both technologies and applications were major reasons and objects of the ongoing revision of the data protection framework of the EU, which is a further reason to deal with both of them.

1.2. Scope and aims of the report

This report addresses in the first place Cloud Computing and furthermore Social Network Sites. The main reason for this scoping is twofold. The first part is that Cloud Computing as an infrastructure technology has broad implications for all areas of society, including business, public administrations, science as well as private households. The impacts of Social Network Sites are more focussed on the relationships between private citizens or private citizens and businesses. The second part is that Cloud Computing technologies are an important enabler for the rapid diffusion and usage of Social Network Sites, but it is also an enabler for other areas like mobile applications (apps) or Big Data.

Within Cloud Computing the report focuses on the potentials and impacts for businesses, but it also takes into account potentials for public administrations and consumers. In case of Social Network Sites the focus lies on the potentials and impacts of the more common, pervasive used public Social Network Sites such as Facebook or Google+, not on the increasing number of web-based restricted social network solutions for businesses such as Yammer (Microsoft) or BlueKiwi (Atos). Consequently it focuses on the implications for consumers.

As outlined before, there are many potentials associated with both technologies, but there are also many challenges connected to them. Given this situation, it is not clear if they will

meet the associated potential and the high expectations. Therefore the overall goal of the project is to analyse this blurry situation and to assess potentials as well as positive and negative impacts for citizens, business and public authorities from a European perspective. This includes in particular the following questions:

- What are the technological and economic developments Cloud Computing is based on?
- To what extent does cloud computing impact the European industry (including the ICT industry), public administration as well as consumers? What are the impacts on society and economy as a whole?
- What are the different issues to Cloud Computing in areas such as privacy/data protection, security, contracts, etc.? Which needs to be addressed?
- What are the different types of Social Network Sites? What are the factors, challenges and issues specifically related to the different categories of Social Networking Websites identified?
- What are the options for action for European decision-makers and in particular for the European Parliament?

2. FOUNDATIONS OF CLOUD COMPUTING

2.1. Defining Cloud Computing

A short review of some controversial discussions on Cloud Computing shows that many of the different views 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. One example for this practice is the remark of Larry Ellison, CEO of Oracle, in 2008 stating: *"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do"* (Dignan 2012).

Consequently there is a strong need for a clear definition of the term "Cloud Computing". Unfortunately there are many of them, but among them there is no one officially acknowledged. Most widespread in literature is the definition of the National Institute of Standards and Technology (NIST), an institution of the U.S. Department of Commerce, which has a working group on Cloud Computing. Other definitions that are in some ways relevant are the one from Gartner, who defines the market based on it, and the one of the EC Expert Group. While we focus on the first, we want to show the differences of the latter ones.

2.1.1. Definition according to NIST

In 2008 the Computer Security Division within the Information Technology Laboratory of NIST was assigned with the task to define the evolving concept of Cloud Computing and to asses in particular security and privacy aspects in public Cloud Computing. A first draft definition was already published in 2009. In this document Cloud Computing was defined as *"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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models*" (Mell/Grance 2009, 2). The definition was cited by many other authors and is today the most widespread and accepted definition. It is, for example, basis for the Federal Cloud Strategy of the U.S. Government (Kundra 2011) as well as for publication in other countries like the guidelines of the German IT industry association BITKOM (Weber et al. 2010). In 2011 the final version of the definition was released with no differences in the main definition cited above. (Mell/Grance 2011).

It is complemented by a description of the characteristics, service models and deployment models. In particular the characteristics are intended to specify this very inclusive overall definition more precisely. The five characteristics are described as the following (Mell/Grance 2011, 2):

- **On-demand self-service**, i.e. the customer can directly access and use his data through self-adjusting service without interacting with the provider.

- **Broad network access**, i.e. the service can usually be accessed and used through any Internet-capable device, including for example smart phones, tablets or any Internet-connected computer.
- **Resource pooling**, i.e. in general the Cloud Service providers resources, like storage or bandwidth, are shared between the users. However it is also possible to customize some parts like security requirements. As a consequence customers do not know the exact location of the different resources used.
- **Rapid elasticity**, i.e. Cloud Services can be easily adjusted to changes in the customers demand.
- **Measured service**, i.e. the user can control its usage of resources and, in case of payments, only pay for resources used in difference to his software licences and self-owned hardware.

Overall we can state that these five characteristics define Cloud Computing much more precisely then other definitions before. In particular, characteristics like resource pooling, elasticity or network access help to identify and differentiate Cloud Computing from related services like Outsourcing. Above that it introduces, as marked before, three service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as well as four deployment models, i.e. Public Cloud, Hybrid Cloud, Community Cloud, and Private Clouds.

2.1.2. Other definitions

Gartner, as a leading market researcher in IT, placed Cloud Computing for the first time in 2008 in the well-known *Hype Cycle for Emerging Technologies* (Gartner 2008). Subsequently, it also tried to define Cloud Computing, primarily to assess it as a market, and stated that it is *"a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies"* (Gartner 2009). Additionally Gartner also released a set of reports in which Cloud Computing and its application were defined more precisely by defining attributes (Plummer et al 2009) and giving insights into the what, why and when (Smith et al. 2009). The five attributes are:

- **Service-Based**, i.e. users should only have to deal with the offered service, not with details of the underlying technologies.
- **Scalable and elastic**, i.e. the ability to adjust the resources and services used to accommodate the changing demands of the users.
- **Shared**, i.e. the resources of the Cloud Service provider will be shared by its users.
- **Metered by use**, i.e. the usage can be measured precisely and consequently; the payment depends on the measured extent of usage.
- **Uses internet technologies**, i.e. users can access the service using devices based on standard internet technologies.

Above these five attributes, the different Gardner publications underline two more aspects. According to the widely accepted scheme they also differentiate between the three main service models (IaaS, PaaS, SaaS), but due to the needs as market researcher they introduce several market segments, which sometimes does not really fit into this scheme. Regarding the delivery model it seems like Gartner focus mainly on two models, either

public or private Cloud services. This implies that hybrid models are seen as a sub segment of public clouds and other models are judged depending on their implementation.

In 2009 the European Commission set up an expert group that should try to depicture the development of Cloud Computing, its impact and relevance for the European economic and research landscape. In 2010 the expert group published a report called "Future of Cloud Computing", where Cloud Computing was defined as *"an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)"* (Schubert et al. 2010, 8). As outlined by the group this definitions is as broad as possible. Therefore they also introduced several criteria including the different service and delivery models as introduced by NIST. Above that they also list a set of key characteristics and capabilities. In difference to the other definitions they divide them into three types: non-functional aspects, economic aspects, and technological challenges.

- **Non-functional aspects:** these aspects refer to different types of properties of the offered services. Given the fact that modern IT technologies allow different ways to achieve them, the result is that Cloud Computing services can vary strongly though they in principal offer the same service. It includes for example elasticity, reliability, agility, etc. (Schubert et al. 2010, 13-14).
- **Economic aspects:** clearly refer to the users interest to reduce the costs and increase the productivity of IT operations. It includes for example cost reduction, pay per use, return on investment or improved time to market etc. (Schubert et al. 2010, 14-15).
- **Technological challenges:** refer to aspects of the realization of Cloud Computing solutions enabling the economic and non-functional aspects. Consequently these realizations can vary due to the technological possibilities, i.e. there is always more than one technical solution. It includes virtualisation, multi-tenancy, security, metering, etc. (Schubert et al. 2010, 15-16).

Concluding we can state that the definition of the expert group is more detailed as the other two, in particular by using different sets of aspects and challenges they try to underline the interrelation of different characteristics.

All three definitions show many similarities, in particular the ones from NIST and Gartner. The definition of the EC Expert Group differs foremost in its degree of differentiation, e.g. the separation and accordingly the total number of characteristics, but not in its overall meaning. Therefore it seems obviously that there could be a possibility to merge them into one definitive definition. But as shown for example by the follow-on report of the Expert group on Cloud Computing published in 2012 (Schubert et al. 2012), Cloud Computing is still a moving target. Reasons lie in the dynamic development of the underlying technologies, but also in the dynamic development of the market and in particular in the marketing of Cloud Computing services. Faced with this problem the expert group comes to the conclusion that existing definitions like NIST, Gartner or their own definition from 2010 mainly reflect the current state of Cloud Computing but not the essentials of Cloud Computing. They try to sort out many points, but end up with three different definitions for users, providers and developers as well as a minimal definition aimed at eliminating all

superfluous characteristics that are not essential for Cloud Computing. This defines that *"an environment can be called "CLOUDified", if it enables a large dynamic number of users to access and share the same resource types, respectively service, whereby maintaining resource utilisation and costs by dynamically reacting to changes in environmental conditions, such as load, number of users, size of data etc."* (Schubert et al. 2012, 22). Although one can share their critics of the existing definitions, the offered solutions are also neither fully convincing nor really convenient. One reason is that the minimal definition could be used for a great variety of services. This creates the possibility to include future developments, which cannot be foreseen at the moment, but also bears the risk that the term could be attributed to offers that are not necessarily Cloud services in the eyes of most people. As a consequence the added value of this new approach is limited.

It shows that the definition of Cloud Computing is an ongoing process driven by different actors with varying interest. Consequently this report uses 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). Above that it also relate to the five characteristics introduced by NIST for the identification of Cloud Services. However, it might be possible that some of them may require changes and adjustments to the future developments in Cloud Computing.

2.2. Classification of Cloud Computing services

As important as the question how to define Cloud Computing is the question how to classify the different identified Cloud Computing services. The literature offers a broad variety of answers (see e.g. Yang/Tate 2012). The spectrum ranges from simple classifications based on the NIST service model to multilayered, complex taxonomies (e.g. Hoefer/Karagianis 2010).

In the IT and software industry typically business models are often used to classify different service offers. In theory and practice business models consists of a broad set of elements including for example strategy, revenues, offers, partnerships (see Osterwalder 2004). Additionally research has shown that some elements only relate to specific industries or specific activities. However several projects tried to research business models for the IT industries and their sub-sectors. In general they also show a broad variety of approaches with different foci (see for example Rajala et al. 2003; Buxmann/Schief 2012; Rajala and Westerlund 2007). Based on a review of this literature four elements seem appropriate to classify Cloud Computing services and offers. These are: 1. service models, 2. delivery models, 3. revenue models, 4. type of actors.

The challenge is that these aspects are still in flux, since Cloud Services are still an emerging market, where on the one hand new technologies continuously impact the possibilities of service offers and on the other hand many suppliers start try-outs of new and old business models. Consequently, there will be no final list of business models.

2.2.1. Service models

Widespread within the literature is the differentiation into three service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). They can be seen as a way how and what is offered by the different Cloud providers. As already mentioned, most definitions also refer to these service models, which are shortly explained in the following:

- **Infrastructure as a Service (IaaS):** in this case the provider provides processing, memory, storage, and network transfer capabilities for customers. Typically the customer does not control the actual underlying hardware infrastructure, but has possibly limited control over selected components (Mell/Grance 2011, 3). However, intelligent management mechanisms allow him to control the capabilities. The model allows customers to implement and run their own software including operating system and applications. The resulting high level of flexibility for customers is contrasted by the required high level of IT skills (Weber et al. 2010, 16).
- **Platform as a Service (PaaS):** in this case the provider provides a platform or environment for deploying applications (Mell/Grance 2011, 2-3). This can range from operating systems for the installation of normal applications to complex runtime environments including programming languages and tools for the development and test of new applications. As in the case of IaaS the customer does not control the underlying infrastructure and platform, but is in control over self-installed applications. It mainly addresses IT specialists (Weber et al. 2010, 16).
- **Software as a Service (SaaS):** in this case the supplier provides working applications, running on its own cloud infrastructure, to the customer (Mell/Grance 2011, 2). Typically the customer can access these applications via different internet based technologies like web interfaces or apps. Customers are neither in control of the underlying infrastructure nor in control of the used applications, i.e. providers mostly offer standardised software packages, where no or little customization is possible. Only few things like industry-specific solutions within enterprise software are available. Those offers are directed at end users and consumers (Weber et al. 2010, 16).

Although this differentiation is widely used, there is also a strong tendency to differentiate the list of service models even more. In recent years many other service models like for example Storage as a Service (Fielder et al. 2012, 19) or Business Process as a Service (BPaaS) (Forrester 2011 (after Dignan 2011)) were introduced. Even more can be found in the Wikipedia entry for Cloud Computing[1]. Not surprisingly, some even name Service as a Service or Everything as a Service as other concepts (XaaS), which is either the attempt to summarise all models under the umbrella of this term or an indirect critic to this inflation of services (see Esteves 2011).

There are limitations of this high level abstraction like for example the neglection of the great variety within the service models and the resulting critics that for example differences between single applications and complex enterprise software in the model of SaaS (see Schubert et al. 2012). Nevertheless this report will be based on this differentiation and will

[1] See http://en.wikipedia.org/wiki/Cloud_computing.

only adjust it if it is needed. This follows the reason that there is no agreement on other ways of differentiations and additionally by applying some of them we otherwise risk getting a victim of specific trends, limited developments or the marketing of specific groups. Additionally a more differentiated classification of service models would not automatically enable deeper insights into the potentials and impacts of Cloud Computing. On the contrary it could lead into the opposite direction and make it difficult to realize the underlying challenges. Therefore, the advantages of such an abstract level outweigh its disadvantages.

2.2.2. Delivery models

Like in the case of service models also delivery models show a broad variety of terms and definitions introduced by different providers, market researchers or agencies. Nevertheless most widespread is a differentiation based on the NIST definition. It separates between the following models:

- **Private Cloud:** In this case the infrastructure is provisioned for exclusive use by a single organization. It can be owned, managed, and operated by the organization themself, a supplier as a third party, or some combination of them. Additionally it can exist on or off premises of the organisation (Mell/Grance 2011, 3; Schubert et al. 2010, 10-11; Qian et al. 2009). Therefore special forms, can be also considered as a private Clouds. These are listed by some researchers as e.g. virtual private Clouds (e.g. Ried et al. 2011), where the cloud is hosted on dedicated, virtual machines in the data centre of the Cloud provider, as well as managed private clouds, where the cloud is hosted by a third party in the data centre of the customer
- **Public Cloud:** In this case the infrastructure is made available to the general public and is owned, managed and operated by a third party specialised in providing such services at their premises. Customers therefore share the resources of the infrastructure (Mell/Grance 2011, 3; Schubert et al. 2010, 10-11; Qian et al. 2009). This is what in public is mainly seen as Cloud Computing.
- **Hybrid Cloud:** In this case the infrastructure is a composition of two or more distinct cloud infrastructures. They can be of same type or of different types like public or private, but they have to be unique entities. Normally, they are connected by standardized and/or proprietary technology that enables data- and application portability (Mell/Grance 2011, 3; Schubert et al. 2010, 10-11; Qian et al. 2009). In general this is a very strict definition, when compared to popular literature such as computer practitioner magazines. There the term hybrid solutions may also be used in cases, where a company uses Cloud Services in addition to its own infrastructure, which does not have to be organized as a Cloud. From the market point of view it cannot be differentiated from the other forms of a Cloud model and consequently each part of the used services is accounted either as public or private Cloud services. Based on that this report does not follow the strict definition of NIST.
- **Community Cloud:** in this case the *"infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns"* (Mell/Grance 2011, 3) and can be owned, managed and operated either by one of the participating organisations or a service provider as a third party involved. Therefore, depending on the actual implementation, this would be either accounted as virtual private Cloud (third party as provider) or a private Cloud (organisation as provider)

due to the fact that it is no public offering. For the using organisations it may be a hybrid Cloud, due to the fact that may have also other capacities. However this type seems to be rather rare.

Based on the scope of the project the report focuses on public Cloud offers and related models, i.e. hybrid solutions, which are addressing consumer and user in small and medium sized companies. In reverse it implies that private Cloud offering, which is technical and organisational often a continuation of previous virtualisation efforts or traditional IT-Outsourcing (managed private Cloud) are of less interest. Moreover the number of challenges are less, because of the internal character the involvement of third parties are not given, while restrictions like data transfer regulation also apply.

2.2.3. Revenue models

There is a broad range of publications dealing with revenue models, which mainly features two aspects: the cost model and the pricing model. Since the pricing mechanism is more obvious than the cost structure of the provider most of the literature focus on it. Though there is set of pricing mechanism like pay per use/pay as you go, flat pricing/subscriptions or auctions, the definition and categorisation varies strongly(see Osterwalder 2004, 95-101; Harmon et al. 2009). This problem is also reflected in the discussion on pricing mechanism in Cloud Computing. They focus mainly on the different types of pay per use/pay as you go mechanism (i. e. Weinhardt et al. 2009a&b; Yeo et al. 2010), which is, as already indicated by some of the definitions and characteristics; seen as an essential novelty of Cloud Computing in contrast to earlier pricing mechanisms in the software and IT industry. They also often discuss the complementary model of subscription based pricing mechanisms, which is also often used (e.g. Youseff et al. 2008; Weinhardt et al. 2009b). Only few publications also discuss other forms of pricing mechanism like market based pricings or so called dynamic pricing mechanism (i. e. Anandasivam et al. 2009). This includes for example auctions as introduced by Amazon Web Services with the Amazon Spot Instances, where customers can bid for free capacities of Amazon. Although it seems like pay as use/pay as you go models are predominant and that they are also future of Cloud Computing, there is also some argumentations against it. Durkee (2010) argues that the on-going price competition based on the pay as use models will create problems for suppliers in the future. Therefore his belief is that suppliers are in need for value-based approaches that would also result in other pricing mechanisms.

Based on the review of literature and offers, we identified four basic pricing mechanism categories that can be used for classification. Each of them can contain several different pricing mechanisms:

- **Subscription based pricing:** this category includes all services offered with fixed fees. Possible examples are fees per user/month as well as fixed fees for a certain amount of service like for a predetermined amount of data storage etc. As already mentioned this pricing mechanism can also contain elements of differentiation to a certain extent.
- **Usage based pricing:** this includes all pricing mechanism based on the actual usage of services. In this case usage can be measured in different dimensions dependent on the service offered as well as the measurement system. Examples are the amount of

data storage, instances or similar. Although this is often claimed as being the novelty of Cloud, comparable pricing mechanism existed before like the performance pricing based on MIPS as used by IBM.

- **Flexible or dynamic pricing:** it includes all mechanism like auction, reverse auctions or spot markets, where prices are formed dynamically in market-like structures. At the moment only few of them exist as already mentioned. Some publications even state that the method, though it is enabled by features of Cloud Computing, will not retain due to its complexity for the user (see for example Khajeh-Hosseini et al. 2010).
- **Advertisement based pricing:** this category, which is not often reviewed in the typical business literature, encompasses all services that are offered without any kind of fees. But since there are no such things as a free lunch, customers get advertisements presented, sometimes even based on the analysis of their usage. While pure advertisement based services are seldom, one can find a hybrid version, the so called *"freemium"* services, where a basic service is financed by advertisement, but upgrades enabling extended services are subscription or usage based. One example for such an approach is Dropbox.

Overall the review shows at least two points. Firstly, it is obvious that nearly all identified categories show some developments towards a hybridization of pricing mechanisms. In particular this tendency is obvious in the case of subscription based services. Somehow it seems at least for this category these **hybrid models** are one way to replace the classical model of licences and maintenance fees. However it is hard to create a fifth category for them due to the fact that the hybrid models differ strongly. Secondly the review showed that some pricing mechanism are, as already hinted, more related to a certain type of service model or customer, like usage based pricing and IaaS or freemium services for private consumers. This shows that, although most people think of one dominant model, the reality is diverse and moreover still in flux. Consequently, this report does not exclude any services because of the pricing model.

2.2.4. Type of actors

Due to the dynamic and evolving character of Cloud Computing technology and market, business models are still in the flux. Consequently newer research argues that they are still developing and have to adjust. Some argue that each service may lead to an own business model (Zhang et al. 2010, Marston et al. 2011), while others argue that a value chain approach is most suitable to describe business models, actors and the resulting ecosystem. One example is Leimeister et al. (2010), where they differentiate between five types of actors and models:

- **Consultants**, who supports customers in selecting, implementing and integrating offered services;
- **Service providers**, who develops and operates services offered and deployed on a Cloud Computing platform;
- **Service aggregators**, who develops and operates services based on other existing Cloud Services. Sometimes differentiated into service and data integrators;
- **Platform providers**, who provides an environment where cloud applications can be deployed;

- **Infrastructure providers**, who provides the necessary scalable hardware and related computing and storage services for the services

The resulting value network (ecosystem) is only a generic snapshot of possible models and actors. In reality many companies combine several types of actors, sometimes even the full value chain, like HP, with its own public Cloud offers. Another point is the appearance of new actors and business models. One good example is Zymory, a spin-off of Deutsche Telekom T-Labs that acts as broker or intermediary between data centres, who want to offer unused resources in order to increase their revenues, and companies in search for computing or storage capacity. In the value network of Leimeister et al. (Leimeister et al. 2010) these new kind of actors would be placed somewhere in-between infrastructure and service providers.

Recently such developments were taken up by the NIST reference architecture, which differentiates five distinct types of actors: 1. Cloud consumer, who uses services; 2. Cloud provider, who makes offers available; 3. Cloud auditor, who independently assess different functionalities (operations, performance, security); 4. Cloud broker (including service intermediation, service aggregation and service arbitrage), who additionally manages and negotiates relationships between providers and consumers; 5. Cloud carrier, who provides connectivity and transport (Bohn et al. 2011, 4-9). Similar to the previous model it also underlines the possibility that actors can take more than one role and that, as a consequence, possible relationships can vary strongly. Therefore it is in most points comparable to Leimeister et al. (Leimeister et al. 2010), but takes a more technical perspective in the description of actors. Finally, there is also the high probability that, like in the software market, strategic and technical alliances or partnerships as well as different types of special arrangements will evolve over time. This will lead to shaping of existing forms of ecosystems and underlying business models or actors and possibly to a creation of new ones. Therefore, the differentiations of actor types are well suited to classify offers, but due to their evolving status they are not suited to exclude or include specific offers.

2.3. Technical foundations of Cloud Computing

2.3.1. Origins and evolution of Cloud Computing

Cloud Computing as a concept is nothing totally new. The idea and concept of Cloud Computing already evolved in the 1960s. In 1961 John McCarthy had the idea to offer computer-services as public services (Garfinkel 1999). The following years ideas and concepts foresaw the shared use of computing capacities through networks. Most of them were related to the development of multi-access operating systems, which started their take up on mainframes in the late 1960s and early 1970s. Though the technical implementation was very basic, the ideas behind them were the same. Some of the researchers even described far more complex concepts closer related to Cloud as it is today, but these were not applicable at that time. Due to the miniaturization and personalisation of computing those ideas and concepts became less noticed.

A new wave of concepts related to these ideas started to evolve together with the technical developments in internet technologies, hardware and distributed systems and their growing

diffusion. In particular, the availability of more and increasingly better network connections led to a revival of the idea to use computing capacities and applications via networks resources. Moreover, Service oriented Architectures and web services had an impact. In the 1990s several concepts and technologies like ASP, Distributed and Grid Computing evolved. Although these approaches differ in their scope as well as their technical architecture from Cloud Computing, they started to lay the ground for it and some companies involved in it like Salesforce became early movers in Cloud Computing. Also the term "Cloud Computing" were introduced in 1997 Ramnath Chellappa, which he defined it as a *"computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone."* (Chellappa 1997). However, the breakthrough of the term only happened since 2008. Until this the other concepts, which will be explained in the following were more prominent.

Application Service Provisioning (ASP), which emerged in the late 1990s, was aimed at the provisioning of IT-based services over a network that could be accessed online via web browsers. The software or application is installed on an external server that also processed the data; a local installation is no longer necessary. The service is accessed independently from the user's location but internet access is nevertheless necessary. Also "use on demand" is part of this concept and ASP also brought a new billing model: The service is paid per-use or a user dependant fee is charged. It can be seen as a predecessor of SaaS. Due to weak networks at that time it could not handle real-time operations and high data exchange rates and the high expectations associated with could not be fulfilled.

Distributed Computing components (or nodes) communicate over a network and make up a distributed system of computing resources. The software components run on different autonomous computers but are combined to one single system to solve tasks. Advantages of distributed computing are the scalability of the system through adding further machines as well as that it seems for the user to be one system. Now middleware, for the first time, plays an important role as interface between user and components. It coordinates the information flow and is a fundamental requirement to hide the complexity from the user as well. A special case of it is **Grid Computing**, where supercomputer are constructed through the networked, loosely coupled computers to perform large tasks on demand. Access is provided over standardized protocols. In the beginning it was strongly driven by the scientific community and led to complex interfaces for usage, but later on also commercial applications appeared. Often Grid and Distributed Computing as terms were used as equivalents.

Finally there is **Utility Computing** that can be seen as predecessor of Cloud Computing. In general it refers to the delivery of particular IT services as a metered service, i.e. IT services were delivered and charged based on usage. The concept itself started to evolve at the same time as ASP, but did not become main-stream until the mid of the 2000s. But while ASP experienced a relabeling into SaaS, utility computing as a term started to gain impact in 2005 by an article forecasting the end of the corporate computing (Carr 2005). The article and the following discussion sketched out many basic principles, virtualisation, service orientation or similar, of utility computing, which are the same for Cloud Computing. However, at this point it was still seen as a niche development like Grid

Computing, which were both often closely connected (LaMonica 2005). However, with the raise of the term and concept of Cloud Computing the term Utility Computing started to disappear.

Altogether these concepts and technologies created the basis for Cloud Computing. Seen from today it is obvious that they addressed different basic technologies like resource pooling and sharing and characteristics like usage based pricing as well as different kinds of service models. While ASP mainly offers Software as a Service, Distributed/Grid Computing has a focus on offering computing power through the aggregation of resources (Infrastructure/Platform as a Service). Finally Utility Computing refers in parts to the segment of Business Process as a service. Above these also other, related developments like Pervasive and Ubiquitous Computing played a role. They describe a world full of smart, always connected devices integrated in our daily life (Pervasive Computing) and intelligent environments reacting on the user (Ubiquitous Computing). This refers to the developments in mobile computing and internet, where small clients use a connection to a Cloud to solve task.

2.3.2. Cloud Computing technology

Cloud Computing is based on a basic architecture as well as several technological developments and requirements, which took place in the last decade. Though there already exist well-functioning offers, there are also still possibilities for further technological developments.

Cloud architecture

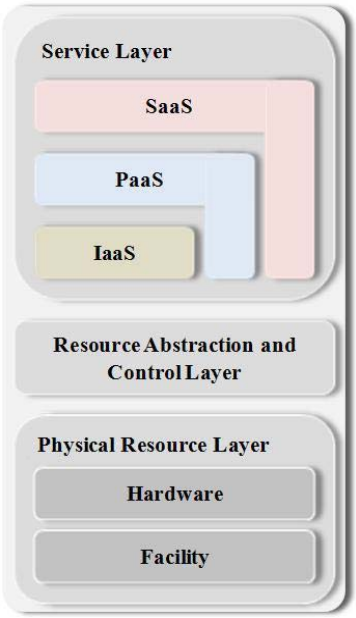
The Cloud architecture according to the NIST reference architecture knows three layers (Bohn et al. 2011, 12-14). The top layer consists of the three services IaaS, PaaS, and SaaS, which were already explained in the previous chapter. It might be important to mention that the control of the user increases from SaaS to IaaS. All three can have a dependency in case that SaaS services are build on PaaS or IaaS. Finally this layer offers also access to each service, normally based on web services (Bohn et al. 2011, 13).

The middle layer encompasses the resource abstraction and control. The first enables the Cloud supplier to provide and manage the usage of the physical computing resources by different users. It is achieved by software abstraction enabling multi-tenancy. For that purpose different types of software are used, typically for virtualization like hypervisor, virtual machine etc., which should help to ensure efficient, secure, and reliable usage. The latter part relates to different types of Cloud software enabling resource allocation, access control, and usage monitoring (Bohn et al. 2011, 13). The physical layer contains all physical computing hardware like computer, network, storage and other computing equipment as well as the resources provided by the data centre facility like air condition, power and other things (Bohn et al. 2011, 13-14).

Consequently the main technological foundations are based on the two concepts of multi-tenancy and service orientation. While the first one describes the ability to manage the access and use of computing resources by different users, the latter one describes the principles how the services are designed and implemented. Both concepts are closely

connected to specific technical implementations. In the case of multi-tenancy the solution is, at the moment, the existing virtualisation and management software, which enables the abstraction required for an efficient use of computing resources by many users. The solution for service orientation is web services, which enable customers to easily use the different service offers.

Figure 1: Cloud Architecture, Source: Bohn et al. 2011, 13



Web services and Service oriented Architecture (service layer)

Services in the Cloud are offered as web services. These rely on Service Oriented Architectures (SOA), which have as their core concept the offering of services over a network. The concept of SOA is several years old and the fundamental elements ot it are open standards, security and simplicity. SOA in itself is only a related concept to Cloud Computing; they are different, but have a certain overlap. Both offer web-based services and are fully dependent on the internet. Cloud Computing is a whole new technology/trend, while SOA is more an architectural paradigm.

Web services are the implementation of a SOA and are prerequisites for Cloud service offering. Web services are defined by the W3C: *"software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."*[2]

Multi-tenancy and virtualisation (abstraction and control layer)

Multi-tenancy and virtualisation are the technical basis of Cloud Computing. Both describe the possibility to share resources to different clients.

[2] See http://www.w3.org/TR/ws-gloss/.

Multi-tenancy is about sharing the same application. Each customer shares the same physical IT-infrastructure and can customize parts of the applicati on but not the code of the application. Each resource or instance is assigned to multiple users, enabling an efficient way to maximise the utilization of the given resources. In addition customers do not share or see extraneous data.

Virtualization is about sharing the same physical hardware. Physical resources, e.g. a number of servers, are aggregated in pools, so that they are manageable as a whole. Then virtual machines are created. A virtual machine is a software implementation of a real machine and has mainly two realizations: system virtual machines, where complete operating systems are executed as well as process virtual machines that only run single programs. In the context of Cloud Computing different kinds of virtualization are distinguished (Baun 2011, 5), e.g. operating system virtualization or application virtualization. Virtualization supports several features (Schubert et al. 2010). An example is the independence of the infrastructure. This enables the code to be applied on several operating or hardware systems, regardless of their limitations. The offered services can be therefore location independent and accessible from everywhere.

Technological requirements of Cloud Computing

Due to the functionalities and basic principles of Cloud Computing there exist some critical requirements, which are the following:

- Networking availability: One of the main technical requirements is a stable and secure network connection between Cloud system and the device or end-user. Also the (insecure) connection is an attractive target for attacking the system. Another point is the network capacity. A strong limitation of the performance is the bandwidth of the internet connection. In local networks the speed is much higher, which should be considered when moving to public
- Reliable Cloud Service Offering and Fault Tolerance: Reliability is a crucial requirement. Therefore, the system must provide fault tolerance to be reliable. It has to cope with network outages and failures on nodes. Most often the data storage is replicated on several data centers all over the world to offer a reliable system. The reduction of any single points of failure is one of the main challenges to offer reliable Cloud services. So, many parts of the Cloud infrastructure are replicated.
- Consistency: This is a main challenge, especially eventual consistency. Strong and Weak Consistency can be distinguished (Vogel 2009). Within Strong Consistency all following accesses have the written value after a transaction. This is not guaranteed in Weak Consistency, not until a specific time interval (inconsistency window). Eventually Consistency is a special form of Weak Consistency, where inconsistency window depend on factors like load, replication nodes or reaction time of the system.
- Data Security: Data security in the Cloud is a significant issue especially for the acceptance of the Cloud service offering. Companies have to be guaranteed that their data is safe in the Cloud. To entrust their internal Data, which worth is seen as a growing value, to a Cloud service is a risk for companies. The prevention or minimization of this risk is one of the difficult challenges for Cloud Computing. As an additional problem is the provability of the data security.

Cloud Computing has still potential for future developments, but there are also a number of challenges that need to be addressed.

2.4. Use cases for Cloud Computing

Cloud Computing allows the dynamically adapted usage, based on the need of the customer, of IT resources (e.g. disc storage, computing power or even software itself) over a network. This enables companies, public services, the scientific community and consumers to scale up their potential IT resources on demand. It can also eliminate the need for big investments into their own IT infrastructure, which at most of the time is not fully used up in normal circumstances but only at peak times. The billing will be, in most cases, „pay as you go", meaning that the user needs only to pay the amount he consumed.

In the following part will be an example for each of the main Cloud Computing areas, SaaS, PaaS and IaaS. The examples will look very briefly in the offered functionalities of the Service. This is not a fully representative review, just a brief look at to show for what and how Cloud Computing can be used.

SaaS example: Dropbox
Description: The most well-known example for consumers may very well be Dropbox. It is at least the most easy to use. Dropbox enables the sharing of data across multiple computer. A user installs the software on its PC and may then use the Dropbox client the same way as a normal folder. The data, files, etc, which are put into this folder, will then be uploaded into the cloud storage system. The user may then install and use the Dropbox client on another PC and it will synchronise the content of the folder to the new PC. In addition the consumer may also use a web interface if it is not possible to install a Dropbox client on the used PC. This enables the user to access this data anywhere at any time (if it is connected to the internet). The collaboration aspect of this service is based on the possibility to create shared folders and enable multiple users to interact with the content of the shared folder. This may be used to update documents, to access information or just share pictures of your holiday with friends the moment they are uploaded.
Use case: An example for the Business usage of Dropbox is Foursquare. This company uses Dropbox to have a central file system for managing digital documents, to share data and documents in a fast way between team members and clients and to have a simple way to work on the same documents between different offices. The mirroring of the data on the computer of each user makes it possible to work on it even when they have no internet connection.

PaaS example: Google App Engine
Description: Google App Engine is a service offered by Google to develop and deploy apps on the Google cloud. It offers a platform to create and run an App without having to work on the underlying infrastructure. In its basic function it allows the user to develop an app in a supported language (at the moment 4 languages) and deploy it on the server, where it may be accessed by different users. On of the main advantages of the Google App Engine is the parallel use and development of the app; it is possible to change the

App in a very small period of time. While the App is running, it will automatically adapt the provided computing power to the needed level.
Use case: An example for the use of the Google App Engine is HUDOA. This company used the Google App Engine to deploy and use their ERP software. It used this as a PaaS to focus on the service itself, ignoring server managment packages, etc. The possibility o run a product and a test version enables them to update their system at a faster rate (months to days) and reduces the cost to develop at the same time as running the old system. The usage led to reduced shipping costs, reduced hardware and operation costs and the possibility to free the IT staff to do other tasks.[3]

IaaS example: Amazon EC2
Description: Amazon EC2 is a Service offered by Amazon. At its core it creates a virtualization of a PC and allows users to use this virtual computer to use it as if it were a physical computer. It is possible, in contrast to a PaaS, to install different software on this virtual computer. The service offered by Amazon include a very fast scaling of the service, may it be downscaling or upscaling, to boot several server in a short time and to use different operating systems on each of the different servers.
Use case: An example for Amazon EC2 is Pfizer. Pfizer uses Amazon mainly to reduce its costs. It enables them to just rent the needed computing power while needed, e.g. to perform difficult analytics. Amazon EC2 is in this scenario an addition to their IT. Pfizer used a job scheduler, which acquires additional computing power as needed. This saves in addition a lot of time and enables them to explore scientific questions in a scalable, timely manner.[4]

The examples underline that Cloud Computing is mainly used for consumer's services and normal business IT services. In the latter case there is a broad range of offers reaching from pure computing and data storage capacities up to complex business IT solutions such as business intelligence or enterprise resource planning. However there are also limits in particular in the business use of 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. In the case of consumer services software offers like tools for synchronisation, storage, foto editing are the usual services. Mostly these are used in combination with mobile devices. Beyond that there is a set of other offers such as social network sites or the streaming of video or music. Some of these services use Cloud technology, but they also use other technologies (peer to peer communication). Moreover some of them even existed before the term "Cloud". Consequently these services are not in our focus, which is also true for all kinds of traditional eCommerce services such as online retailing, online booking or similar, though there are nowadays often based on Cloud infrastructures.

[3] See https://cloud.google.com/files/Hudora.pdf.
[4] See http://aws.amazon.com/solutions/case-studies/pfizer/.

3. ADOPTION AND IMPACTS OF CLOUD COMPUTING

3.1. Overview on the current market situation

At a first glance it is no problem to find actual numbers on the current market situation of Cloud Computing at different levels, but a second and closer look reveals some difficulties related to the comparison and analysis of the available numbers.

The first challenge is related to the market segmentation. Based on a review of market reports several markets can be identified: 1. (Public) Cloud services market, which covers spending of commercial and private consumers for Cloud services offered by a third party (Cloud provider). Consequently it also covers all spending related to hybrid cloud models.; 2. The market for IT services related to Cloud Computing, which covers mainly spending of customers (end-users) for training, integration, consulting and similar services related to introduction and use of Cloud Computing; 3. The market for Cloud technology, which covers spending for technology enabling Cloud Services, i.e. hard- and software that is necessary to build up Cloud infrastructures and to offer Cloud services. As a consequence it contains spending of Cloud Service providers, but also spending of companies who buy their own private Cloud. However there are also many markets more like markets for different types of private Clouds, which appear in this model in parts in the markets for Cloud technology and related services, but it is often unclear what is counted for what. Overall there is a strong focus on business spending. The second challenge is related to the underlying methodology, i.e. the question in which market and market segment the different activities are counted. This problem can occur either within a market or between different markets. However, it can be expected that that in the next years a harmonization of the general categories between at least the bigger market researchers will take place. Finally there is the challenge of availability, which includes two dimensions. The first one is that some very detailed and interesting market research only exist in very specific and/or non-comparable datasets. The second dimension is the factual availability of such reports. Most often the market researchers only publish some sneak previews to their reports, while the full report with the detailed numbers are only available for purchase.

Against the background of these challenges we will mainly use the public available data for public Cloud services[5] as a proxy for the overall development based on the believe that the public Cloud market is the biggest market and that the others markets will grow in relation to it as it is the main driver of Cloud Computing. Nevertheless, the recent events around the different programs on tapping or accessing data might impact this situation as discussed further below.

3.1.1. Overview on existing market studies and forecasts

According to all main market researchers the market for public Cloud Computing services is, beside Big Data and Mobile Computing (Apps, etc.), the fastest growing segment in the software and IT services market. These three are expected to have a considerable impact on the market landscape as well as on the use of computers in the coming years (see for

[5] Please note that this includes citations of market research reports from different web sources. Normally we name the market research company as well as the source of the information.

example EITO 2012). Moreover these three are interrelated. For example Big Data analysis requires big data storage and computing capacities, which many companies could not afford for such purposes. Therefore Cloud Computing is an essential enabler for it. A similar, but more multifaceted relation also exists between Mobile and Cloud Computing. Vice versa Cloud Computing needs both segments as drivers and show cases of its usefulness. These three show considerable growth rates beyond the normal growth of the overall market. In total size Cloud Computing outweigh the both others.

Overall market development

The review of existing market studies shows that there is broad spectrum within the different forecasts. One reason for this are different methodologies, which in- or exclude different segments. Another one are the basic assumption like overall economic growth for different regions and similar.

Table 1: Overview on forecasts in billion US-Dollar for the development of the Public Cloud services market, Source: Gartner 2012, Gartner 2013a,b, IDC 2012, IDC 2013a, Forrester 2011 (after Dignan 2011)

	2011	2012	2013	2015	2016	2017	2020
Gartner	91,4	-	131	-	206,6	244	-
IDC	-	40,0	47,4	-	100,0	107	-
Forrester	40,7	-		97,0	113,9		241,0

The main reason for the obvious differences between Gartner on the one side and IDC and Forrester on the other 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. Though the forecasts vary in terms of absolute amounts, clearly for these reasons, there is one thing in common: All researchers forecast an annual growth rate (CAGR) beyond 20%, which shows the strong dynamic of the market. For example, IDC, which uses a Cloud definition close to the NIST definition, estimated 40 bn. $ as the size of the market for public Clouds in 2012 (IDC 2012) and a size of 47,7 bn. $ for 2013 (IDC 2013a). This underlines the expected growth rates. Due to the fact that this growth is outpacing the growth of the overall market for software and IT services all three market researchers believe that the overall share of public Cloud Computing will grew in the next years (Gartner 2012, Gartner 2013a,b, IDC 2012, IDC 2013a, Forrester (after Dignan 2011)). The actual value depends again on methodology for both, Cloud Computing as well as for the overall market. Concluding this, it can be stated that Cloud Computing will become an essential part of the overall market. This is reinforced by the fact that these forecasts do not include segments like the IT services and consulting related to Cloud Computing as well as the software licences for Cloud technology required by the Cloud service providers. Moreover this development will also impact the market for IT hardware like for example a shift within the different server segments (see for example Cattaneo 2012c). However there are some analyses that might give an impression on the size of these segments by IDC. For Cloud professional services. i.e. IT services related to Cloud Computing, IDC sees a market of 9,6 bn. $ in 2013 (IDC 2013b) and for the market of hosted private Clouds, which only covers a specific form of private Clouds, IDC expects a value of 24 bn. $ in 2016

(IDC 2013c). Though there are overlaps and methodological problems, the number clearly shows that these segments also show a considerable size as well as considerable growth rates.

While these forecasts are mainly based on an overall positive view of the further development of Cloud Computing, there are also critics who state that Cloud Computing will soon pass the peak. Typically the truth might be found somewhere in the middle, but based on the current position of development it seems hard to predict where it will be. This perception was fed during 2013 by the disclosure on the NSA Prism program and similar activities in other countries, which may lead into growing reluctance. This assumption was recently underlined by different studies for the US Cloud industries (Johnson 2013, Castro 2013). These studies show that in particular US based Cloud companies had problems due to the recent discussion on the NSA practices, because there is growing reluctance to use US Cloud providers. In some cases even projects were cancelled. Overall it is estimated that it can lead to losses up to 32 bn. $ in 2016 for the US Cloud providers[6]. However, the resulting question is if this will pose chances for non-US based providers or if customers will stop their engagement in Cloud Computing at all. All recent forecasts do not deal with this question.

Development of the different service models

Similar to the situation of the forecasts for the overall market for public Cloud services, the forecasts for the different service models segments vary in the same way. Most obvious is that the segment of Business Process as a service, which we defined as part of SaaS, varies between Gartner and Forrester extremely, while IDC does not introduce this category. This might be one reason for the huge differences in the overall market size and underlines the challenge of the different methodologies.

According to all major market researcher the market for SaaS (in our case including the different BPaaS segments if available) is the biggest one in terms of absolute value at the moment and will remain the biggest in future (Gartner 2012, Gartner 2013a,b, IDC 2012, IDC 2013a, Forrester 2011 (after Dignan 2011)). Both other segments, IaaS and PaaS will be, in absolute values, only small markets in comparison to it. Nevertheless there is tendency within all forecasts to state that both segments will grow with a higher rate than SaaS in the next years (Gartner 2012, Gartner 2013a,b, IDC 2012, IDC 2013a, Forrester 2011 (after Dignan 2011)). As one reason for this Gartner sees a growing trend of more experienced users going towards PaaS solutions in sub segments like for example Business Intelligence and Big Data, where such offers give more possibilities to adjust and customize the applications to their own needs (Gartner 2012). The trend towards SaaS is obviously a result of the current adoption and usage patterns. With a growing number of companies, in particular SME and private consumers starting to use Cloud services, it seems normal that standardised product solutions gain importance. Most of them are already used to standardized products like the Windows Office family. Moreover the flexibility of IaaS or PaaS also requires more knowledge on the basics of the technology, in particular it also requires more time for implementation and continuously administration. Therefore it is not a surprise that consumers and SME are not attracted by such offers. On the other hand this

[6] The estimation is based on the Gartner forecast of 2012.

flexibility is, as already indicated, one reason why bigger companies may develop a tendency towards such solutions. They have the financial and human resource capabilities to afford it.

Table 2: Overview on forecasts in billion US Dollar for the development of the Public Cloud services market by segments, Source: Gartner 2012, Forrester 2011 (after Dignan 2011)

	2011				2016			
	IaaS	PaaS	SaaS	BPaaS	IaaS	PaaS	SaaS	BPaaS
Gartner[7]	4,27	0,9	11,88	71,94	24,44	2,92	26,55	144,74
Forrester	2,94	0,82	21,21	0,53	5,65	11,26	92,75	4,28

Within the different segments of Cloud services all forecasts are seeing a clear trend towards more diversity regarding the type of services offered as well as the distribution between the different sub segments. The growing number of services, which will be also outlined in the following overview on existing services, is a result of the growing number of bigger and smaller suppliers that started in the recent years to migrate their offers into Cloud solutions. Additionally, the growing experience also led to the trend to migrate more and more complex applications like enterprise resource planning (ERP) as well as complete business process into Cloud services. Finally there is also a growing number of completely new offers that are enabled by the existence of other Cloud services, i.e. services combine different Cloud services to new offers. As a consequence of this development the distribution of revenues also starts to change. While in the early phase few applications like customer relationship management in the SaaS segment were dominating, the existence of more and more advanced services lead together with more experienced users to a trend towards other services like ERP or BI solutions. Other examples are the early dominance of computing and storage services in the IaaS segment, which are now complemented by more advanced backup services, or the tendency of offering more types of PaaS services for specific purposes beyond development platforms that can be adjusted to user needs.

Regional development of Cloud Computing

Regarding the regional development it is not surprisingly that North America, in particular the U.S., are the biggest market for Cloud Computing at the moment. According to all forecasts it will show in terms of absolute value the greatest growth. However in terms of growth rate emerging markets like China or India are seen as the coming markets. Europe is at the moment the second biggest market behind the US and followed by Japan and the other more mature Asian markets (Gartner 2012, Gartner 2013a, IDC (cited after Bloomberg 2012). Consequently Gartner (2012, 2013a) as well as IDC (Bloomberg 2012) indicate the possibility that this fast growth of the emerging markets can lead to outpace Europe in the long run. The strong growth in emerging countries is not really surprisingly. One prominent reason is that most companies and organisations in these countries do not have a strong and long time grown IT infrastructure. As a consequence the migration to new approaches with clear benefits does not require the same efforts as in other areas. As reasons for the slow growth in Europe at least two points were named: Firstly, the lower adoption rate in general caused by a greater reluctance against Cloud Computing, and

[7] Please note the difference to the overall forecasts of Gartner results from the additional category Cloud Management and Security services (2011: 2,39; 2016: 7,94), which was not included in this overview.

secondly, by the economic crisis of the Euro zone. The first argument clearly relates to the development of adoption and usage patterns (see 3.2). There it is clearly shown trend that in the US consumers as well as businesses, in particular SME, adopt Cloud Computing earlier and faster than in Europe. A positive development is that the adoption/usage and, as a consequence the market, in Europe gained a stronger momentum in the recent time. This is underlined by the regional forecasts of PAC for Europe (Fielder et al. 2012, 20). Nevertheless this forecasts also shows a surprisingly strong position of the IaaS segment in Europe (including storage solutions), which is bigger than the SaaS segment. This could be an indication that European companies have a stronger tendency towards solutions with a better control of the whole system. This could also imply that there is a stronger tendency towards private Cloud solutions in Europe as in the US. Based on the available data it is not possible to conclude this and it remains an open question.

3.1.2. Cloud Computing services and providers

Due to the fact that Cloud Computing is an evolving technology and market, it is not possible to deliver an exhaustive overview on offered services or providers. However, within the different market segments of Cloud technology, IaaS, PaaS, SaaS and Cloud related IT services, some trends and players can be identified.

Overview on Cloud services

Overall, there is growing number of **Cloud technology**, in particular software solutions for the management of Cloud systems in different variations. This encompasses No-SQL databases (e.g. Couch DB), virtualisation software (eg.. VM Ware), distributed caching (e.g. Oracle Coherence), infrastructure management (e.g. Open Stack) and integration solutions (e.g. Cloudswitch). Underneath there is tendency to use Open Source solutions like Open Stack or Open Nebula, which are supported by main suppliers like IBM or Google. There is also a growing market for underlying hardware, which is most likely a sub segment of the data centre hardware market dominated by companies like IBM, Dell, HP, Huawei, Cisco and others. As some of them are also suppliers of the Cloud Computing technology and services, they are able to offer fully integrated services to their customers. Another trend supporting this development is the growing number of solutions for modular data centre server platform combining server hardware, switches, management, and virtualisation software in a bundle.

Typical offers within **Infrastructure as a Service (IaaS)** are computing infrastructure (e.g. Amazon EC2), storage infrastructure (e.g. Rackspace Cloud Files) backup infrastructure (e.g IBM Smart Cloud Managed Backup) or brokerage infrastructure (e.g Gravitant). Additionally also load balancing, content delivery infrastructure (e.g Amazon CloudFront) or management infrastructure (e.g. Amazon Cloud Watch) are offered as IaaS services. In some cases there is a more detailed differentiation for example in the segment of computing infrastructure between solutions for provisioning physical hardware (servers) and virtual machines. One point is that in all categories solutions can be found that in principle can be used for the provision of public or private IaaS services, which are often less known as the offers of the big public service providers like Amazon or Google. Finally there is a tendency to comprise several IaaS services into packages and sell them under a specific label like Amazon Cloud Formation, HP Cloud or Rackspace Cloud.

Typical **Platform as a Service (PaaS)** offers can be differentiated into four types: general purpose platforms (e.g. Microsoft Azure Platform); development platforms (e.g. IBM Rational Software Services); database platforms (e.g. Amazon Dynamo DB); and integration platforms (e.g. Informatica Cloud). One recent trend in this segment are Business Intelligence Platforms that provide collections of tools for analysing different types of data from normal business data to big data collections. But due to the different types of offers for it ranging from ready to use solutions to custom made analysis the borderline to SaaS is blurry. It should be also remarked that like in the case of IaaS some of the named examples are suitable to be used for both, public or private Clouds.

The segment of **Software as a Service (SaaS)** offers a broad variety of services similar to the normal application landscape. Typical examples are customer relation management (CRM) (e.g. Salesforce CRM), enterprise resource planning (ERP) (e.g. SAP by Design), business intelligence (e.g. Datameer), collaboration tools (e.g. Jive Social Business Software, supply chain management (SCM) (e.g. Aravo) or human resources management (e.g. Workday). However, this is only a selection, not an exhaustive view. Many others categories like Cloud Advertising and Payments, e-Commerce services or industry operations could be easily added. As already indicated there exists the trend to more complex applications, which led to the tendency to create a new segment called Business process as a Service (BPaaS). It is obvious that most market researchers strongly focus on the business market and neglect markets for private applications based on Cloud Computing. One reason might be that in many cases of cloud based solutions for consumers the borderline to the other markets, in particular the one for mobile apps, is hard to draw. Another one might be that this market is less driven by direct purchases, but by revenue models based on advertising or other methods like the in-app purchases of extra goods. Finally there is also an uncertainty if applications like Cloud gaming will succeed at all. Therefore this remains an unsolved challenge for the future years.

Cloud related IT services are services related to introduction and use of Cloud Computing services, mainly for businesses as users. Typical examples are: **Selection & Decision**, i.e. the support to decide on the use of Cloud Computing in a company as well as the support to identify and select the suitable provider; **Training**, i.e. training of end-users and management of the company in the right and efficient use of Cloud services; **Implementation**, i.e. support for the factual installation and operation of a Cloud service, either public, private or hybrid models; **Integration**, i.e. support for the integration of a Cloud service into the existing IT landscape of a company. There are other services or combinations possible dependent on the demand of the market. Similar to it, the suppliers of such services also offers a great variety. One group consists of big Cloud suppliers like IBM and HP, which have their own service business units offering these services for their own products, but partially also to other suppliers. Another group is composed of big IT services companies like Accenture, CapGemini or Atos that offer the full range of services from implementation and operation of private and public Clouds to all other services related to Cloud Computing. Finally there is the great majority of small and medium sized IT services companies, which also offer, depended on their capabilities, different types of services related to Cloud Computing

Overview on Cloud service providers

Though the number of providers for Cloud services is still increasing with a high rate, the list starts to shrink drastically if you take into account the size and impact. Moreover the remaining companies sound familiar to the IT and Internet community. They can be characterized according to the time they entered the market.

The first group encompasses companies like Amazon, Google or Salesforce. They entered the market as early movers; some even say that Amazon has created this market. Although Amazon main business is e-Commerce, it was a logical decision to improve the utilisation of their massive resources, which are needed for their main business, all over the world. Google on the other hand is primarily a search engine, but with its move into advertising it already started to use technologies, which are now considered to be typical for Cloud Computing. In contrast to this Salesforce, founded in 1999, started as a company for Application Service Providing (ASP). After a long phase of suffering especially its CRM SaaS offer became more and more a success in the middle of the 2000s. Later on Salesforce managed to access new fields and keep pace with its competitors.

The second group, which consist of companies like VMWare, Citrix,Terremark or Rackspace, started as specialists for technologies or infrastructures building the foundations of Cloud Computing such as virtualisation or data center operations. Nowadays they deliver important parts of the Cloud technologies and software, e.g. OpenStack, virtualisation tools, e.g. Zen, and similar. Additionally they also started their own public Cloud offers. Beside this, this segment is also an example of the high dynamic in Cloud Computing in terms of mergers and acquisitions. Citrix and Rackspace bought in recent years many small providers and technology specialists like Xen (Citrix) or JungleDisk (Rackspace). Despite this VMWare and Terremark became themselves targets. EMC bought VMWare already in 2004 and recently Terremark was taken over by Verizon.

A third group consist mainly of the great worldwide active IT services provider and hardware producers like IBM, HP, Dell or Cisco. They were soon followed by more regional IT service providers and national telecommunications providers like T-Systems/Deutsche Telekom, BT, Fujitsu Technology Solutions or Atos. On the one hand nearly all were capable to develop or purchase solutions and on the other hand they also had a strong customer base and many alliances with other existing IT companies. Consequently many of them became full service providers from Infrastructure to specific services, most likely they offered it in a first step to their customer base as private Cloud solutions, but some soon started also to offer massive public Cloud offers like HP or Dell. A subgroup of them are the software product companies like Microsoft, SAP or Oracle. Their common characteristic is that they started to talk about Cloud Computing, but that their own offers appeared quite late at the market for different reasons. Therefore they can be considered as the markets latecomer. This trail is nowadays followed by many smaller and medium sized companies like IT service providers or specialised software product suppliers, which now also move their business into the Cloud Thereby they often rely on services of one or more of the big suppliers.

Finally there is the group of "Cloud born" companies, i.e. companies with service offers only created for Cloud use and based on Cloud Computing services of other suppliers. These appeared soon after the start of Amazon Web Services. They started to gain attention with the boom of mobile platforms enabling different kind of apps as well as the need for synchronisation and similar features. In difference to before mentioned groups they also target consumers as customers and thereby spread the concept of Cloud Computing beyond the specialists discussions. Although this market is smaller, it led to a push for Cloud Computing in business. Because of the trend that many consumer started to use their smart phones and tablets also at work (bring/buy your own device - BYOD) and thereby introducing Cloud Computing solutions into their companies many companies were forced to deal with it. The most prominent example for this is Dropbox, which started in 2008 as a synchronisation and file sharing service based on freemium revenue model. In a short term the service became very popular and attracted millions of user. Moreover their use led to the fact that Dropbox grew beyond a file storage service and became more and more a collaboration service (Barret 2011). Although most users only use the space freely available, Dropbox generated 240 Mio. in revenues in 2011 and is now one of the most valuable start-ups in the Silicon Valley.

Though the market is still evolving, some points are obvious. The first point is that only a number of companies like Google, Amazon or IBM will be able to act as full-scale providers. This is a consequence of the enormous investments needed for the Cloud Computing infrastructure. But new models like the brokerage approach of Zymory and others like Spotcloud enable smaller data centres to offer their unused capacities. If successful, this could create a counterpart to the big players mainly offering their own resources. However this is only one example for the fluid state of the technology and market. It shows what kind of consequences could evolve from the different developments of them and how difficult it can be to assess them. It clearly refers to the open questions posed already before: What are the dominant revenue models; which new services will evolve after the transformation of the existing ones into the cloud, and finally which new business model will result out of it, to name a few. The second point what nearly all of these companies have in common is the fact that most of them do not publish the revenues of their Cloud services. In case of companies like Amazon, Google, Microsoft or IBM it is therefore nearly impossible to specify the percentage of their overall revenue origin from Cloud Computing. In some cases estimations by market researchers are available, which clearly shows that the percentage of the overall revenues in case of these companies is little (below few percent). Nevertheless these few percent still amount for a total value of round about 2 bn. $ in the case of Amazon (Babcock 2013). The different offers of Microsoft, in particular Microsoft Azure (PaaS) are estimated to generate annual revenues of $ 1 bn (2012/2013; Bloomberg 2013). More or less all of these companies announced plans or strategic visions that in the next few years Cloud services will become an important part of their business. IBM, for example, announced a targeted revenue from Cloud in 2015 of 7bn $ (Kelly, 2011). In contrast to this the revenues of specialist companies like Rackspace or Salesforce give a more detailed insight. Salesforce revenue in 2012 was round about 2,2 Bn. $, of which most, but not all is related to Cloud Computing (Streetinsider 2013). Although the revenue grew fast in the last years, Salesforce closed nearly all years with small or bigger losses (Henschen 2012). In case of Rackspace analysts estimate that Rackspace out of the

total revenue of 1,2 bn. $ 300 mio. $ were related to Cloud Computing (O´Gara 2012). However, there is also a great number of small and medium sized companies offering Cloud services. According to a recent survey by KPMG (2013a) with over 170 Cloud service providers worldwide there is clear trend towards a growing share of Cloud related business. At the moment the average share of revenues is 26%, they expect a raise up to 50% in the next three years. Finally most of the cloud born start-ups do not name details on their revenues. If information is available, they do not specify how these revenues are composed, i.e. how big the shares of user payments or advertisement revenues are. An exception is Dropbox. According to public information it reached revenues of 240 Mio. $ in 2011, though its main business model is a freemium service where more than 90% of the user only use the freely available services (Barret 2011).

From a European point of view one point is that at the moment most of these companies have their headquarters in the US, while only a few European players appear as global players in this field, offering their services outside of Europe. Another point is that not all of the American companies have located data centres in Europe, although Europe is for now the second biggest market. In case they have data centres located in Europe, there is a clear tendency towards a small set of countries for several reasons. Most prominent example is Ireland, where beside the low level of data protection rules in an European comparison also other reasons such as taxation regulations play a prominent role for the question where to place the European headquarter. Overall this situation is a mirror picture of the past decades, where mostly US-based companies dominate the markets and using a set of specific locations for the entry of the European Market (OECD 2013). If this will change in the future depends strongly on both, the overall development of Cloud Computing as well as the development of the legal, social and economic environment and is therefore as hard to predict as the rest.

3.2. Adoption and usage patterns of Cloud Computing

Similar to the numbers on the market development there exist many studies dealing with adoption and usage patterns of different types of user. These studies have the problem that they were made mainly by consultants and market researchers for specific purposes. Consequently the methodological quality of these surveys differs strongly. The data base is also often quite small, in many surveys lower than 100 respondents. Both, the low degree of representativeness as well as the quality differences, limits the usability of their analysis. One exception is a study commissioned by DG Connect, which was carried out by IDC between 2011 and 2012. In this case representative samples of round about 1000 companies and the same number of consumers in Europe were asked about their patterns. Therefore the analysis is mainly based on this study. It will be compared with available data from the US and other countries as available data permits. Though these data are latest from 2012, it should be marked that more recent surveys focus more on patterns and best practices of adoption instead adoption levels (e.g. KPMG 2013b).

3.2.1. Adoption and usage by business users

The survey for companies addressed companies of seven main sectors (finance, manufacturing, distribution, healthcare/education, government, telecoms, and other services) in nine countries of the European Union (Czech, Republic, France, Germany, Italy,

Poland, Hungary, Spain, Sweden, UK). In total 1056 companies responded. In a first overview 64% of respondents used Cloud Computing and only 36% did not. A more differentiated look shows the details:

Table 3: Adoption of Cloud Computing by European business users, Source: Cattaneo et al. 2012b, 16

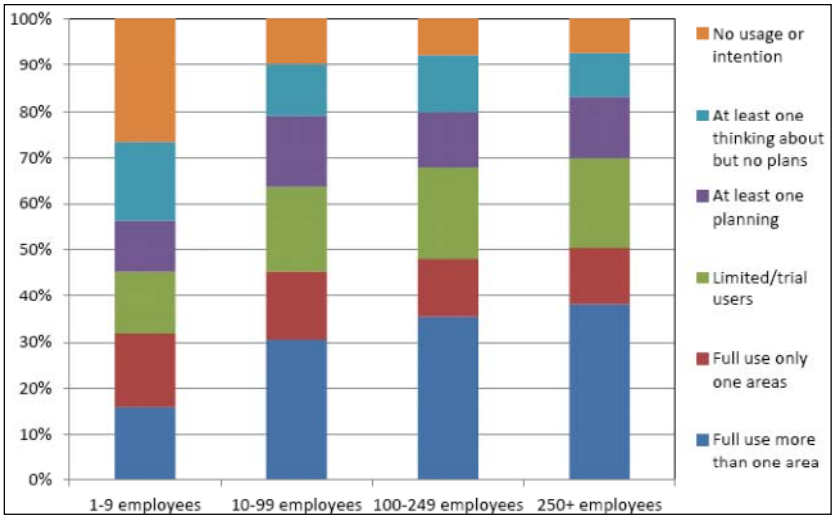
	Type	**Description**
11%	No usage	No usage/intention at all
12%	Thinking	Considering the usage, but no actual plans
13%	Planning	Evaluating or planning to use one or more areas
19%	Limited use	Limited or trial use of one or more areas
13%	Full use one area	Full use of Cloud services in one area
32%	Full use more areas	Full use of Cloud services in more than one area

Overall the results shows that there is already strong group of companies (45%, dark-grey) currently using Cloud services (users in the following), i.e. they already adopted Cloud services and use it in one or more areas. The second group, which either evaluate/plan or make trial/limited use (tester in the following), also amounts for 32% of the companies. Finally the group of companies, who only thinks about or has no plans/intentions (latecomer in the following), amounts for 23%. Moreover further results of the study show that most enterprises (more than 50%) started the adoption in the last two years before the survey (Cattaneo et al. 2012b, 20). Overall it seems that Cloud Computing is already present in some forms in European companies, but that the situation varies. In comparison to that the situation in the US shows some differences. According to a study of the Cloud Industry Forum (Cloud Industry Forum 2012) with 400 respondents from all sectors (including public sectors as in the IDC study) already 76% of the American companies use at least one or more Cloud services. Both surveys were done at roughly the same time (November/December 2011 and January 2012), so this cannot explain the difference in the adoption pattern. One point of uncertainty is the question to which extent limited/trial usages were counted in the survey for the US, but even taken into consideration Europe remains at a difference of 12%. A more recent survey of NTT Security among 700 IT decision makers (companies with 500+ employees) in ten countries all over the world underlines the gap between the US and Europe (BusinessWire 2013).

Looking at the adoption patterns by the size classes of European enterprises reveals a clear picture. The bigger companies are more likely to use or test Cloud services. Although this result is no surprise, there are some differences to the US. According to the study of the Cloud Industry Forum (2012), but also others like SpiceWorks (2012), the adoption in the class of enterprises up to 100 employees seems to be higher than the one in the next class with up to 1000 employees, which would be different as trend than in Europe. However, due to the different size classes it is hard to derive further differences, but it seems that in contrast to Europe in particular SME embrace Cloud services in the US. Comparing the adoption patterns in the different industry sectors does not reveal big differences. The

adoption level varies roughly between 41% (healthcare/education)and 54% (distribution). Due to the lack of data it is not possible to compare this to the US. Regarding the different countries in Europe there is no clear statement possible. The results show that the level of companies currently using Cloud services vary between 30% (Czech Republic) to 60% (Poland). It is neither possible to differentiate them along geographical location (east, west, north, south) nor size (big, medium, small) (Cattaneo et al 2012b, 18). Therefore it suggests itself that there are other reasons for this difference in Europe, which cannot be clearly resolved with the available data.[8]

Figure 2: Adoption of Cloud services in Europe by business size, Source: Cattaneo et al. 2012b, 21



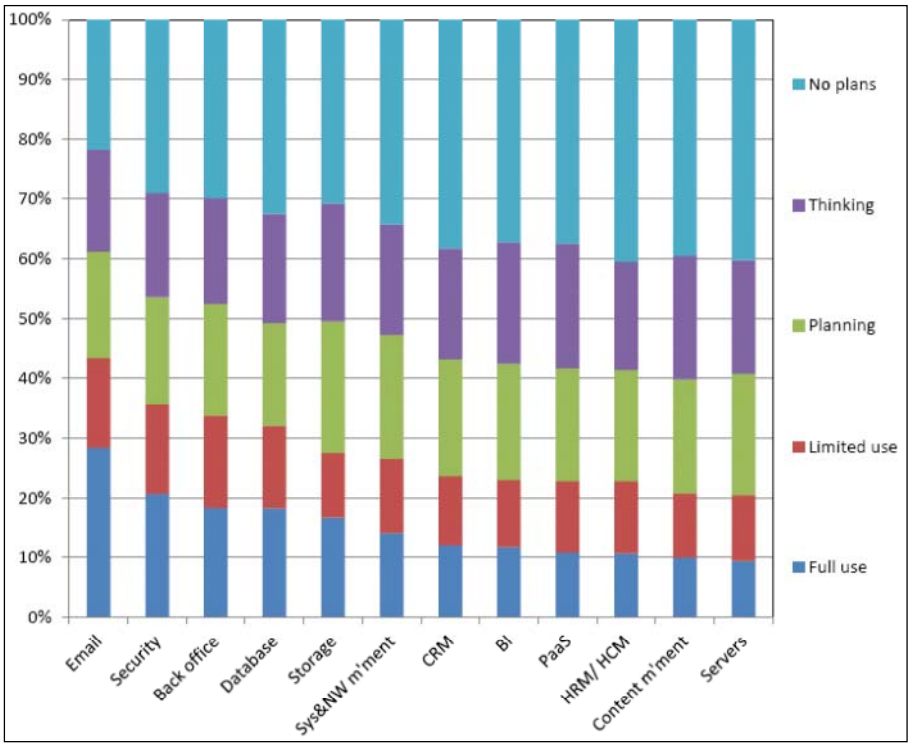
At a first glance the results regarding usages patterns does not provide any big surprises. Most companies use Cloud services for simple purposes like email, which encompasses mail services like Gmail or MS Exchange, or security. A little surprise is that these are already followed by the section of BackOffice, which encompasses a broad range of services ranging from procurement platforms and accounting solutions to full-scale ERP solutions. This is followed by the segments of database and storage also encompassing a great variety of services. However it is no surprise that HR (Human Resources) and servers are at the bottom of the group. While the direct use of computing capacities requires some technical knowledge, the HR is very critical due to its personal data (Cattaneo 2012b, 14). Based on that we can conclude that in particular simple services are already used as Cloud services, but that there is tendency to move on now towards more complex and partly critical services. In general the same statement seems to be valid for the adoption in the US. Although the definitions are not the same, the study of SpiceWorks (2012) indicates the same trends for the US.

These results confirm what was already outlined in the section on markets in different regions, in particular that Europe is lagging behind in the adoption of Cloud services. A surprise is that particular SME in the US adopting faster than their European counterparts, which is also one explanation for the big differences in terms of market size; SME are the majority of European enterprises. In terms of maturity, i.e. the extent of usage of more

[8] The survey of ENISA among European companies, in particular SME, unfortunately also does not reveal more insights (ENISA 2009)

complex Cloud services, it is hard to say how big this difference is at all. Gartner (2012) claims that Europe is lagging behind the US at least for two years, but others fear that this lag is even bigger (Borja 2012).

Figure 3: Usage patterns of Cloud services in Europe by different types of services, Source: Cattaneo et al. 2012b, 14



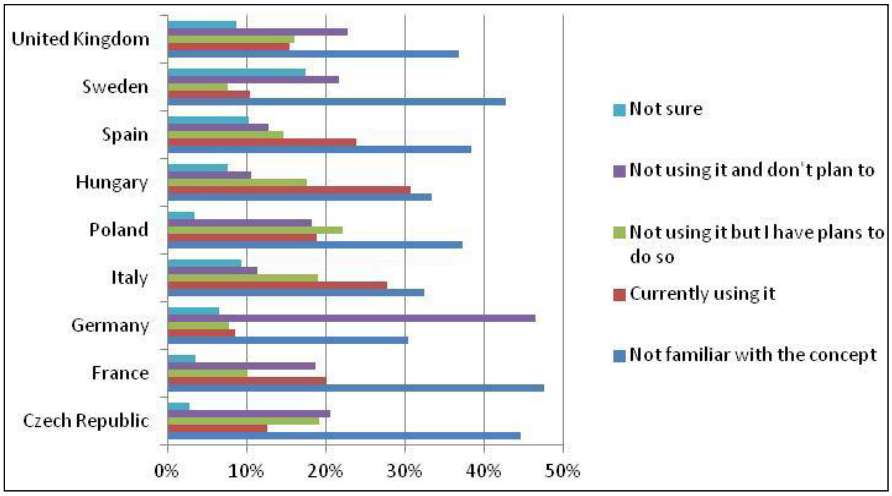
3.2.2. Adoption and usage by consumers

The comparison of different studies on the adoption and usage of Cloud services by consumers reveals that the already discussed problem of defining Cloud Computing is even more problematic in this environment. In opposite to the business segment the answer to the question what consumer Cloud services are varies strongly. Examples for this problem are question if activities like the usage of online portal for an online search or social networks are already Cloud services for consumers. From the studies it seems that in European surveys the definition is broader than the one in US surveys. Therefore a direct comparison of data is only possible to a very limited extent and requires a reflection of this problem during the analysis.

The survey of IDC, which is based on nearly 1000 consumer respondents from nine EU Member states, clearly shows that there is some variation regarding the usage of Cloud services in between these countries. While in Germany less than 10% of the respondents stated that they are currently using it, the number in Hungary is above 30%. At a first look this variation cannot be explained by the typical patterns like the geographical location of country, its size or its level of economic performance. Therefore other factors seem to be more helpful to explain this variety. One possible explanation might be the attitude towards privacy and data protection. The latest Eurobarometer on this topic (TNS 2011) shows that this can only explain a little bit, but not all results. For example the level of trust in case of data protection to Internet companies is in both countries, Czech Republic (25%) and

Hungary (23%) above the European average (22%), but the adoption varies strongly between them. Moreover in Sweden already 26% trust internet companies, but the adoption is the second lowest behind Germany (TNS 2011, 137-145). Also we can vary this with other results from the Eurobarometer, but overall it shows that there are some helpful indications, but no full explanation. One reason might be that number of respondents per countries is at the lower limit of representativeness. Another point is that parts of the respondents were maybe not aware that they in fact used Cloud services, because a look at the number of persons who used online storage (upload and store of content) in the picture below it shows that more people used such services, which are most likely Cloud based services. Consequently the results should not be taken as fixed statements.

Figure 4: Familiarity of consumers with the concept of Cloud Computing in selected European countries, Source: Cattaneo et al. 2012b, 55



With regard to the usage patterns the IDC report shows two main points. The first point is that services like information search, streaming or blogging, where people only disclosure some information as they like are used by nearly all respondents. In opposite to this people are less willing to store their content/data online. Only one exception from this trend is the use of social networks, but as stated before there is the question if some of these activities are really Cloud services. However some of the numbers for services suggest that in Europe more people then shown by the first picture are using some kind of Cloud services. Nevertheless it is not possible to conclude final numbers out of the information available. The second point is that it is obvious that people are less willing to pay for the same services. As shown by the different results for nearly all services only few people are willing to pay for services as long as these are also freely available. Nevertheless this is an interesting result, because while the services are free of charge people pay a different price: Advertising. Even in some case individual usage patterns are used for target advertising, which means that much more personal information are disclosed then maybe in case of a paid services. The difference is smallest in particular in the segments of streaming offers for music, videos or other multimedia content. Overall these results are not really surprisingly and confirm at least in parts existing perceptions of adoption and usage patterns.

Figure 5: Usage of free consumer Cloud services by types of services in selected European countries, Source: Cattaneo et al. 2012b, 51

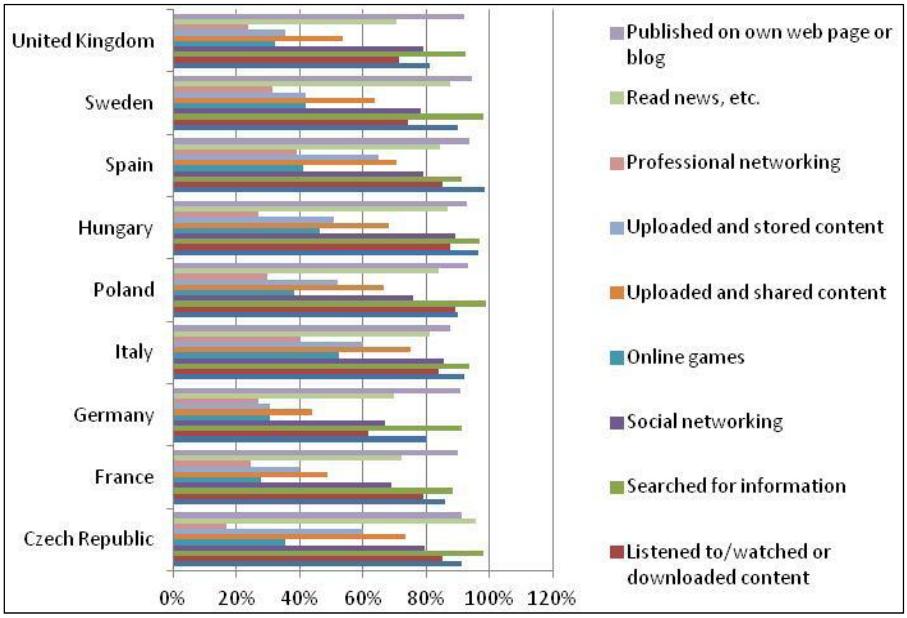
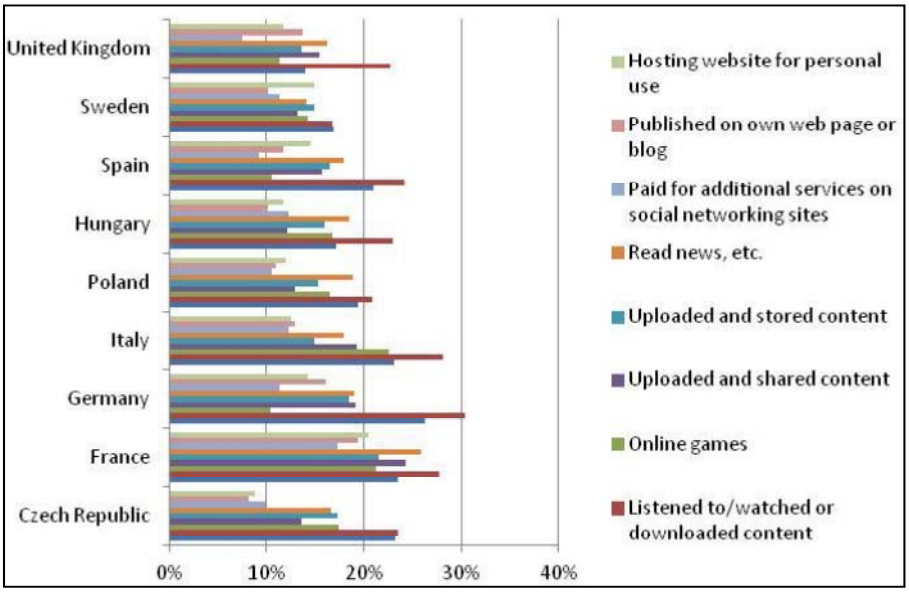


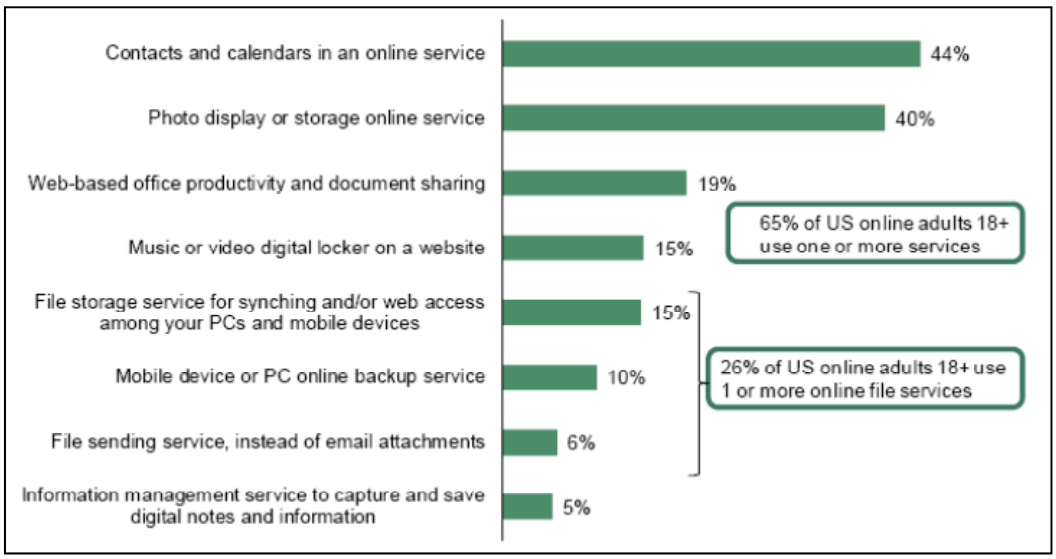
Figure 6: Usage of paid consumer Cloud services by types of services in selected European countries, Source: Cattaneo et al. 2012b, 52



Also, not surprisingly, studies for the US seem to indicate the same pattern regarding payment as in Europe. A study carried out by PwC in 2012 showed that any types of fees would clearly affect the usage of Cloud services, in case of the study the usage of a digital locker for multimedia content (PwC 2012, 12). Regarding the overall adoption and usage it is hard to make comparisons, due to the fact that the question and therefore types of services in focus are not comparable. In recent studies like the one by Forrester (2012), which was commissioned by Cloud service provider, the focus is in a narrow sense much more focused on typical Cloud services like online calendars, storage or streaming. Overall this study of Forrester among more than 2000 consumers concludes that nearly two-third of the US consumers use one or more Cloud services. According to the study services like

online schedules, storage of photos and with a clear distinction collaboration tools are the services mostly used. Based on that it is not possible to judge on the degree of personal information involved, but it seems also obvious that at least the online storage of data and personal documents is also not as widespread as other services (Forrester 2012, 6-8).

Figure 7: Usage of consumer Cloud services by types of services in the United States, Source: Forrester 2012, 7



Overall the results show that the adoption and usage by consumer does not really lag behind the adoption in business. Some articles even state that the number of early adopters in the consumer segment was higher than in business (Schofield 2012; Layo 2012). This also reflects that many companies were forced to deal with Cloud Computing because employees used services on their own devices for work. This trend, called consumerization of IT, is expected to continue as the recent hype around the BYOD (Bring/buy your device) shows (Trend Micro 2012).The underlying belief is that people want to use the full scale of devices like notebooks, smart phones and tablets. Moreover, the borders between private and business use is becoming more and more blurred. Consequently Gartner already forecasts that the personal Cloud, which will consist of a mix of private and business devices using different kinds of Cloud services for work and life purposes, will replace the old PC in the coming years. It is obvious that this new mobility will strongly impact usage patterns in the next decade (Schofield 2012; Layo 2012).

3.2.3. Adoption and usage by governments

As already indicated in the previous section on adoption and usage patterns in business, the survey of IDC (Cattaneo 2012b, 19) as well as the one of the Cloud Industry Forum (2012, 3-5) both included government and public services in their general survey. The IDC survey for Europe expresses that government and public service reaches average values of adoption and usage about ~42% of users or respectively ~63% if limited use is counted as well. The survey for the US states that 63% of public services already have adopted and use one or more Cloud services. Although it seems from this first view that with respect to public services and administrations Europe is at the same level as the US, but a report by KMPG (2012) on the adoption in ten countries worldwide shows that there are considerable

differences in the way how it is done. Therefore it seems helpful to review the public activities to determine if there are differences and to what extent. From the point of this study, there are two points most relevant: First, which type of Cloud models are used (public, hybrid, private), and second for what purpose, i.e. for internal use of services or also for purposes like e-Government/-Administration, communication or other public services like health records etc (KMPG 2012, 21-26).

On the level of the EU member states the picture varies strongly, but it seems hard to detect clear patterns. For example the survey of KMPG (2012) encompassed five member states (Italy, Spain, Denmark, Netherlands, UK) and the comparison of them shows strong differences towards the question to which extent the countries are expected to implement Cloud computing in public services. Regarding this Italy and Denmark are leaders towards a full implementation of it, while in the other countries the tendency at the moment is more towards testing or setting up partial implementations. Possible factors influencing this development could be size of the country, degree of centralisation (central vs. federal structures), interest in cost savings, but also many others (KMPG 2012, 21-26). In the case of Denmark due to the structure of the national identity system (called CPR) a strong centralised system already existed, where records from the public registration system, national health services or tax system and others were stored centrally (Friedewald et al. 2008). Therefore it seems the move into the Cloud was small, but additionally the official documentations of the Agency for Digitisation show that there are many initiatives on-going on different levels like the transition of the central platform for companies to submit invoices to the state (NemHandel) into a public Cloud service[9] as well the development of a national strategy for Cloud Computing. However, there seem to be no plans for a central Cloud of the public services.[10] In opposite to that, the British National Strategy implemented a national Cloud platform called "G-Cloud", which is a platform for all public services in Great Britain. One key element is to set up a kind of an open marketplace displaying services that can be procured, used, reviewed and reused across the public sector. The major aim of the program is to reduce costs of public services through centralisation of infrastructures and the reuse of programs and apps. The program is the central pillar of the government's Cloud Computing Strategy and supports the overall ICT strategy for Great Britain by inter alia setting standards, creating lead users in order to enable the British ICT industry and supporting industry the take up of Cloud services in private business.[11]

Comparable, but with a much broader focus, the French government announced the "Andromedé" Cloud. On a first look it is a combination of a R&D support program and a national Cloud platform, enabling the secure and data protection compliant use of Cloud Computing. In opposite to the British program this platform is not only directed at public services, but also at companies. Therefore it is led by an industry consortium, but the French state keeps a control stock of more than 30% (Auffray 2012). However, after some troubles, it was announced that the program is now split into two consortia, one led by

[9] See http://digitaliser.dk/resource/567373.

[10] See http://www.digst.dk/Arkitektur-og-standarder/Cloud-computing.

[11] See http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf.

Orange and Thales and another one led by SFR and Bull. In both projects the French government will invest the same amount of money. Above that there are only few information about the actual usage of Cloud Computing on different levels of the French public services available. In opposite the situation in Germany is much more diverse. On the national level the Federal Ministry of Economics and Technology is funding the R&D support program "Trusted Cloud". It is aimed at developing applications for the use in public services or private companies, in particular in small and medium sized enterprises (SME). Consequently the program is organised into four pillars: Basis technologies, industrial applications, applications for the health system and applications for the public sector.[12] Above that level there is ongoing discussion that the Ministry for Interior plans to implement a national German Cloud that is similar to France directed at the public services as well as companies in Germany (Kalenda/Pößneck 2011) Nevertheless there are also a number of Cloud activities on the state level in Germany, but most of these activities are aimed at private clouds, which should help to reduce costs and improve service quality.[13]

If looking at the European level there is a lack of information about if and how European administrations and organisations use Cloud services. Only the project leaflets of the 7th FP indicate several activities in the area of scientific organisations including also European organisations. However, there no further information to find about European administrations use of Cloud Computing. In contrast to this, there are many activities on the political level. In particular the European Commission has launched several activies in the course of their Cloud Computing Strategy, which is a central pillar of the Digital Agenda (COM 2010/245/EC). The key document of it is the communication on "Unleashing the potential of Cloud Computing in Europe" (COM 2012/529/EC), which was adopted in September 2012. It describes the main challenges and necessary activities from the point of view of the Commission. At the moment the European Parliament is working towards a resolution on it (Castillo Vera 2013a). Several actions named in the communication are already on their way. Most recently the "Cloud for Europe" project started, which is an important part of the European Cloud Partnership. It is aimed at identifying obstacles for the use of Cloud Computing in public services and address them by the initiation of innovative procurement processes (Strickler 2013). Moreover these instruments also play an important role in the recently adopted ICT research program of Horizon 2020 program. Overall, these activities show that recently the use of Cloud in public services is now becoming a central point. However, there is the question how the activities on the European and member state level can be coordinated to fully exploit their potential.

In the US the "Federal Cloud Computing Strategy" was adopted in February 2011. It is based on a long-term process that started already in 2008, when, as mentioned before, the National Institute of Standards and Technology (NIST) begun a process to define Cloud Computing. Central element is the introduction of a "Cloud first policy" requiring that public services have to give priority to Cloud as the first alternative for new IT systems.[14] This Cloud first policy went into effect in 2012, but already the US government started several

[12] See http://www.trusted-cloud.de/documents/01_Goerdeler_BMWi.pdf.

[13] See http://www.kommune21.de/meldung_13367_Kommunen+auf+dem+Weg.html.

[14] See http://www.cio.gov/documents/Federal-Cloud-COmputing-Strategy.pdf.

initiatives before. In a first step the General Service Agency (GSA), that provides central services for the federal and local governments in the US, moved in 2009 the general information portal for citizens USA.gov into a third party hosted infrastructure. The aim was to improve the service quality (number and length of down times) while reducing the operational costs. Initially it used a public IaaS offer from Terremark, but the GSA decided to move USA.gov portal and the datat.gov portal, which is the central portal for the Open Data strategy, to the public IaaS environment of CGI. Meanwhile other federal ministries and agencies also started to move their portals into other public Cloud services (Montalbano 2012). The other central project of the GSA was the establishment of apps.gov, which should be a storefront for cloud solutions for all federal and local public services (ministries, agencies, etc.). In principle it is based on a flexible IaaS environment and offers users the chance to search for existing solutions. However, the GSA shut down Apps.gov in December 2012. Officially the GSA stated the need to further develop their offers for customers as the reason for this step, but in recent time there was some critic on the platform stating that it was a political project not backed and taken up by its userbase (Weigelt 2012). Nevertheless it worked well as a flagship and speed up the process of Cloud Computing in public services in the US. Consequently there are a set of other projects ongoing like the Department of Health and Human Services use of Salesforce CRM solution for their regional centres as well as the use of Salesforce at the Census Bureau (Violino 2011; Wyld 2010). Another example is the engagement of NASA in the development of the Nebula project, which turned into an open source technology for Cloud Computing (Wyld 2010).

Overall this illustrates three points about Cloud Computing for public services in Europe and its differences to the US. First, the situation in Europe is quite diverse and foremost driven by national initiatives. Only recently first steps towards a coordination started at the EU level. Second, most of these activities are still at an early stage. Finally, the national programs and strategies are more often aimed at great national clouds that are also aimed at companies and not only public services. They are often seen as a key stone to enhance the national IT industry competitiveness. Although the latter point may be no official intention of the current US strategy, it is seen at least as a side effect of it (Higgins 2012). In most other parts the US approach differs clearly from the ones in Europe. One point is that as an early adopter some of the projects of the federal government already achieved a stable status. Another point is that the US tends to use public Cloud services already offered, while some of the EU member states prefer to develop their own Cloud platforms, mostly in cooperation with national IT service providers. In this respect these countries are comparable to Japan, where the Kasumigaseki Cloud represents also a national Cloud platform for public services (Wyld 2010). Due to the fact that this will take time to develop and implement, most states virtualizes their existing data centres into private Clouds in the meantime to profit from cost reductions.

3.3. Identification and assessment of barriers and drivers

In order to determine the challenges for Cloud Computing in Europe that needs to be addressed, the first step was an initial identification of barriers and drivers. It served two purposes: Firstly, it supported the identification of impacts, positive as well as negative ones; secondly, it helped to determine the importance of them. Together with the results of

the impact analysis this was a major input for the selection of challenges (see section 4). Though this analyses focus on the situation in Europe, it also takes into account the fact that many of the identified points have either relevance in other world regions as well as that they also partly require global approaches due to the nature of Cloud Computing.

The review of the studies and articles also implicate some limitations. First of all most of the studies deal with Cloud Computing from a business point of view, because business use is seen by most studies as the crucial segment for further development of Cloud Computing. Though many of the points are also of importance for other users, they are often less reflected. In some cases public services are also analysed, but mostly together with business users. Consumers are often only mentioned shortly. One reason for that might be that in many cases the definition of consumer Cloud services stays vague and include services like streaming services such as Spotify, which are technically sometimes cloud based, but more often a peer-to-peer based service, or Facebook, which uses a worldwide distributed private Cloud, but which are not a Cloud service per se. Another argument in these studies is that barriers like availability, confidentiality and integrity are also seen as important for consumers, but that it is more feasible that due to their importance these issues will be solved with business users first. Although this viewpoint might be true, it bears the risk of overlooking developments like the consumerization of IT that might be one major trend in the next few years. Another one is the problem of the varying definitions, which was already addressed before. Similar to the problem of the varying definition of Cloud Computing, the varying terminology for drivers (sometimes enablers) and barriers among the different studies are problematic. Therefore one challenge is to sort and bundle or unbundle these different terminologies. Related to this is the question of the empirical basis of the different studies and the methods of data gathering and analysis. Many research articles are based on general opinions and less on empirical evidences. Although all arguments might be true, it increases the challenge of assessing single facts. In case of surveys and interviews the selection of questions and topics is often limited or, even worse, it might be based on the authors' intention and interests. Furthermore, all studies lack of long time empirical evidences like for example longitudinal studies of the impact and benefits of Cloud on organisations. Another point is that many of the barriers and drivers are interrelated or can even fulfil both functions depending on their current status (and maybe the point of view of the author). One example for the latter point is the availability of network connections, which can act as a barrier, in case it is insufficient, but it can also work as a driver of the development if enough network capacity is available. Consequently the identification and assessment need to reflect these points.

Finally, another limitation is that these studies deal foremost with the users' point of view. From an overall economic perspective this scope neglects the question if there is, similar to the adoption patterns in IT, a lower take up of Cloud service by European suppliers and, if the answer is yes, what are possible reasons for it. Though there is no definitive answer at the moment to it

Regarding the market situation, the overview of existing suppliers has already shown that the majority of important players in the emerging Cloud segment are of US origin. This is

confirmed by other studies that analyse the European deficits in participating in emerging IT markets (Veugelers et al. 2012, 12). It seems like that the current situation of the emerging market for Cloud services starts to reproduce the current situation of the overall software and IT services industry, which is for decades shaped by a dominance of American companies. Consequently we will also have a look at possible barriers for the development of the supply side. But while only a few studies (for example Rossbach/Welz 2011) deal with the situation of European Cloud suppliers, there is a continuous track of studies on the competitive situation of the IT and internet industry as a whole (for example Aumasson et al. 2010; Veugelers et al. 2012; Hoorens et al. 2012), which is used to derive barriers for the European Cloud suppliers. The main challenge here is to determine which of the overall barriers have a specific significance for them.

Overall results

First of all it is obvious that in the existing studies the number of barriers outnumber the number of drivers. One reason might be that many existing studies in Europe, based on the assumption that Europe lags behind, focus more on the barriers and risks and less on driver or benefits. As expected, there is also a strong focus on the demand or user side, in particular on business use. This latter point seems remarkable given the growing impact of private use on business use, which is seen as one of the major trends in the coming years. The number of factors related to the supply side is lower. Due to the high number of barriers and especially due to different naming and differentiations within the different reports there was a need for consolidation. Another differentiating characteristic is that for most of the barriers related to the demand side more research is done. In contrast, the barriers for the supply side are less specific and deal more with general problems of high technology in Europe.

Another point is that there is set of factors that are ambiguous, either because they are drivers or barriers for demand as well as for the supply side or they appear as drivers or barriers dependent on the different viewpoints. One example for the latter point is, as indicated, the question of security. While many people are afraid of security breaches caused through the storage of their data in premises of Cloud providers, other argue that Cloud providers normally are more serious and professional about security than many companies, in particular small and medium sized companies. An example for the former point is interoperability/standards and the related vendor lock-in. At a first glance it is often seen as a barrier for the adoption by customers, because it would reduce their operational flexibility and lead into dependencies from one supplier. But at a second look, the point also reveals its importance for the supply side, because on the long term such a situation would hinder effective competitiveness and would discriminate especially new firms entering the market. Both example show that the factors and actors are closely interrelated and that in many cases more viewpoints are possible.

Analysis of drivers

Overall, the analysis of drivers showed that drivers receive less attention than barriers. It is also not surprising that the few studies dealing with it focus strongly on drivers' significance for the adoption in business. There are only few studies dealing with more general aspects like infrastructure or technology, most often labelled as enablers. As a consequence drivers

specificly for consumers are mostly neglected, which is remarkable in that respect that some studies name consumerization of IT as one driver for business, but neglect the question why these persons use their mobile devices, presumably firstly bought for private use, also for work. In case of the barriers this is not the case due to the fact that many highlighted concerns of business are also highly relevant for consumers like data protection or security.

Table 4: Overview on identified and assessed drivers

Driver	Used synonyms or components	Source	Priority
mobility	integration of mobile devices	Cattaneo et al (2012c) Fielder et al. (2012, 32)	medium, long term higher
cost savings		Cattaneo et al (2012b,c) Colt (2011, 7 / 19) Fielder et al. (2012) Armbrust (2010)	high
flexibility	flexibility of IT sourcing flexibility of organisation	Cattaneo et al. (2012c, 22-24) KPMG (2011, 7-8) IBM/EUI (2012, 3)	medium to high (long term)
productivity	standardisation gains flexibility of organisation increased collaboration	Colt (2011, 6-7) Cattaneo et al. (2012c, 22-24) KPMG (2011, 7-8) IBM/EUI (2012, 3)	medium to high (long term)
innovation		Cattaneo et al (2012c, 22-23) KPMG (2011, 7-8) IBM/EUI (2012, 3) Fielder et al. (2012, 37)	medium to high (long term)

In principle most of the studies identify cost savings and resulting effects like increased competitiveness as the major driver for the adoption of Cloud Computing. Although this argument is true, it should be noticed that the time horizon of this driver is only short- and mid-term. The reason is that with a growing overall adoption of Cloud Computing in business the cost and all other resulting advantages will decrease. Consequently one can expect that other factors like innovation or flexibility will gain of importance in the future, because in the long-term they offer more potential to differentiate in competition for example by niche strategies or new innovation cycles. Finally it should be also noticed that most of these advantages are subject of decisions on company level. As a consequence it is complicated or impossible to induce incentives to do so. Only more general drivers like infrastructure or research can be influenced in different ways. Finally this may be another reason for the low attention on drivers.

Analysis of barriers

Table 5: Overview on identified and assessed barriers

Barrier	Used synonyms or components	Source	Priority
Level of R&D	low level of R&D funding	Turlea et al. (2010, 75) Turlea et al.	lower

	low level of BERD	(2011, 55)	
pre-commercial procurement		EC COM (2007, 799) Wessner (2008) Edler (2011) OECD (2011)	medium
lack of human capital	lack of skilled developers lack of skilled users	Aumasson et al. (2010, 263-272) Korte et al. (2009)	medium
public procuremnt and the role of the state		Aumasson et al. (2010, 231-240 / 142-143)	lower
network availability and realibility	sufficient network capacities reliable network	Fielder et al. (2012, 76) Cattaneo (2012a, 19) Schubert et al. (2012, 5) Couturier (2011) Hofman/Woods (2010) Fielder et al. (2012, 76) Cisco (2012)	medium
lack of interoperability	standards for data transfer interoperable API	Fielder et al. (2012, 74) Cattaneo et al (2012a, 19, 37-38) Cattaneo et al. (2012 c, 33-40)	high
legal jurisdication and consumer rights	jurisdiction in case of multiple countries in particular consumer laws	Cattaneo et al (2012c, 33-41) Bradshaw (2011) Colt(2011,11)	high
terms of contract/SLA	lack of transparency of terms lack of clear SLA	Bradshaw (2011) Couturier et al. (2011) Fielder et al. (2011, 67-71)	medium to high
data protection and privacy		Cattaneo et al (2012a, 45, 2012c, 28) Cattaneo et al. (2012c, 32-44) Colt (2011, 7)	high
data security and integrity	physical security physical integrity	Cattaneo et al. (2012c, 32-444) Asokan (2011) Fielder et al. (2012) Robinson et al. (2010) Bigo et al. (2012)	high
data location and retention	data location/localisation needs access by third parties	Cattaneo et al. (2012c, 32-44) Colt (2011, 11-12) Buchmann (2012) Lynn (2012) Fielder et al. (2012, 60)	high

		Robinson et. al (2010)	
data availability and reliable access	outage of data center data loss based on tech. Problems bankrupcy/acquisition	Cattaneo et al. (2012c, 33-40) Fielder et al. (2012, 48) Bohnert (2012) Cachin/Schunter (2011)	medium to high
market fragmentation	challenges of cross-border operations payment VAT etc	Aummasson et al. (2010, 224-227)	medium
vendor lock-in	technical lock in financial/legal lock in	Cattaneo et al. (2012 c, 33-40) Cot (2011) Hofmann/Woods (2010)	high
lack of trust	lack of trust loss of control	Cattaneo et al. (2012b, 12,41,55; 2012c, 33-40) Colt (2011, 22-23)	high
lack of transparency	transparency of total cost transparency regarding update/customization transparency of audits/certifications	Colt (2011, 22) Cattaneo et al. (2012a, 60) (Cattaneo et al 2012c, 32-40)	medium to high
lack of financial capital	lack of capital for founding lack of capital for growth	Veugelers et al. (2012, 25-35) Aummasson et al. (2010)	medium

As expected the analysis of barriers shows a strong focus on barriers that are in particular related to the business use of Cloud Computing and less on specific challenges for public services or consumers. Not surprisingly the analysis points out that the focal area are all barriers related to data security, data location, data availability, trust and privacy. In nearly all studies they are among the most important ones and it is obvious that they have a high significance for business as well as for consumers. The detailed view of it also underlines that these barriers are strongly intertwined. Moreover, they also influence the market development, which is reflected in the lower adoption of Cloud services in Europe. The interrelation and its impact is less astonishingly because they all can be seen as a result of one basic principle of Cloud Computing: The loss of the physical control over IT and data and its consequences. Therefore trust and legitimation will play an important role for the further uptake of Cloud Computing for business as well as for consumers, in particular after the disclosure of the massive surveillance actions in the US and Europe. This also underlines the need for an increased knowledge diffusion and trust building in case of Cloud Computing or other emerging technologies, which should not only be focussed on the

knowledge transfer between research and industry, but also on knowledge diffusion between research, industry and society with a focus on non-technical aspects (trust building). Related to this another cluster of barriers arises around the legal and regulatory framework, particular questions concerning the jurisdiction, consumer rights and contractual issues (terms of contracts/SLA). All points are applicable to both, business as well as consumers, but the importance may differ. In particular the topic of SLA and liability is especially for small and medium sized companies and consumers of great importance, because they need to rely on the use of standard contracts and SLA and are not able to negotiate customized contracts and SLA's as bigger companies can do. The contractual issues also refer to another cluster with a particular high significance for business, i.e. the question of vendor lock-in and related technical and legal issues like interoperability and standards. The reason for its significance is quite obvious given the problems that can arise from it like a lack of flexibility due to problems with data portability and integration or dependency on single vendors. They directly lever out the related benefits for users or in the worst case flip them into the opposite. Not surprisingly, fears regarding this lower the probability of adoption. Finally the latter cluster also shows that many of these barriers also contain a specific technological component like vendor lock-in and interoperability or data availability and scalability of systems. This is also something that needs to be reflected.

While this sketches a clear picture for barriers on the demand side, the one for the supply side does not seem to be so clear. Some points like vendor lock-in as well as standards and interoperability are clearly also of importance for Cloud providers. Also contractual issues or questions like data protection might be of indirect importance, in particular for start-ups and smaller and medium sized enterprises, because it would provide clarity necessary to enter the market. Whereas these points also show a certain degree of specific relation to Cloud Computing, the other points are generally broader and affect not only Cloud service provider. However, some of them bear individual points that are at least of certain significance and even more for Cloud Computing. One example is the market fragmentation, where points like the VAT regulations or the eCommerce directive have a specific relevance not only, but also for Cloud service provisioning. Other factors like lack of financial capital or the importance of the different types of public procurement refer to general challenges, which are also of relevance for ICT in general as well as for other high tech industries.

3.4. Impacts of Cloud Computing services

Cloud Computing currently turns the provision of IT resources upside down. It is therefore not surprising that Cloud Computing does not only affect its users which range from businesses via public administrations through to consumers but also the ICT industry and the society and economy as a whole. While there are plenty of estimations with respect to impacts of Cloud Computing on its users and their environment, there is hardly any robust evidence. Moreover, there is a quite emotional and controversial debate.

3.4.1. Impacts on businesses and public administrations

Cloud Computing affects both businesses regardless of their size or industry, and public administrations. The reviewed literature provides some interesting insight into impacts of

Cloud Computing services. The estimated numbers concerning some of them vary however between different studies.

On the one hand, according to recent studies, the cost situation is among the primary drivers for cloud adoption. Many businesses and public administrations adopting Cloud Computing expect to be able to benefit from cost advantages to some extent. Although hard to measure accurately organizations mainly perceive the total cost of ownership (TCO) of Cloud Computing as lower than the one of alternative approaches to the provision of IT resources. As organizations usually want to preserve cash, being able to shift capital expenses (CapEx) to operational expenses (OpEx) is desirable. Such a shift in expenses can typically be realized by using cloud services. Further popular drivers are related to flexibility and scalability. Apart from flexibility and scalability themselves also agility, capacity for innovation and mobility are mentioned frequently. These impacts make Cloud Computing increasingly be seen as a prerequisite to remain competitive. On the other hand, recent studies suggest that issues related to security and business continuity inhibit the adoption of Cloud Computing. Business and public administrations do not only have concerns with respect to negative impact of Cloud Computing on security and compliance but also with respect to difficulties in terms of interoperability.

Impact on the cost situation

The most often mentioned impact that Cloud Computing has or is going to have on businesses is the one related to the cost situation. Also governments, both local and regional ones, could possibly realize significant savings if Cloud Computing is used. The initial costs for using cloud services are low as compared to running comparable services on one's own servers (Ecorys 2009, 63). This is especially important for start-up companies which usually don't have the funds required to set up and run own servers. It has been difficult to find reliable numbers for such cost savings, though. The case studies above provide insight into the nature of some savings.

Hogan et al. (2010) differentiate between three types of cost savings related to Cloud Computing. They base their findings on proprietary research provided by EMC, but do not describe their methods and findings in much detail. The authors differentiate between (1) IT capital expenditure (i.e., servers and computers), (2) IT labour costs and (3) IT power and cooling costs (Hogan et al. 2010). According to Hogan et al. (2010, 33), up to 40% can be saved in public clouds with respect to IT capital expenditure, up to 31% with respect to IT labour costs, and up to 80% with respect to IT power and cooling costs.

IDC conducted several related studies on behalf of the EC. We quote the final report by Cattaneo et al. (2012c) as well as an earlier, more detailed version by Cattaneo et al. (2012a, b). Cattaneo et al. (2012a, b, c) surveyed 1.056 businesses and found that 78% saw cost savings when using Cloud Computing, the average cost savings being between 10% and 19% (Cattaneo et al. 2012, 22). The authors, however, use a rather broad and somewhat unclear definition of Cloud Computing services and respondents were not required to provide much detail on their perceptions with respect to cost savings (Cattaneo et al. 2012, 28). The questionnaire was not released but it appears that examples of cloud

services were provided by IDC and that respondents were then asked whether they use them and to what extent they think the services allow cost savings.

The majority of companies still manage their data on premise or in from of traditional outsourcing to a nearby data centre. While rather general statements on the impact of Cloud Computing on the cost situation of businesses and public administrations can be made, it can't be said that cost savings of a certain amount arise from using a specific Cloud Computing service. There are numerous factors related to the user organization, its environment and the used service that affect the potential for cost savings. In 2011, the EC expected 25% to 50% savings through the adoption of Cloud Computing (COM 2011/896/EC, 1). Only one year later, the EC quoted IDC's estimation of cost savings between 10% and 20% (COM 2012/529/EC). As Cloud Computing seems to be a difficult area for reliable estimates, we suggest treating the figures that are available with caution.

Impact on flexibility and scalability

Cloud Computing allows businesses to experiment with and to implement new services faster (Fielder/Brown 2012, 36) because there is no time needed to deal with computer hardware a lot (Ecorys 2009, 63). For example, if a program developer is hosting an app and needs more computing power, it is easier and faster to rent computing power via a cloud service than to buy the needed servers (Meyer et al. 2012).

The factor scalability is related to flexibility, but focuses on the demand for computing power. Through cloud services such as Amazon S3 (Scalable Storage Service), it is easy to adapt the computing power to what is really needed. This is much easier than building up or expanding an own 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 (Venkataraman/McArthur 2011). So a start-up company may start with limited capacity but increase capacity easily at a later point in time. If such a company had their own servers, they might have costs for overcapacity in the beginning, and later, when business prospers, it might not be able to match the demand.

The flexibility and scalability of Cloud Computing can reduce the time until 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 itself (Woloszynowicz 2011). Cloud Computing itself is an innovation that givesn the opportunity to create new services and businesses, not only for specialized markets but also for wider consumer use (Ecorys 2009, 67). Many examples for companies that use Cloud Computing can be found, e.g. Airbnb, Ubisoft and Spotify (Amazon 2013b). Especially start-up companies that use cloud technology can be innovative.

Impact on security and business continuity

Cloud providers can offer higher levels of security for data than most of their customers can themselves as they often do not have the necessary know-how. While some organizations have a very professional management regarding attacks or backups, others, mostly SMEs

do not. In other words, SMEs without specific security know-how may benefit particularly from professional security management in the cloud. Organizations that store data in the cloud (Fielder/Brown 2012, 48) have to deal with issues such as transmission security, trust in the Cloud Computing service provider, and the possibility of insiders eavesdropping. If a business transmits data into the cloud, it loses control over it to some extent. 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). Over 60 self-selected experts were interviewed. The general anxiety of malicious attacks aimed at cloud providers also increases the fear of loss of control (Borgmann et al. 2012, 11). For instance, it is often unclear what legal authority would be in charge and how a trial would be pursued if needed. Another issue may be that a cloud provider goes out of business and the data stored there cannot be accessed anymore (Fielder/Brown 2012, 48).

In terms of information security, concerns are mostly related to availability and confidentiality. It is crucial for businesses that their services are available; otherwise they can lose customers and revenues. With respect to availability, two main points are particularly relevant. 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 provider (Borgmann et al. 2012, 51). In case of an outage of a large provider, more than one company will be affected. Additionally, cloud 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 et al. 2012, 11-14). The other point is the availability of sufficient bandwidth (Schubert et al. 2012, 11 and p. ii). Although the access to fast Internet connections is growing in Europe, it can still be a problem. Broadband access is available in cities but not yet in many rural areas. Since businesses not only reside in cities, this can be a problem for Cloud Computing. Consequently, 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. Confidentiality of business-critical and customer data is crucial for businesses. For business users this means that they have or should be concerned if access to their data in the cloud is limited. The questions arise how well data is protected and what kind of data a business user should put in the cloud as what not. This is especially important for customer data for which privacy regulations apply as well as for business-critical data. With Cloud Computing, the infrastructure may be shared with competitors, which might bring in new risks.

The questions that arise with respect to issues of liability and contract issues are crucial for businesses and are quite difficult to handle. Since cloud 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 (Cattaneo et al. 2012c, 65). Various aspects of cloud contracts were discussed by 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.

Summarising, one can say that business customers need new competencies to negotiate with cloud providers, to keep their data under sufficient control, 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. The assessment of the reliability of cloud providers can be difficult for businesses (Robinson et al. 2012, 68). There have been attacks recently that targeted cloud services; for instance, the cloud service Evernote which had 50 million users in 2013 world-wide was subject to an attack. Both user names and passwords were stolen (Vaughan-Nichols 2013).

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 and public administrations will have to deal with new types of issues, such as keeping control of the whole process, assuring confidentiality and managing legal issues. This means that if cloud providers achieve to be perceived as trustworthy, the cost savings even larger cost saving should be possible in the future. The European market in particular could benefit if customers could easily identify cloud providers which comply with European legislation, and which do not make data available to competitors or foreign governments. Certification might play an even more prominent role in the future. This way Cloud Computing could have a much larger economic significance in the future and a large effect on traditional IT providers.

3.4.2. Impacts on consumers

Cloud Computing is not only a phenomenon which is relevant for businesses and public administrations but also one that affects consumers. Of particular importance from a consumer perspective is convenience but also privacy and security issues play an important role. On the one hand, Cloud Computing affects the lifestyle and behaviour of consumers. The use of cloud services, however, does not only make the lives of consumers more convenient but also makes them increasingly dependent on technology. Additionally, Cloud Computing is expected to drive the blurring of the boundary between work and private life. On the other hand, while many cloud services aimed at consumers do not come with financial costs for their users, they come with costs for users in the sense that they have to give up part of their privacy. Consumers, however, do not only expect to face negative impacts in terms of privacy but also have security concerns. Several security breaches in the last years have damaged the confidence of consumers in cloud providers noticeably.

Impact on lifestyle and behaviour
Cloud Computing makes data accessible 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)" (COM 2012/529/EC, 4). Another aspect however is that Cloud services only work if the consumer is online. This requires reasonable fees for transmitting data and good connection quality. Mobile data roaming fees, for instance, hinder the upload of holiday videos or photos or the download of larger amounts of data such as videos while abroad. Also, in remote or holiday areas, basements, trains etc. connectivity might be low or non-existent. The use of Cloud Computing services accelerates the reduction of the separation between private and work life, which already has been going on for many years. Employees bring their own devices (BYOD) and use their own software or services and thus bypass their company's IT department, for instance by using Dropbox for team work or by renting an Amazon server. Work documents can now be accessed also from the home computer or from mobile devices. This puts additional pressure on employees to respond faster and to work more. On the one hand, employees try to avoid it. Within the scope of a study, only 30% of the interviewed employees said 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. Yahoo!'s management, for instance, has forbidding its employees to work from home (Goldsmith 2013).

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. 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.

Impact on privacy and security

The more services are transferred to the cloud, the more consumers become dependent on the cloud provider, the Internet and their access devices. As already mentioned, there may be no suitable network access when travelling or on holidays. If a service is down, the consumer can usually not do much to recover the data. In 2009, for instance, 800.000 users of the smartphone Sidekick had temporarily lost personal data from their devices. The servers holding the data were run by Microsoft (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.

Many Cloud Computing services used by consumers can be used free of charge, at least if rather small amounts of data are stored or processed. Examples are Dropbox, Gmail, Evernote, Zotero or Apple iCloud. Free services are sometimes designed in a way that they are somewhat clumsy or limited as compared to the premium versions of the services. Of course, there are other costs users face including the exploitation of their data for various purposes. Consumer data might be sold or used in other ways. This is shown, for instance by the controversy that developed around the photo service Instagram in 2012 and its plans to change their terms and conditions of how pictures of users can be used for advertisements and how they can even be sold (Pepitone 2012, Schneier 2013a).

Instagram had to withdraw their plans after heavy critique by its user base. Apart from that, the photo service Flickr recently 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).

However, besides privacy also security is an issue for consumers. Insiders at cloud providers might read private data just as governments. Legislation permitting the government access to data stored or processed at a service provider to some extent exists in many countries (Greif 2012). 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.

Conclusions
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.

3.4.3. Impacts on the ICT industry

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

Impacts on market and industry structure
As outlined before (see chapter 3.1.) one experiences some difficulties to assess the impact of Cloud Computing on the market and industry structure for several reasons. One reason is the availability of data, in particular beside the market for public Cloud services. Above that each market survey follows its own methodology, which varies strongly between different market researchers as well as the market researchers themselves vary their methodology over time.

Overall, most of the market researchers agree that the share of public 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 (IDC 2012; IDC 2013a; EITO 2013). Taking other recent market studies on Cloud-related IT services as well as private Cloud services (IDC 2013b, c), the share might be already at 6-7%.[15] Consequently Cloud will develop to an independent, fully-fledged segment of the market. According to their estimations, the classical software product segment (including maintaining) is mostly affected as well as specific parts of the IT service market such as IT outsourcing. While parts of this enormous growth will result from the overall growth of the software and IT services as well IT hardware market, it will also replace parts of existing markets, in particular the classical segment of software products based on licenses and maintenance contracts as well as IT service segments like Outsourcing. However, there is

[15] These estimation are based on the IDC data, which also provides data for the EITO report. According to it the size of the global software and IT services market will be 770 bn. € (~1.050 bn $) in 2013 (EITO 2013).

some uncertainty about the extent of these impacts. In an early forecast commissioned by the European Commission on Mobile and Cloud Computing, PAC and Idate stated that both developments will lead to stagnation and decline of revenues from IT services and licences after 2016 (Aumasson et al. 2010). Other forecasts do not touch this question in detail, but Gartner (2012, 2013a) as well as IDC (after Bloomberg 2012) clearly state that Cloud Computing will be the driving force of the overall market. In the long term the implications are the same. Nevertheless some open questions remain. One question is whether the loss in the IT services due to the shrinking of outsourcing services will be compensated by the growing need for Cloud related services like integration and implementation or not. In case of growing tendency towards hybrid models (Rüdiger 2012) this increase could be even stronger then the loss and lead to further grow.

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). Apart from 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 2013a). 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.

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 users, 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 like hosting companies (e.g. Terremark, Strato) or most of the telecommunication providers (e.g. BT or Deutsche Telekom). Others like Amazon may be a surprise at a first glance, but given the fact that their 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 users. Moreover also smaller software companies could exploit these opportunities by using the infrastructure of other providers such as Amazon. Overall Cloud Computing offers foremost many opportunities for existing software and IT companies, but there are 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 a yearly revenue of more than 200 million $. Though many users (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 providers 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 a data centre infrastructure. This is also reflected in research on new business models for Cloud Computing, which show new types 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 actors 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).

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 a utility comparable to electricity or water. As many other discussions in the context of Cloud it already started in the early 2000s (Carr 2003). The argument of Carr and others 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 a 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 (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 (see chapter 2.2) 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 or if the overall structure will change in long term. 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.

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 adds that many small companies struggle to sell their services and products, especially on markets outside their national borders, due to a lack of knowledge of how to use new services, without providing details (Ecorys 2009, 11).

Conclusions

Overall, it can be stated that Cloud Computing 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 Cloud Computing 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 will be merged 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 SMEs, which have experience with relevant Cloud technologies or particular business services. Thirdly, as a consequence the industry structure and in particular the dominance of companies based in the US will not change much. 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, in particular because of the recent disclosures on the practices of the NSA. Therefore, it is needed to address challenges that hinder European IT companies.

3.4.4. Impacts for the society and economy as a whole

There is only a limited number of researchers and studies that dealt with the overall economic and societal impact of Cloud Computing (Etro 2009; 2010; 2011a, b, ;DIW 2010; Cattaneo et al. 2012c; Hogans et al. 2010) or related developments such as Future

Internet (Hoorens et al. 2012). As outlined before all studies are forecasts based on specific econometric models and estimations of future developments like future cost savings. This has to be reflected in the following review.

Impact on employment

At the moment only forecasts and estimations regarding the impact on employment exist, which are all quite positive. *Job creation* is an often named impact of Cloud Computing and its adoption (Wauters et al. 2011; Aumasson et al. 2010; Cattaneo et al. 2012c; Hoorens 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 (Cattaneo et al. 2012c, 9). Another estimation is 1 million jobs (Etro 2010, 108). Cattaneo et al. (2012c) 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." (Cattaneo et al. 2012c, 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 (2010, 2011a, b) 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 of 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 two studies which present large parts of its method is Etro (2010) and Hoorens et al. (2012), which are both based on optimistic assumptions and expectations. However, there are also a few critics who 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 et al. 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.

Any rise of new jobs is closely connected to the creation of new businesses. 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.

Impact on 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; 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 (Cattaneo 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) (Cattaneo et al. 2012c, 61). But for 6 years, it would be at least 540 billion. The numbers appear inconsistent. Based on Cattaneo et al., the European Commission expects "an overall cumulative impact on GDP of EUR 957 billion [...] by 2020" (COM 2012/529/EC, 2).

Impacts on technological sovereignty

From a European point of viewn it is noticeable that as already described before (see section 3.1 and 3.2) few US based Cloud Computing providers have a strong global role because the US allowed Internet services relatively early and developed huge economies of scale, as well as companies with significant investment capabilities. This creates a clear challenge to the technological sovereignty of Europe.

Impact on civil liberties

One example for possible impacts on the civil liberties is possible adaptation of content and censorship. The big content providers already censor content and will continue doing so, which is in particular relevant for cloud based, consumer oriented services such as streaming. 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).

Impact on sustainability

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 (Hoorens et al. 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 (COM 2012/225/EC, 5). It mentions the positive aspects that Cloud Computing could bring, e.g. saving energy through low-energy data centres and the use of green energy (COM 2012/529/EC, 4). In all four documents mentioned, no figures on a change of energy consumption because of Cloud Computing have been mentioned.

Conclusions

For the society as a whole, regarding jobs and growth, Cloud Computing has limited impact at the moment. The estimates for the next five to ten years provided by different researchers (Etro 2009, 2010, 2011a, b, Hogan et al. 2010, Cattaneo et al. 2012c, DIW 2010) appear to be based on optimistic input variables for cost savings and the emergence of new SMEs. Another point is that the models use 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 show 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 highly 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, in particular where it is created. 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 reliable, privacy-protecting European Cloud providers appear. 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.

After all, this review shows that at the moment both large job growth with Cloud Computing providers and large job reductions in company IT-departments apparently have not yet appeared. On the other hand, Cloud Computing offers entrepreneurs methods to kick start new businesses as we can see with examples like Airbnb, Zotero, the examples mentioned at Amazon or Facebook apps that run on the basis of Cloud Computing. So in sum there appears to be some hype about Cloud Computing, which is usual for the industry. 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.

4. CHALLENGES OF CLOUD COMPUTING

Based on the results of the identification and assessment of barriers as well as the analysis of the different impacts a set of six challenges was selected. It will be analysed in detail in the following sections. Among them are information protection, privacy and data protection, governance issues (data location, third party access, etc.) and contractual issues. Above that challenges for the market competitiveness, partly also identified in the impact analysis, as well as technological challenges are further subjects of the following analysis.

4.1. Technological challenges

Though there are only a few technological challenges named in the analysis of barriers and impacts, there are reasons two have a more detailed look at some challenges for two reasons. The first one is that among the identified impacts, drivers and barriers some relate to technological capabilities. One example is flexibility which demands efficient and highly scalable infrastructures. The second reason is that some challenges are reinforced by technological issues. The most prominent example is the vendor lock-in resp. the challenge of data portability, which can be reinforced by a lack of standards. Consequently these challenges will be shortly analysed in the following. Finally it should be noted that information security is also a technological challenge, but due to its importance it is treated separetly. Moreover information security is not only a technical issue, it also relates to organisational aspects, governance (see section 4.4) as well as to legal issues (4.5.3).

4.1.1. Interoperability and standards

The issue of standards and interoperability 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. In particular in combination with legal challenges regarding contract termination (see section 4.5.2) it will gain also a growing importance for Cloud Computing, because together they can result in a vendor lock in (see section 4.6.1) (e.g. Aumasson et al. 2010, 191-198; Ecorys 2010; ESA 2009). The reason is that one way to achieve 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.

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).

Given the fact that the challenge of standardization and interoperability for Europe exists for a long time, there are numerous efforts to increase standardization and interoperability. It includes efforts for strengthening the European position like the promotion of the role of ETSI (European Telecommunications Standards Institute) as well as the support of European companies to participate in in industrial standardization committees such as as IEEE, which are the dominant way of standard setting in the IT industry. Similar to that also different initiatives in the field of interoperability were started, for example the adoption of a European Interoperability Framework (EIF) for eGovernment services. Overall, most of these activities had little success. Finally the EU adopted in 2012 a regulation on standardization in 2012 (Regulation 2012/1025/EU) as a result of review process of these previous activities. Since it will take time until the implemented measures will work, it is hard to estimate its impact for the European role. Beside of that there are also some others, mostly industry driven initiatives related to standards and interoperability in the field of Cloud Computing. Some examples are the development of two frameworks and toolkits (OpenStack[16] and OpenNebula[17]), which are developed as open source and aimed at supporting interoperability, standardization and portability. Furthermore the Organization for the Advancement of Structured Information Standards (OASIS) started efforts in Cloud standardization like TOSCA (Topology and Orchestration Specification for Cloud Applications)[18], but also other institutions such as IEEE or OSBF and others did so (Heise 2012). This poses the question, if there will be a common framework and which one it will be or if even proprietary solutions will profit of this situation.

4.1.2. Data management and scalability

Data management and scalability are still challenges in Cloud Computing because data - as well as the code - are both not structured optimally. Due to this resources are wasted and resource utilization could be far more optimized in the future. At the same time, the size of data is constantly growing. Big Data is a challenging factor for storage and computing resources. 1.2 zettabytes of data were produced in 2010 and will increase to 8 zettabytes[19] in 2015 referring to a market research study of IDC (Gantz/Reinsel 2011). Traditional relational databases can't cope with this amount of data. Since recent years the NoSQL movement offers techniques to store large amounts of data but lacks in ensuring the consistency of data. Therefore, further research is necessary in this field. Especially within update intensive applications the offered support is very restricted because ensuring consistency and integrity is difficult (e.g., due to duplications or concurrent access). The amount of data is growing faster than storage and bandwidth do. In this field also the increased usage of mobile devices is challenging for the existing systems.

With respect to the challenge of providing scalable data management, Agrawal et al. (2010) emphasize the trade-off between consistency and high scalability and availability. The authors highlight design principles for systems providing scalable and consistent data

[16] See http://www.openstack.org/.
[17] See http://opennebula.org/.
[18] See https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca.
[19] 1 zettabyte = 10^6 petabytes

management for cloud computing applications. According to Agarwal et al. (2010) scalable data management should be based on the following design principles know from key value stores

- Segregate system and application state;
- Limit interactions to a single physical machine; and
- Limit distributed synchronization.

However, while data management systems based on these principles are good only for single key atomic access, applications increasingly require scalable and consistent access to more than a single key. Traditional database servers running on commodity machine instances in the cloud often become a scalability bottleneck (Agarwal et al. 2010). Key value stores like BigTable or Simple DB cannot be used as the majority of Web applications are designed to be driven by traditional database software. Migrating them to the cloud results in running the database server on commodity hardware instead on premium enterprise database servers. Agarwal et al. (2010) stress that porting these applications to utilize key value stores is often not feasible due to technical and logistic reasons. They conclude that modern applications in the cloud require data management solutions that can run efficiently on low cost commodity hardware, while being able to support high data access workload and provide consistent access to more than a single key. Das et al. (2010) propose with G-Store such a scalable data store for transactional multi key access in the cloud. Schubert at al. (2010, 50, 59) go in another direction and state that in order to improve scaling and distribution behaviour, the actual structure of cloud based programs and data needs to be improved through new segmentation concepts and distributed programming models. From their point of view, communication, latency, user location, and in particular consistency handling will play major roles in the context of cloud computing to enable large scale efficient applications. The problem that user behaviour and demands are not easily predictable will persist in the future and thus scalable data management systems will continue to be important. An effective usage of resources must be possible even without being able to estimate the resources needed at a particular point in time well.

4.1.3. Conclusions

The two points underline the importance of technological development for the further development of cloud computing. Standards and interoperability are important for two reasons. Firstly, because only interoperable cloud services enable users to fully exploit potentials of cloud computing such as dynamic usage and flexible payment. Secondly, standards and interoperability prevents vendor lock-in, which is a concern representing a major barrier for cloud adoption. Therefore this challenge needs to be addressed. Considerations with respect to scalable data management are important in the context of cloud computing as the amount of data being processed is growing constantly and as the majority of Web applications are designed to be driven by traditional database software and porting them to utilize alternative data stores is often not feasible.

Possible measures are:

- Support for the the EIF and others by implementation in public procurement processes
- Support of participation of European members, in particular from SME, in industry-driven standardization bodies

4.2. Challenges in data security

Basically, there are the classical security issues of confidentiality, integrity and availability. We look at them one by one.

4.2.1. Main challenges

Confidentiality

The discussion of the Snowden-documents indicates that there is no confidentiality of data on computers connected to the Internet. Two reasons for that are mentioned. One is that the NSA has a large facility to eavesdrop Internet traffic, such as having a three days rolling buffer of data on 150 servers (Bowden 2013). The dangers inherent in the centralization of data processing have received explosive attention on the heels of the leaks by NSA contractor Edward Snowden 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).

The other reason is that the NSA can also read encrypted information by using backdoors. The latter, reportedly, are in operating systems, cryptographic software, and random number generators ("Bullrun", cf. Guardian 2013a; Shumow 2007; Ferguson 2007). „The NSA saves all encrypted data it encounters; it might want to devote cryptanalysis resources to it at some later time" (Schneier 2013c). The Guardian also reported that the British GCHQ knows ways to read encrypted traffic (Guardian 2013a; Guardian 2013b). The Stuxnet malware was another piece of evidence that some large organisation knew about the possibility of new zero-day attacks for months (Falliere et al. 2010). Also the anonymisation service Tor has been hacked, according to BBC, by a law enforcement agency (BBC 2013).

Well-reputed technical experts, such as Bowden and Schneier, believe that the claims concerning the NSA are true. Schneier concluded that the whole Internet has been undermined by the NSA (Schneier 2013d). As the issue of backdoors is somewhat less visible in the media, we present one "evidence" from the Guardian website (Figure below). Note the last sentence which mentions the plan to insert backdoors in commercial IT and crypto systems. It has been said that the NSA is "enabling [this] for encryption chips" (Guardian 2013c), too, so tamper resistant hardware might be undermined, too.

Still, from a scientific point, the Snowden and Guardian documents may contain errors or be misunderstood. For instance, Snowden has been claimed to have said: "there are strong crypto systems that can still be relied on" (Guardian 2013d). This may have been misleading, if read in isolation. Snowden apparently meant that information encrypted using well-reputed cryptographic software cannot be deciphered. However, it appears that institutions such as the NSA can hack into the endpoints, to read the communication in the clear, and Snowden seems to be aware of this: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately,

endpoint security is so terrifically weak that NSA can frequently find ways around it.“ (Snowden 2013)

Figure 8: A document from Snowden, published on the Guardian website (Guardian 2013c)

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1]Includes enacted OCO funding. Totals may not add due to rounding.

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

(TS//SI//REL TO USA, FVEY) This Project supports the Comprehensive National Cybersecurity Initiative (CNCI) by investing in corporate partnerships and providing new access to intelligence sources, reducing collection and exploitation costs of existing sources', and enabling expanded network operation and intelligence exploitation to support network defense and cyber situational awareness. This Project contains the SIGINT Enabling Sub-Project.

(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.

Another sentence which may give reason to doubts is this one: „Another program, codenamed Cheesy Name, was aimed at singling out encryption keys, known as 'certificates', that might be vulnerable to being cracked by GCHQ supercomputers.“ (Guardian 2013a) However, certificates are no encryption keys. Rather, they are digitally signed statements indicating who the owner of an encryption key is. Also, these encryption keys are not vulnerable, rather they are public. In sum one might say that the evidential value of the Snowden documents might warrant further analysis. However, it appears the US government did not claim them to be counterfeit. To the contrary, NSA director Keith Alexander was quoted saying, when asked about his reaction to German expressions of surprise: "We don't tell them everything we do or how we do it. Now they know." (Reuters 2013).

Summarising it becomes clear that there is a high risk that all computers by US manufacturers, in particular the mainstream software, have been undermined by the US government. While physically separated systems might have some security left, connected systems can no longer be assumed to reliably protect passwords, business secrets or similarly sensitive information (for details, see Schneier 2013e). Furthermore, the enormous mass of data stored in clouds represents an 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. Herfert and Waidner add that Cloud Computing providers "avoid publication of security incidents which damage their reputation" (Herfert and Waidner 2013).

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). Snowden's revelations may have already fundamentally changed public perceptions of the risks/benefit calculus in connection with cloud computing.

Integrity

The integrity of systems on the Internet can, of course, be violated by institutions such as the NSA. There are also many other attacks by other individuals or organisations imaginable, such as hacks into the management interface or hijacking of accounts.

Availability

Regarding availability, there are several issues. One is the availability of Cloud servers. For example, Amazon had significant outages, causing harm to the customers of AWS. 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. A second issue are Denial of Service attacks. 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. A third issue is the availability of the network. While many networks, such as DSL, have a fairly high availability, they are not as permanently available as a local computer. Regarding wireless access, availability is an even larger issue. So Cloud Computing is not yet quite "available everywhere and to anyone", as a European Commission document (COM 2012/529/EC) put it – not to mention wireless data roaming fees. On the one hand, issues of wireless connectivity are being addressed, for example by using digital dividend spectrum for LTE with obligations to cover remote areas. On the other hand, there will remain remote areas, tunnels, basement or simply outages which will make ubiquitous access to Cloud Computing services difficult.

On a different level, the observation remains true that users lose control of their data when transitioning to the cloud.

4.2.2. Consequences

Consequences regarding confidentiality

Developing computers which are able to keep secrets confidential while on the Internet is the most important challenge. Not only to protect European citizens and businesses against secret services, but also for having a more solid computing base against any sort of crime: "Today's NSA secret techniques are tomorrow's PhD theses and the following day's cybercrime attack tools." (Schneier 2013f) If one wants to have computers which keep secrets reliably confidential, it is necessary that they do not have any flaws or Trojan horse functionality (backdoors), in their soft- and hardware. This means:

- To have operating systems which do not contain backdoors.
- To have cryptographic software without backdoors.
- To have application software which does not communicate secrets to other places.
- To have hardware which is free of Trojan horses.

The reason for the latter demand is not only the academic discussion of possible Trojan horses (e.g. Becker et al. 2013) and the indications referred to above, but also the worries about Trojan horses in chips manufactured, e.g. in China (CPNI 2102), and last but not least the assumption that if unhackable software gets used, institutions such as the NSA would investigate to undermine hardware, just like they apparently undermined cryptography once people started using strong cryptography. The above mentioned components would need to be of high quality, just like in the railway or aerospace industry, on a smartcard like level, or even proven (Kuhlmann, Weber 2009; Heiser 2013). Without a secure computing base, minimum security standards for achieving a high level of confidentiality, as aimed at by the European Commission (COM 2012/529/EC) or Parliament (Castillo Vera 2013a), cannot be achieved.

As users will wish to continue using their existing applications, the concept of virtualisation could be used for isolating existing applications against malware. This would mean to have a highly secure isolation architecture. Two computers using legacy applications could then work and communicate securely, isolated from any possible new malware. Well-defined tunnels could be used to let isolated applications communicate with each other. For communicating data between remote computers, encrypted channels would be needed, which require a well-controlled infrastructure for certifying public keys, which would have to be better than, e.g. Diginotar (Jacobi et al. 2012), most likely with much more government control. The solution sketched here is not really new to the computer security community. Industry and military have been taking steps into such directions (Grawrock 2006; Darpa 2012), but Europe should make sure it does not contain unwanted functionality. An entire, open system for civilian use does not yet exist, only partial solutions of various security quality. How a full system can be created will be discussed below under "policy options". Regarding the abuse of confidential data transmitted in the clear, e.g. normal, unencrypted private emails or private SNS data, legal solutions may be needed, which will be discussed below.

Yet another option for processing data in the Cloud, in a confidential manner, would be to use tamper resistant components or homomorphic encryption. While homomorphic encryption does not appear to be practical for the near future, Cloud servers could use tamper resistant modules to protect data against insiders. Remember the idea to use "Trusted Computing" chips to avoid that users copy music data. The principle could be reversed: servers could process data without administrators being able to read them. This could be likened to much enhanced HSMs. The user data would be encrypted when leaving the module. While this approach would technically be feasible, its cost are higher; it is unknown how much such a kind of remote, confidential processing would cost more per bit, if applied at large scale.

Consequences regarding integrity

Regarding integrity, a well-designed system, as sketched above, would also facilitate building proper means to protect data against manipulation or loss. Given the current threats of confidentiality, this is a minor issue. Still, data in the cloud face risks that legitimate users might try to manipulate data, e.g. through code-injection. Also drive-by-exploits are possible (cf. Enisa 2013). However, isolation could be used to limit risks, e.g. if a drive-by-exploit could be limited to a general surfing compartment, to be deleted after use, so that the exploit would not be able to reach its target (Weber 2012). Also, providers may not use sufficient protection of their systems, including of backups. These are general issues which have been addressed, e.g. in the STOA eGovernment project (cf. Jacobi et al. 2013b). They need to be addressed with professional handling and could be made subject to certification of providers.

Consequences regarding availability

Regarding availability, let us start with network availability. Regarding fixed networks, for video and other high-capacity demand, using fibre optics is useful. It appears that the Swedish model of communities providing local networks is a feasible approach (cf. Sandgren, Mölleryd 2013). Broad demand for this has been reported from families with several members interested in parallel download. However, the provision of DSL and fibre appears not to be economic in less densely populated areas. Here, wireless communications can help. Broadly speaking licensed communication can solve this, as well as unlicensed. Licensed communications can take the form of auctioned spectrum with obligations to cover remote areas. Some EU-wide licenses could spur diffusion and competition. Competition would increase if users of remote areas would be put into a position to set up unlicensed, wide-range networks by themselves, as proposed by Elsner and Weber (Elsner and Weber 2013).

Regarding denial-of-service attacks, users may wish to have local facilities to continue their work.

4.2.3. Conclusions

Regarding security, the most important problem is that – according to discussions in the media and by security experts, following the Snowden revelations – the security of software and possibly also of hardware has been undermined by the US government. As one document stated, it is the plan of the US government to: "Insert vulnerabilities into

commercial encryption systems, IT systems, networks, and endpoint communications devices." For having any reliable confidentiality of data on computers, the most important policy measure, in our view, would be the following:

1. The development of open soft- and hardware, which does not contain any backdoors, should be explored. For practical usability, it should be compatible to existing software. The latter could be realised using, e.g. virtualisation. This should initially be supported by means such as research funding. The development of these secure computers could additionally be encouraged, e.g. by procurement policy or by making it mandatory, e.g. in some sectors.

Related activities have been discussed in Heiser (Heiser 2013) and Castillo Vera (Castillo 2013b). We think the option goes far beyond the draft Network and Information Security Directive. The Commission ICT work programme addresses, however, the issue by demanding secure end-to-end security with a holistic approach (EUCO 169/13 ,Decision C(2013)8631), but we think building such hard- and software is a large and difficult project which is hard to solve within the usual size of EU-funded IT-projects. In any case, this option is not a short-term issue.

The following two measures could be transposed more quickly:

2. To address day-to-day risks of Cloud Computing, the use of checklists for keeping systems secure could be encouraged, the use of sufficient backups, etc. (cf. Jacobi et al. 2013b). The use of comprehensive security policies could be certified. Breaches should at least be reported to the certifying institution. In the medium run, certification could show the use of secure computers or secure virtualisation.
3. The EU could regulate that data from European citizens and businesses should only be managed by European companies with European management on computers residing in Europe. This is a radical option which could be used e.g. in negotiations. It means that a new balance between free contracting and privacy protection would be needed.

The latter measure would, of course, not help against backdoors in foreign equipment, but make copying and eavesdropping more difficult and illegal.

Other security related policy measures could be:

4. To create a realistic use of Cloud services, both business and private users could be educated to anticipate that providers lose data or are not available, so independent backups are needed, as well as fallback procedures.
5. To allow confidential processing of data in the Cloud, it could be estimated what such processing in remote tamper-resistant modules would cost when applied at large scale.

Finally, another measure on a different level could be:

6. The European Parliament could also investigate which steps to take to achieve a clean-up of the intensive spying activities of the US. The Parliament could support calls for US-internal activities. To quote two proposals by a US expert: "We need a special prosecutor... This prosecutor needs free rein to go through the NSA's files and discover the full extent of what the agency is doing, as well as enough technical staff who have the capability to understand it. He needs the power to subpoena government officials

and take their sworn testimony. He needs the ability to bring criminal indictments where appropriate… We also need something like South Africa's Truth and Reconciliation Commission, where both government and corporate employees can come forward and tell their stories about NSA eavesdropping without fear of reprisal." (Schneier 2013b, cf. the UN's investigation by Ben Emmerson, according to the Guardian(2013e)

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

Data protection is a fundamental right - as laid out in article 8 of the Charter.(European Union 2000, Article 8) Directive 95/46 is the legal instrument which elaborates this right. Whenever personal data are processed in provision of a cloud service, data protection law will be relevant.[20] The Directive lays out a series of rights for the data subject and a series of obligations which the controller must follow. The Directive does not necessarily prevent data being processed, but seeks to subject this processing to a series of rules and make it transparent to the data subject.

Challenges to data protection law can arise as technological development changes the possibilities and context of data processing. This brings into questions the presumptions around which the data protection framework was built. Cloud computing is such a development. (Article 29 Data Protection Working Party 2012, 4-6). Part 4.3.1. considers the difficulty in applying the Directive to the cloud. Part 4.3.2. considers the ongoing data protection reform (the Proposed Data Protection Regulation). Part 4.3.3. considers features of the Regulation which may address issues isolated in 4.3.1. The section concludes in part 4.3.4. with a brief comment on the significance of the recent vote on the Regulation in the European Parliament and a set of policy recommendations.[21]

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

Definition of Applicability of European Data Protection law and Jurisdictional Issues

In cloud services, the location of the data or service may not be known to either client or provider and provision of the service may take place across multiple jurisdictions. However, the Directive uses 'territorial' applicability criteria. Article 4 states that the Directive applies to activities of controllers which are; a) established in the EU, or b) utilise equipment based in the EU. This raises a number of issues. 1. The cloud provider might be recognized as the data processor – rather than the data controller – despite having significant control over the means of processing (see next section for terminology clarification). The lack of reference to the processor in Article 4 means the criteria applicability might not be met, despite the logic for the application of the Directive being present. 2. In the case of non-EU controllers, the definition of 'equipment' is key in establishing the applicability of the Directive. The idea of 'equipment' fails to describe the combination of infrastructure necessary for cloud service provision. (European Data Protection Supervisor 2012, 10-11). 3. Even where the Directive's application is clear, the location of a data controller outside the EU makes oversight, or punishment for transgressions of data protection law, difficult.

[20] Article 2(a) states: ''[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 [by] factors specific to his physical, physiological, mental, economic, cultural or social identity'.

[21] There are numerous types of cloud service and data protection law is extensive and complex. This contribution addresses only the general challenges posed by cloud computing to data protection law.

4. There may also be conflict of laws issues. Data controllers operating outside the EU will be subject to the laws of the states in which they operate. Obligations set out by such laws may contradict those laid out by the Directive.(Bigo et al. 2012, 44).[22]

Definition of Roles and Responsibilities

The Directive outlines a number of types of actor. Each actor has a set of responsibilities in ensuring all requirements in the Directive are fulfilled. There are three key actors (defined in Article 2). 1. The data subject is the identifiable natural person to whom any personal data relate (Article 2(a)). 2. 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' (Article 2(d)). 3. 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' (Article 2(e)). In the cloud environment, the cloud client has generally been held to be the data controller and the cloud provider to be the data processor.

However, in reality it can be difficult to identify actors.(Article 29 Data Protection Working Party 2012, 7-10) Particularly in relation to who is really controlling processing.(Hon et al. 2012b, 3-13) It has 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 a controller, other of the controller's duties may be more clearly located with those who would normally qualify as data processors – for example, ensuring 'appropriate technical...measures to protect personal data against...destruction'.(Directive 95/46/EC, Article 17) Even when roles are specifically allocated – for example in a contract – these may not match the reality of control.[23]

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

Cloud service providers may utilise infrastructure and sub-contracted providers located in multiple places. In turn, data may be made available to numerous locations. Accordingly, cloud service providers may rely on continuous, worldwide, flows of data. This may necessitate transfers of data outside the EU. In order to ensure that citizens' data remains protected, transfers outside the EU are only permitted in certain situations. 1. If the Commission has decided that the third state provides an 'adequate' level of protection (Article 25).[24] 2. If the transfer falls under any one of a list of exceptions in Article 26. 3. Provided the transfer is subject to a contract between two controllers or a controller and a processor. 4. Provided the transfer occurs based on Binding Corporate Rules (rules defining standard data processing practise within a company/group of company operating multinationally).(Article 29 Data Protection Working Party 2013)

[22] In relation to controllers established in multiple EU states, there may be problems in determining which Member State's law is applicable. Each Member State has a different transposition of the Directive.

[23] 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. In this case the distribution of responsibilities may be unsuitable for the cloud client's activity or be impossible to execute.

[24] 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.

However, the Directive was drafted with the presumption that international transfers would be limited, linear and easy to track. Each of the above options has drawbacks when applied to the cloud. 1. Only a limited number of countries qualify as 'adequate'. Accordingly, this exception is only of limited use and is geographically restricted.[25] 2. The Article 29 Working Party 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 most cloud transfers do not match. 3. Binding Corporate Rules offer a good solution when processing remains within a certain organization, but have little relevance if data goes beyond an organization. 4. Only standard contractual clauses elaborated by the Commission certainly meet the requirements of the Directive. There are only a limited number of such clauses and the variety of cloud services means pre-approved standard clauses may not always be relevant.(European Data Protection Supervisor 2012, 16-20)

No Binding Interpretation Mechanism

The challenges in applying the Directive to cloud computing remained challenges due to the fact that data protection law did not have the capacity to effectively adapt to technological change.(COM 2010/609/EC) This was partly due to the rigidity of the terms and concepts of the Directive itself. However, it was also due to the fact that European level interpretation mechanisms 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 is limited. Further, national level interpretation has had the counter-productive effect of leading to divergent approaches between Member States, fragmenting European data protection law.

4.3.2. 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, as has the social and economic importance of data processing. The legal context has also changed. The use of a Directive as the instrument of regulation has been limited 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 Treaty of Lisbon, for example, elevated the Charter to the highest level of EU law. Accordingly, in 2009, the Commission began a process of data protection reform. This process culminated with the 'Proposed Data Protection Regulation' – intended as a replacement for Directive 95/46.(COD 2012/0011/EC) At each step of the reform process, the challenges posed by cloud computing were key factors driving the reform.(SEC 2012/72/EC). The overall goals of the proposed Regulation remain essentially unchanged from those of Directive 95/46. Equally, the Regulation retains most of the Directive's concepts, principles and definitions. However, the choice of a Regulation means the framework will be directly applicable in Member State

[25] The Safe-Harbor agreement suffers not only from the above territorial limitation, but also from a lack of oversight and enforcement mechanisms.

law and despite general continuity, there is innovation in the Regulation of relevance to cloud computing.[26]

4.3.3. 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. 1. 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 ensure the applicability of the Regulation to any service where either cloud client, or cloud provider, is established inside the EU. 2. In Article 3, the Regulation also clarifies that 'offering goods or services to' or 'monitoring the behaviour of' data subjects inside the EU, will trigger applicability. Therefore, if the service provider is established outside the EU but offers services within the EU, the Regulation will apply.

Clarification of Roles and Responsibilities

The Regulation aims to readjust the definition of actors and roles. Changes attempt to clearly locate the actor which truly 'controls' processing, as data controller. 1. In Article 4(5), the Regulation states that 'the controller [is the entity which] alone or jointly with others determines the purposes, conditions and means of the processing'. The EDPS suggests that, if the cloud provider controls the conditions of processing, they could be considered as a 'controller'.(European Data Protection Supervisor 2012, 12-14) 2. In Article 24, the Regulation clarifies that; should there be more than one identifiable controller, there must be an arrangement between the controllers to ensure data protection rules are followed and data subjects' rights are guaranteed. Any arrangement establishing joint control should distribute responsibilities in line with the reality of control over processing.[27] Following a more targeted allocation of roles, the Regulation increases the responsibly and accountability of controllers and processors (the principle of Accountability is expressly mentioned in Article 22). Related to this, the Regulation introduces a set of novel obligations on controllers and a novel set of rights for data subjects. Certain of these may be of relevance to cloud computing.[28]

[26] It is important to note that our point of reference is the current draft of the proposed Regulation. This is only one draft in a legislative process which may undergo significant change.

[27] The EDPS notes, however; there may still be imbalances in power between cloud provider and client which prevent balanced responsibilities distribution.(European Data Protection Supervisor 2012, 13)

[28] For example, the controller must implement data security measures to ensure data are adequately protected (Article 30) and, in certain cases, to conduct a data protection impact assessment to isolate and minimize risks in advance (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).(European Commission 2012b, Articles 22, 23, 30, 31, 32 and 33). Article 17 gives the data subject the; '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 data. Article 17 also makes the controller responsible 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'. Article 18(1) gives the data subject 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'. Cloud services will thus be obliged to provide a copy of data in a transferrable format. The Commission will decide which format. Article 23(1) states: 'the controller shall...at the time of the determination of the means for the processing and at the time of processing...implement appropriate technical and

International Data Transfers

The Regulation still imposes limits on transfers of personal data outside the EU. However, the Regulation also proposes changes aimed at protecting data subjects whilst simultaneously loosening the formalities on cloud providers. 1. The regime proposed in the Regulation demands that both controllers *and processors* secure legitimation for transfers (Article 42(1)). 2. 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'. 3. 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) allows the extension of BCRs to external sub-processors. It should be noted that this option requires further clarification.[29]

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. 1. The Commission retains certain powers to clarify the meaning and application of a number of concepts and definitions. These powers 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.[30] 2. The Regulation outlines a central, binding, interpretation mechanism. This can be used when there are disagreements between DPAs as to the 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.

4.3.4. Recent developments and conclusions

As part of the legislative process, on 21st of October, an amended version of the Regulation (with 104 amendments reduced from 3999), was backed – with overwhelming support – in a vote in the European Parliament's Committee for Civil Liberties, Justice and Home Affairs.[31,32]

organisational measures and procedures [so that] processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'. This Article creates the obligation to take data protection rules into account at each step in the development of a data processing system – including in organisational systems. Article 23(2)then states: 'The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose'. This Article creates the obligation to ensure that the minimum level of privacy infringement is the default.

[29] There are criticisms of the approach in the Regulation. 1. Many of the mechanisms for allowing international transfers still require confirmation from the Commission whilst others will require significant elaboration before they become effective. 2. 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.

[30] The quantity and centrality of these powers has come under heavy criticism.

[31] The following documents show the Regulation, with proposed amendments on 07.10.2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[32] http://europa.eu/rapid/press-release_MEMO-13-923_en.htm, 'LIBE Committee vote backs new EU data protection rules' (last consulted 21.11.2013).

The draft Regulation voted on by the LIBE committee generally affirms the architecture and principles of the Commission's Proposed Regulation. However, certain of the amendments made to the initial proposal will be of relevance for the regulation of cloud computing. Two seem of particular importance.[33] 1. In relation to territorial scope, the Commission's proposal stated, in Article 3(1): 'This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union'. The Parliament's draft extends this Article with: 'whether the processing takes place in the Union or not'. The territorial scope of application of the Regulation would thus include the processing of personal data in the context of activities of a data controller's or data processor's establishment, even where this processing did not take place in the EU (for example, if data were processed in the cloud, EU data protection law would still apply).[34] 2. The Parliament's draft would also add more stringent provisions as to when data are transferred to third countries. In particular, if a third country were to ask a company (a cloud provider, for example) to disclose personal data processed in the EU, that company would first need the permission of the relevant European Data Protection Authority, and to inform the person concerned, before making the disclosure.[35]

This vote gives the mandate to the European Parliament's data protection Rapporteurs to negotiate with the Council on the legislative package. As soon as the EU Member States agree on a common negotiating position in the Council, inter-institutional talks can begin in earnest. It is the Parliament's stated wish that an agreement on the legislative reform should be reached before the May 2014 European elections.[36] In relation to the ongoing reform process, the following policy measures could be recommended:

- Support, and if possible expediate, the current process of data protection reform
- Support the choice of a Regulation as the legal instrument
- Support the strengthening of pre-existing individual rights in the Regulation
- Support the range of new rights offering further control to the data subject
- Support the range of novel obligations on the data controller
- Support clarification of data protection principles relating to cloud computing
- Support the accountability principle
- Be cautious with European level 'command and control' approaches.
- Support less rigorous consultation and notification requirements
- Support European level consistency and interpretation mechanisms
- Support the creation of the European Data Protection Board
- Support proposals which allow justified international flows of data

[33] The draft makes a number of other amendments which may have an impact on cloud computing. For example, Article 17 (the right to be forgotten) has been strengthened and the right to data portability has been linked with the right to access. The sanctions system for violation of data protection law has been strengthened – including fines of up to 5% of annual turnover. The data breach notification time has been relaxed – from 24 hours, to 72 hours. http://europa.eu/rapid/press-release_MEMO-13-923_en.htm, 'LIBE Committee vote backs new EU data protection rules' (last consulted 21.11.2013); http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20130502BKG07917&language=EN, 'Q&A on EU data protection reform' (Last consulted 21.11.2013).

[34] http://europa.eu/rapid/press-release_MEMO-13-923_en.htm, 'LIBE Committee vote backs new EU data protection rules' (last consulted 21.11.2013)

[35] http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20130502BKG07917&language=EN, 'Q&A on EU data protection reform' (Last consulted 21.11.2013).

[36] http://europa.eu/rapid/press-release_MEMO-13-923_en.htm, 'LIBE Committee vote backs new EU data protection rules' (last consulted 21.11.2013).

- Consider options to ensure the applicability of the Regulation where relevant
- Look into methods of accountability, oversight and enforcement abroad

4.4. Challenges in ICT governance

This section gives an overview over current debates about political ICT governance practices as they relate to cloud computing; describes the basic governance problems related to 3rd party data access and retention; relates assessments of the Safe Harbour regime; and indicates the problematic relationship between the current EU data protection legislation process and ongoing EU-US free trade negotiations.

4.4.1. Overview: A sea change in ICT governance

With regard to the governance of globalized ICT, the world seems to be at a crucial point of political choice. The Internet has so far been governed by a regime of technical, organizational, legal and political measures established under relative U.S. hegemony. Oversight of the technical structuration of the Internet through such systems as the IP address system, the domain name system, and the continuing development of the TCP/IP protocol have been placed with U.S. based organizations. Much of the technology for safeguarding and communicating information has been developed in relatively opaque modes of cooperation between the U.S. private and military sectors. And most importantly, much of the server and network infrastructure that underpins the Internet on a daily basis has remained based in the U.S. and is therefore governed first and foremost by U.S. legislation.

Earlier, critique of this governance regime was generally only voiced from outside the Western hemisphere. Europe for its part has had occupied a special place in the global landscape as the 1995 Data Protection Directive has installed higher privacy standards than that of other nations. And based on a general trust in the benevolence of the U.S.-centered Internet governance regime, Europeans have been able to believe that the Safe Harbour agreement with the U.S. projected the same protection level into their relationships with U.S. based ISP's. But with the Snowden revelations described earlier, the tensions underlying U.S. hegemony have become illuminated. One the one hand, the question of the strategic interests of other nations and peoples have moved to the forefront of mainstream political discourse, also in Europe. The trust underlying the Safe Harbour regime – and by extension the entire perception of Europe's unique position within global ICT governance – has been fundamentally shaken. "Data sovereignty" - a term which earlier only circulated among non-Western autarchic regimes – has gained currency in Europe with rising concerns about the ability of Europe and its member states to provide adequate privacy for the citizens in the digital world (Bowden 2013c). On the other hand, the discrepancy between the universalist ideals of the ICT community and the deep real-world reliance on U.S. supporting structures have produced an impulse towards increased internationalization of the Internet's underlying frameworks (Wilhelm 2013). The leaders of a number of key organizations responsible for coordinating internet Infrastructure, for example, recently released a common statement in which expressed "strong concern" about the revealed surveillance practices and called for accelerating the globalization of central infrastructure functions (specifically ICANN and IANA) (Montevideo Statement). And at the latest annual meeting of the Internet Engineering Task Force, the IETF took upon itself and other

stakeholders to act to better protect Internet users from pervasive surveillance through e.g. the revision of protocols and spread best practices (IETF 88, 2013).

While the current debate about the trustworthiness of Internet based communication and cloud computing focuses very much on the actions of the NSA and its allies in the European intelligence community, signs of the erosion of trust in the existing governance regime have actually been visible for years before that. Security and privacy have 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 2013a, b). A public consultation carried out by EC in 2011 thus showed agreement from 90% of its respondents that with cloud computing "liability in cross-border situations is unclear" (EC 2011, 1), while a number of respondents voiced the opinion that "international data transfer compliance mechanisms do not provide effective data protection for customers or legal certainty for companies" (EC 2011, 7). Focusing too narrowly on U.S. surveillance practices also obscures the picture with regard to our own domestic intelligence practices. As we shall see below, while the U.S. is unquestionably at the forefront of surveillance technology and seemingly the leading proponent of blanket surveillance and while the European data protection legislation in pure form embodies stronger data protection principles than those encased in U.S. legislation, we cannot from this conclude that the EU is a safe haven of privacy protection. Member states have their own intelligence operations and national law enforcement agencies, which have basically the same need of gaining access to the information of companies and private citizens as their U.S. counterparts. While concrete practices for obtaining such access may be less high-tech, legal provisions to provide are not far behind those of the U.S. if at all. At EU level, counter-terrorism legislation also is in a difficult relationship with data protection.

The lack of trust in cloud computing and similar expansions of Internet technology poses difficult strategic questions and dilemmas, which divide actors who see the problem from different perspectives. The data protection legislation proposal presented by Commissioner Redding takes a "hard" line with regard to the establishment of trust with a focus on control and enforcement; a line which was recently amplified by Civil Liberties MEPs proposing, for instance, to up fines from 1 mill. EUR or 2% of annual turnover to 100 mill. EUR or 5% of annual turnover, "whichever is the greatest" (Dasilva 2013:3). This line clashes with the "soft" line proposed by Commissioner Kroes. Seeing the role of government as being: "to ensure that European achievements, such as effective data protection and the Single Market, do not clash with cloud computing" (Kroes 2011), the Commissioner developed a "cloud-active" (Kroes 2011) EC cloud strategy aiming to establish trust in cloud computing through cross-sectoral collaboration. The heart of the political matter is, of course, the issue of cloud-driven economic growth versus caution in the face of threats to citizens' rights.

4.4.2. 3rd party data access and retention

From a technical and legal point of view, the core of the discussion is the matter of governing 3rd party data access and retention.

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. 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).

Beside different national laws, there is a number of ways to access data on a European or international level. The first one is the Council of Europe Cybercrime Convention. It 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. It 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. The second way that can pursuit by law enforcement is to gain access data 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.

Finally, 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.

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 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 (U.S. Senate, 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 (FISA) 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 2013c). Others, however, argue that while U.S. operatives may only legally 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). Constitutional or not, the provisions for surveillance in the FISA legislation provide de facto an almost unlimited space for manoeuvre with regard to the surveillance non-U.S. persons, including provisions for "expressly political surveillance over ordinary lawful democratic activities" (Bowden 2013c, 19). And while future political or court decisions within the U.S. may render the NSAs surveillance practices explicitly illegal, under the current state of affairs "there are no privacy rights recognised by U.S. authorities for non U.S. persons (**T**he difficulty of governing Cloud Computing, which arises from the plurality of jurisdictions involved, is well-known. But over the past year the world has gained insight into trans-legal (if not illegal) practices of third-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. The proposed regulation seeks to provide means for the enforcement of European privacy policy in international markets. Currently, it seems that this approach has support in the European Parliament.

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 Safe Harbour. The benefits of greater enforceability are obvious. 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. Strong European leadership may alleviate this disadvantage. 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. 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. And while "Europeanisation" of cloud governance may be preferable to other tendencies of Member State actions, which point towards nationalisation, there are real risks of a global polarization that may spill from matters of ICT governance into areas of economic, strategic and perhaps even military collaboration.

Figure 9: Governmental authorities' access to data in the cloud. Source: Maxwell and Wolf, 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

One pathway forward, which may meaningfully supplement the proposed strengthening of Europe's position, may be a true internationalisation of governance structures underlying the functioning of the Internet. So far, the world has relied on an Internet governance regime largely founded on U.S. hegemony. But now, we see calls for the severance of historical ties between core Internet infrastructure and the U.S. military-industrial complex. If Europe is ready to answer this call, it may contribute to a sea change in ICT governance

and a global step forward towards the realization of the liberating potentials of a neutral, open Internet., 23).

In Europe, the question of legality goes deep as well. European cloud providers were quick to see a silver lining in the Snowden 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 provides a rather simplified 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 on the following page) 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 ruling is still forthcoming, but an opinion issued recently by the Advocate General states that the data retention directive "is as a whole incompatible with article 52(1) of the Charter of Fundamental Rights of the European Union" (Villalón 2013: 31) The data retention, in other words, seems not to live up to the criteria to be met when imposing limitations on citizen's rights.

4.4.3. The Safe Harbour agreement

The 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. 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 (Bowden 2013c; 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, which MEPs suggest to amplify even further. Such enforcement measures, along with more detailed demands for documentation of data protection practices, seem to represent a step forward with regard to trustworthiness established through control and enforcement capacity in comparison with the existing Directive (Brodies 2012). However, as has been discussed in detail in chapter 3 of this report, enforcement of privacy principles is perhaps hopeless in a sector, which delivers its services through the use of infrastructures systematically undermined by the NSA (Bowden 2013c, 13-14). Prudence would dictate that lessons learned from the weaknesses of the Safe Harbour regime should be applied to the concept of BCR-for-controllers, which might be seen as a governance backdoor (Bowden 2013c, 25). And perhaps the only pathway leading to sustainable solutions lies in the development of uncompromised technologies rather than legal frameworks.

4.4.4. International harmonization?

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 for Europe, these otherwise often opposing interests overlap. There might be good reasons for European institutions and European cloud initiatives to establish a high-level dialogue with those technical Internet governance institutions wishing to work for a true internationalization/globalization of the Internet's underlying infrastructure as expressed in the Montevideo statement and elsewhere (Montevideo Statement 2013; IETF 88, 2013)

Notably, a draft resolution created by Brazil and Germany concerning the right to privacy in the digital age was recently passed in the UN (UN 2013) and will be subject to a vote in the UN General Assembly around the time of the publication of this report. This draft expressly aims at strengthening the obligation of states not only to "respect", but also to "protect" (UN 2013, Art. 4(a)) citizen's rights to privacy – a formulation emphasizing active enforcement (Goodman, 2013). This emphasis is bound to create opposition, but it may be precisely the route that the EU could take. Of course, whether the UN is the most efficient forum for creating the governance structures necessary for such enforcement can – and will – be debated.

4.4.5. 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. Already before the recent events, there was an 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. 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 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. 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.

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.
- Scrap the Safe Harbour agreement, avoid other entirely trust-based solutions
- In lieu of international data protection governance agreements comparable to the European data protection regulation in-the-making, uphold the principle within the regulation of extraterritorial applicability of the regulation
- Ensure hands-on extraterritorial enforcement of European privacy principles (see legal section).
- 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 (see security section).
- 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.

4.5. Contractual issues and customer rights

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 section 4.3). 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.

4.5.1. 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.

- 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.
- 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.
- 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.

IaaS v SaaS: There is less variance in the terms and conditions offered by IaaS than SaaS; IaaS services are more similar than SaaS.

4.5.2. Common main features and issues in Cloud Computing Contracts

Cloud computing assumes that data will be stored and processed across multiple data centres – even the provider and user of the service may not be aware of where data are processed. Accordingly data may be processes in multiple **jurisdictions**. This can introduce a degree of jurisdictional uncertainty unless (and even if) clarified in the TOS.[37] Often, the **choice of law** is left to contracting parties. The choice of law may provide certain advantages to the cloud provider. For example, Californian courts are more likely to recognise disclaimers and limited liabilities as stated in the TOS, than EU courts.[38] For example, Bradshaw et al (2010) note that a number of cloud service providers seek relatively short limitation periods in which a customer must bring a claim in respect of a service. Consumers are likely to be protected from such limitations under EU consumer protection legislation[39].

The Rome I Regulations are the EU legal rules establishing applicable law in contractual obligations (Regulation 593/2008/EC).[40] Article 3 recognises that applicable law can be

[37] 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 either the customer's local law or no choice of law.

[38] 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.

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

[40] 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.

chosen by the contracting Parties. Where no law is chosen, Article 4 provides mechanisms for determining applicable law.[41] A number of factors are taken into account under Article 4, however, the overarching idea is that the contract should be governed by the law of the country with which that contract is most relevantly connected. Unfortunately, establishing a real and substantial connection between jurisdiction, contract and the parties involved, can be interpreted widely. Some considerations in choice of law for cloud service provision may include: the nature and quality of their commercial activity in the jurisdiction; 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; the paying customers or end users resident or domiciled in; the location of the cloud service; the location of the data (or data centres); the location of the service provider; whether the service provider has a business presence in the jurisdiction; whether the service provider advertises, markets or solicits business in the jurisdiction. Article 6 of the Regulations provides for consumer contracts, and would generally apply the law of the country in which the consumer has their habitual residence.

Another challenge is provided by the **data transfer and data location outside of the EEA.** It is often the case that cloud service providers will transfer data to different data centres. These locations may in different jurisdictions including outside of the EEA. The identification of an exact location for data may be difficult. 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. It is discussed in section 4.3.

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. The key concerns of organisations entering into contracts for cloud services relate to losses associated with misuse of data, service interruptions or failure, and data integrity or loss. Cloud service providers may attempt to exclude liability by introducing prejudicial clauses into their service agreements. They may also try to exclude certain types of liability by choosing a preferential legislative jurisdiction. Bradshaw et al have also noted significant differences in the form of liability excluded by cloud provider depending on the country of origin of the provider.[42] Despite service provider attempts to disclaim liability, EU law

[41] 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."*

[42] 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. 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

typically does not allow the exclusion of liability in the same way as US law might. Article 23 of the Data Protection Directive addresses the issue of compensation for persons suffering damage as a result of unlawful processing or of an act incompatible with national data protection law. Persons suffering such damage are entitled to compensation unless the controller can prove that they are not responsible. Under the current Data Protection Directive, the data controller is responsible for processing carried out by the data processor. The proposed revisions to the Data Protection Directive may apply responsibility directly to the processor (for details see section 4.3).[43]

Acceptable use policies (AUPs) are a deterrence mechanism widely used by cloud service providers to protect themselves in the event of misconduct by their clients or customers of clients by prohibiting specific activities – for example using the service for bulk unsolicited commercial email.[44] Bradshaw et al (2010) note that AUPs for cloud service providers are largely homogenous in the set of activities and behaviours prohibited. However, many AUPs use language which is unsuitable to the client's customer base – for example clients may have multiple customer constituents. In this case, 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.[45] **Service Level Agreements (SLA)** elaborate the level of service to be provided and typically include mechanisms for auditing service delivery and compensation for underperformance. SLAs typically contain the following: 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; a compensatory mechanism for compensating clients in the event of underperformance.[46] Failure to meet performance levels in cloud service agreements can result in significant losses for clients. UK case law has found that contractual attempts to exclude such losses may not be sufficient to insulate the service provider from liability for such losses.[47] In most cases standardized SLA are used and only customers with bargaining power can negotiate individual SLA. In principle, the EU **Unfair Terms** Directive (Directive 93/13/EC) requires that contracts must be drafted in such a way to prevent the imposition of terms prejudicial to consumer rights. It introduces the notion of "good faith" in order to prevent significant imbalances in the dealing of consumers and suppliers. Unfair terms are not

indemnifications from clients against any claim against the provider arising from the client's use of the service. Hon et al (2012) note that clients who are in a position to negotiate their contracts, sought (and in some cases succeeded) to avoid such clauses relating to liability and indemnification. They note 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.

[43] 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.

[44] Other examples include using the service for 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 or any illegal or unauthorised activity including infringement of intellectual property of others.

[45] Where AUPs (and indeed TOS) require clients to affirmatively prevent '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.

[46] 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.

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

binding on consumers. Article 5 of the Directive requires contract terms to be drafted in plain and intelligible language and states that ambiguities will be interpreted in favour of consumers.[48] 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. It 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."*

Bradshaw et al (2010) found that, in standard form contracts, many cloud service providers reserved the right to **change contract terms** unilaterally. Such variation may be communicated by reference to an updated version of the contract on the provider's website. In such an instance, continued use of the service is considered acceptance.[49] In case of a dispute, contracts for cloud service provision will typically include a provision for **dispute settlement**. The jurisdiction relevant for dispute settlement will typically be the same as that providing the applicable law. 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. At the moment there are initiatives towards a simplification of dispute settlements, including also online dispute procedures.[50]

Contractual issues related to **termination** depend on whether the contract comes to a natural and expected conclusion or is terminated due to breach of contract.

In either case, the contract should make provisions for termination and the consequent handling of the client's data. 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. If the contract expires naturally, there may be an auto-renewal clause – this is are common and typically involves an advance notification system.[51] In relation to 'unnatural termination', the service contract usually specifies a number of termination events.[52] The acquisition of

[48] 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

[49] 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.

[50]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.

[51]Some negotiated contracts may seek longer terms with guaranteed renewals for reasons including continuity of service and guaranteed pricing.

[52]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 cloud service provider or even change of control is typically not addressed.[53] In heavily regulated sectors, clients may require the option of termination where such is requested by a regulator. The treatment of data on termination is a key issue and is often cited as primary factor in vendor lock-in concerns (see also section 4.7.1). There are three main issues: 1. data preservation following termination – the client will want to ensure they have reasonable time to access data. Bradshaw et al. (2010) note that cloud service providers deal with data preservation following termination in three ways: 1. provision of a grace period at the end of a service contract; 2. immediate deletion at the end of the service agreement; 3. through a hybrid approach neither obliging the deletion nor preservation of data, nor undertaking to delete data and offering a grace period at their discretion.[54] 2. Data transfer - the client may want support transferring their data or applications to a new service. The transfer of data is a significant concern of clients. There is a worrying dearth of tools made available for clients wishing to transfer data to new services.[55] However, not all portability issues are initiated by the service provider. In some instances, clients require customisation that results in migration and portability issues. 3. Data deletion following termination – the client will want to ensure that their data has been deleted. This may include – although this is not often explicitly stated – the deletion of metadata and data replicated for the purpose of system performance (incl. caching).

4.5.3. Contractual issues related to security

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

[53]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.
[54]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.
[55]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

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. An emerging contractual issue in this context is that 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 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.

McDonagh (2012) identifies two areas of law with respect to the **security of data** in the cloud: 1. obligations under data protection legislation, an, 2. access to data for law enforcement purposes. This section focuses on the first. For the latter one see section 4.4.

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 into 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 (2012) provide a detailed list of 14 safeguards relating to the controller-processor relationship. 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 related to standards and best practice frameworks including PCI-DSS, ISO27001, ISAE3402[56] and COBIT are common assurances for security in IT and increasingly cloud computing and clients may contractually require cloud service providers to achieve and maintain them. While 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.

4.5.4. 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 exist 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.

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.

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 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 (e.g. Directive 96/9/EC, Directive 2001/29/EC, Directive 98/84/EC, Directive 2006/116/EC, Directive 2009/24/EC, Directive 2000/31/EC, Concil Decision 2000/278/EC).

The liability of Cloud service providers for illegal content uploaded by their clients is dealt with by the Copyright Directive (Directive 2006/116/EC) and the Electronic Commerce

[56] The international standard ISAE3402 replaced the globally used US standard SAS70 in 2011. ISAE3402 is a standard for reporting on controls at service providers.

Directive (Directive 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. 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 (Directive 2006/116/EC, Article 5). 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. Article 12 describes the conditions under which mere conduit or caching is exempted. 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. 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. 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.

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 (Reed 2010). 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.

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. In December 2012, 25 EU Member 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. 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.

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.

4.5.5. 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. 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. Similar to that most of the existing standardized SLA show such features.

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

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.

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 2001).

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

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. Above that, research suggests that trustmarks have the greatest effect on perceived trustworthiness in an Internet context, 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 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.
- 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 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.

4.6. Competitiveness of the market

The competitiveness of markets is a crucial point for the further development of Cloud Computing in Europe. It is crucial for users, who would benefit from competitive markets in terms of price, quality 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. Based on the fact 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. In the course of the project five challenges were identified that are specific for Cloud or have at least a high significance for Cloud, which are explained in the following. There are many more challenges influencing the competitiveness, partly interrelated to the one's discussed here, but as outlined the focus is on the most important one's from the Cloud Computing perspective, but there are others, which are partly interrelated to the issues discussed here.

4.6.1. Vendor lock-in

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 as indicated in section 4.1.1, 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. Similarly, customer-driven customisation may result in lock-in as the customisation impacts interoperability. It is clear from the 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 4.5.2 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. Application lock-in typically occurs where an application has been designed 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 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 as outlined before. In case of standards there is a strong tendency in the IT industry towards de facto standards set by a few number of globally acting companies, mostly of US origin (see 4.1.1). The same argument is valid in the case of interoperability, which would at least ease the problems of communication and interaction (see also 4.1.1).Though data portability is addressed in the draft of the new regulation on data protection, there are further points that need to addressed at the legal level (see 4.5.2).

4.6.2. Market fragmentation

The fragmentation of the European market is an issue for both, users as well as providers of Cloud Computing. Nevertheless, in the past the discussion on the fragmentation often focussed on the disadvantages 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 customers, business user as well as consumers, because it also relate to issues like the fragmentation of the regulatory framework. However since parts of this broad spectrum are already addressed in other sections, the focus here is on challenges related in particular cross-border payments and transactions as well the harmonization of the regulatory framework. Though many of the problems within cross-border transactions and payments were already addressed for example by the eCommerce directive (Directive 2000/31) or the single payment areas (SEPA), there are challenges left. Firstly there are a few challenges that are specifically posed by Cloud Computing. A good example 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 are raised and cannot be reclaimed. In case of other US firms that also open subsidiaries in Europe like Amazon or Google, it must be stated that they do so after achieving a certain size and structure (including legal and tax departments). 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). Secondly, there are other challenges due to different implementations of existing measures by the member states, which may require further harmonisation. A first step regarding this is the planned regulation on data protection. 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 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). Given the announcement of the European Council in October 2013 on the

single, digital market until 2015 (EUCO 169/13), it will be a question to which extent such harmonisation take place. Beyond this it should maybe also noted in this context that cultural diversity (e.g. languages) should not only be considered as a problem, but also a chance, if it is perceived in the right way. It can also create innovation as shown by the example of Skype that was invented to circumvent the diversity of the European telecommunication system.

4.6.3. Lack of innovative, fast-growing companies

The lack of innovative, fast-growing enterprises refers to "overaging" of European companies even in high tech sectors, which is considered to be another reason for the lagging behind in productivity (Phillipon/Veron 2008). It addresses a broad set of issues dealing with challenges and issues for providers, but it is strongly intertwined with the market fragmentation. The set of issues and challenges addressed here 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. Additionally, the discussion is also often enlarged by a general discussion on the entrepreneurial culture, which 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. 2010, 184-185). Detailed analyses even show that the differences between the member states vary strongly (Eurobarometer 2010). Beside market fragmentation 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 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 by either older European or US companies (Veugelers et al. 2012, 9-12). A 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. Especially the software and IT service as well as the internet sector are affected by it (Turlea et al. 2010, 75; Turlea et al. 2011, 55). Another 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 procurers in the field, because 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). An example for this is the SBIR program in the US, where the state as procurer offers small companies the chance to develop innovative solutions desired by public agencies. 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). 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. Since then 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, despite the long time and several initiatives and the lack of improvement, 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. It needed coordination of RTI and industrial policies through the Office of the Chief Scientist (OCS), tailored instruments like YOZMA, support through capacity building measures for example in human capital and finally perseverance. (Breznitz 2006; Breznitz 2007). It underlines 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.

4.6.4. Broadband coverage

Availability is a crucial precondition for the success of Cloud Computing and one major aspect of it is the existence of enough bandwidth capacity. Though Europe has made some progress in broadband penetration due to the different initiatives in recent years, a closer look on the situation 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, which creates imbalance for the chance to exploit the potentials of Cloud Computing (EC 2013, 46). Even more critical is that 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%). Other NGA technologies like vDSL or Docsis 3.0 only have limited perspective in further grow of bandwidth beyond 100 Mbps. In case of the high speed mobile access the situation is little better with 26,2% coverage of LTE in Europe (SWD 2013/217/EC, 72), but both details pose the question if this is sufficient for a heavy utilisation of Cloud Computing as desired. Though there is no clear answer in the current research, which bandwidth for fixed and mobile networks is needed, 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. There is the fact that the further deployment of FTTB/H technologies would require a high amount of further investments, which raises the question how to finance it in particular for telecommunication providers. Neither increased prices for customers nor usage fees from service provider are desirable. The first approach may lead into a growing digital divide including a lower utilisation of Cloud Computing. The consequences of the latter approach are discussed 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, it could negatively impact the competitiveness of the market and thereby the overall potentials and impacts of Cloud Computing. Nevertheless, there is also the legitimate question how the telecommunication providers should finance the further development, which also needs to be addressed.

4.6.5. Lack of skilled workforce

The development of the human capital base is a factor, which is in a mid and long term perspective a necessary framework condition influencing the competitiveness of Europe in Cloud Computing. 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. But they 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 well researched by many studies on the member state or EU level (Korte et al. 2009), there is no 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 addressing the increase of skilled IT labour force as well as the pillar six of the Digital Agenda, which 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 skilled workforce in alternative ways. One example could be to include, beside women, other groups like the growing number of elderly people or young students that stopped formal IT education. 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 a different formal degree. Another point is that there is lack of knowledge how the requirements for skills will change in the next years. It refers to two challenges. The first is the change of requirements caused by Cloud Computing and other technologies such as Big Data. Though this partly researched, in particular for SME using Cloud Computing (Laugesen et al. 2011) and addressed 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 challenge is the possible change of skills requirements caused by a growing number of young people that are familiar with all kinds of digital technologies, which may impact skills requirement in the future.

4.6.6. Conclusions

In case of vendor lock-in 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, it is necessary to limit the possible negative aspects by addressing the related issues. This can be achieved by the introduction of rules and processes for data portability as well as by the support of technical solutions enabling migration and portability. From that point of view the following policy measures can be considered:

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

Market fragmentation includes many aspects ranging from the regulatory framework to socio-cultural aspects. As outlined some are already addressed in other sections of this report, while others like cultural diversity should maybe be not only considered as problem, but also a chance for Europe. The European Council set recently the target to achieve the single digital market by 2015. Therefore both problems for cross-border operations as well as the lacking harmonisation of the regulatory framework need to be addressed. The resulting policy measures could be:

- 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. However the analysis has shown in each of these aspects different challenges that need to be addressed. Based on that possible policy measures can be identified:

- 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.

The vision of a society utilizing Cloud Computing will raise future requirements regarding broadband 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 challenges of the imbalanced development within Europe as well as of the need for a further development of NGA technologies and how to finance it. Possible Measures 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 as well as 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 on developer as well as

user side. Given the fact that there is already a lack of qualified personnel identified in Europe, there is strong need for further actions in future. Measures could be:

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

5. SOCIAL NETWORK SITES

Social network sites (SNS) bear great potential to enable individuals in articulating and showing their social networks in a novel form of digital environment. Various definitions of SNS (or similar notions, often used synonymously, like social networks, social network[ing] sites or services or platforms, see Mack et al. 2007; Richter/Koch 2007; Schmidt 2009) exist that address this characteristic. Ellison and Boyd (2007) provide a prominent definition, that offers a broad view on SNS: "A social network site is a networked communication platform in which participants 1) have uniquely identifiable profiles that consist of user-supplied content, content provided by other users, and/or system-provided data; 2) can publicly articulate connections that can be viewed and traversed by others; and 3) can consume, produce, and/or interact with streams of user-generated content provided by their connections on the site." (Ellison and Boyd 2007, 158)

The broader view of this definition allows including a wider set of services and applications (such as photo or video-sharing, blogging or news aggregation tools etc.) referring to the increasing role of sharing and creating content. It also highlights the platform character of contemporary SNS with a variety of additional features integrated that reinforce their rapidly expanding functionality. In line with this view, the following major characteristics of SNS can be identified (Boyd/Ellison 2007; Ellison/Boyd 2013; Nentwich/König 2012):

- A user profile, i.e. a unique web page providing details of a user, serving as the main (bi-directional) access point to the SNS environment. Profiles are central network nodes, which can be addressed through various channels.
- A public (or semi-public) display of connections; i.e. a list of contacts (e.g. friends, colleagues, etc.) showing the connections between the user and his/her contacts.
- The option for users to navigate across those connections (e.g. viewing profiles that are associated with the list of contacts).
- Communication and interaction features such as instant messaging, chats, bulletin boards, etc. to interact with other users and/or user-generated content.

These main (interrelated) characteristics build the baseline for most SNS functionality. Although many additional features exist, they mainly ground on these core components.

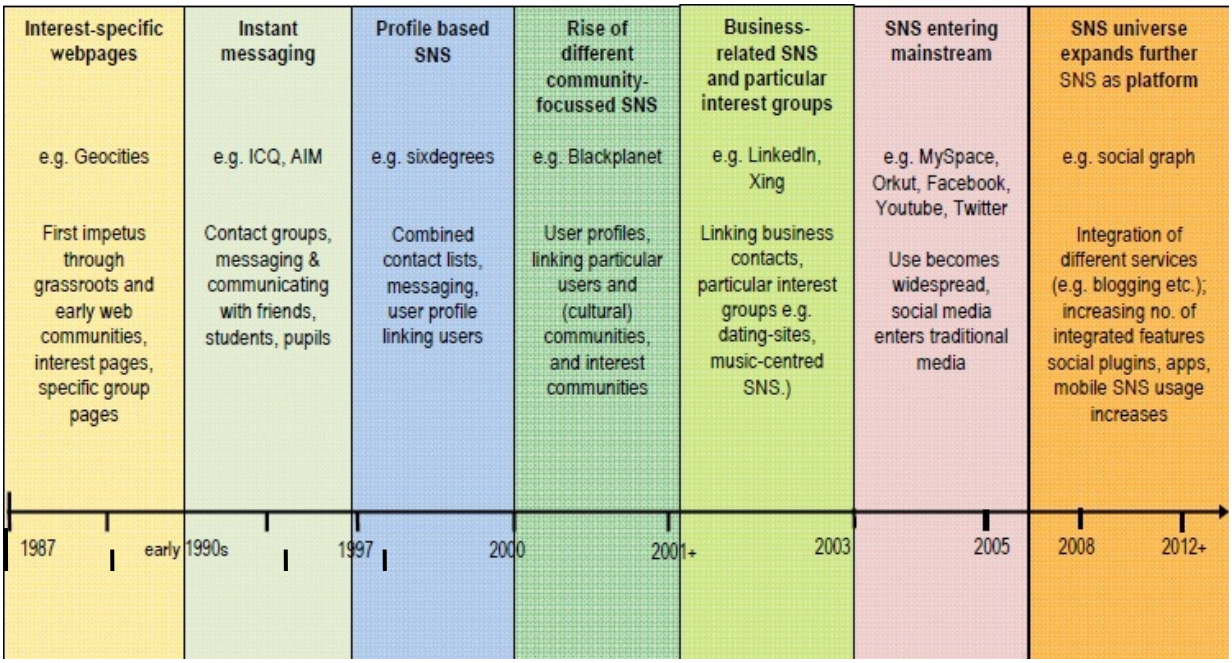
5.1. State-of-the-art

Although they are a relatively novel phenomenon, Social Network Sites have their beginnings already in the late 1990s. In 2003, SNS became more widespread and with the occurrence of Facebook in 2004, SNS quickly turned into a global phenomenon. Today, SNS usage is among the most popular internet activity with Facebook as the leading network worldwide. With 229 million active users merely in European countries, Europe is Facebook's biggest market. The development of SNS from a niche application towards a mainstream phenomenon happened in a relatively short period of time. Figure 10 provides some insight into the history of SNS and main stages in this development.

Already during the late 1980s/early 1990s, first impulses in the development towards contemporary social network sites occurred. Early web community pages (such as Geocities as most prominent during that time) and interest specific sites enabled novel forms of

communication that slightly changed the web landscape. Early adopters such as grassroots organisations and idealistic communities (e.g. Friends of the Earth or other environmental activists) made use of online community pages to exchange their visions and ideas. These sites occupied small niches in the World Wide Web where people started to exchange thoughts and ideas based on common interests. They represent early examples of SNS.

Figure 10: SNS evolution from niche to social mainstream



With the increasing use of communication tools such as chat rooms and instant messaging (e.g. ICQ, AIM), the next important development stage was initiated. These messaging services fostered synchronous and more lively communication. To some extent, they vitalized the widespread but loosely bound online communities and provided new options to establish connections between community pages. IM services such as ICQ allowed users to create contact lists and group them e.g. in circles of friends or similar. These possibilities played a crucial role in the further development. With the increasing role of user profiles to describe the characteristics of a particular user SNS began to take more concrete shape.

With sixdegrees.com, the first real social network came into being in the late 1990s. It was the first service combining different features such as contact lists, instant messaging and user profile as main entry point which is today state-of-the-art in most SNS. This also enabled the integration of previously separated services such as chatting, instant messaging and networking in a single SNS environment. Although sixdegrees had several million users, it failed to establish a sustainable business. Hence, it had to shutdown in 2000 despite of its leading role in the evolution of SNS. However, the concept of profile-based SNS remained and evolved further. From the year 2000, an increasing number of different community-centered SNS started, which supported several combinations of profiles and contact lists aiming at connecting users, e.g. based on their cultural backgrounds (e.g. AsianAvenue, Blackplanet) or on particular interests (e.g. dating sites such as match.com). In the next wave, SNS became increasingly attractive for commercial actors and networks focusing on business-related networks (e.g. LinkedIn, Xing) became more relevant and widespread. At the same time, there was a significant increase in SNS

focusing on particular interests (e.g. hobbies, sports, travelling, etc.). Most prominent at that time was MySpace – the formerly most popular SNS worldwide that initially served as network for musicians and their fans.

Since about the year 2003, a variety of new sites and services appeared and SNS steadily turned into a mainstream phenomenon. In South American countries (especially in Brazil) Orkut became a very popular network and MySpace had its highest usage rates during this time. Also today's major player Facebook entered the stage during that time and quickly expanded on a global scale. Concurrent to the widespread diffusion and usage of SNS, user-generated content and social media in general boosted worldwide. As a consequence, services such as blogging, content-specific platforms (e.g. photo/video-sharing, Flickr, YouTube, etc.) have been integrated more deeply into SNS environments and are nowadays integral parts of several SNS.

Nowadays SNS can be seen as part of social mainstream shaping the Internet experience of many users worldwide. Major players like the ubiquitous Facebook or Google+ count several hundred million users57. In addition to the major operators a variety of specialized network sites exist with different usage contexts ranging from dating or friend seeking to professional use such as job seeking, education, business contacts as well as in science and research (e.g. LinkedIn, Xing, Yammer, Academia.edu, ResearchGate). As SNS evolve fast as regards usage and scope of applications integrated, also services such as micro-blogging (e.g. Twitter), video platforms (e.g. YouTube), social bookmarking services (e.g. Delicious) or news aggregation tools (e.g. Reddit) can be defined as SNS.

The phase of integration is still on-going and SNS increasingly serve as platforms for many services and applications that become more and more integrated into SNS environments. This transformation of SNS into platforms is not least driven by the rise of so-called social plugins that also trigger further expansion of SNS environments across the (outside) web.

5.2. Structure and functionality

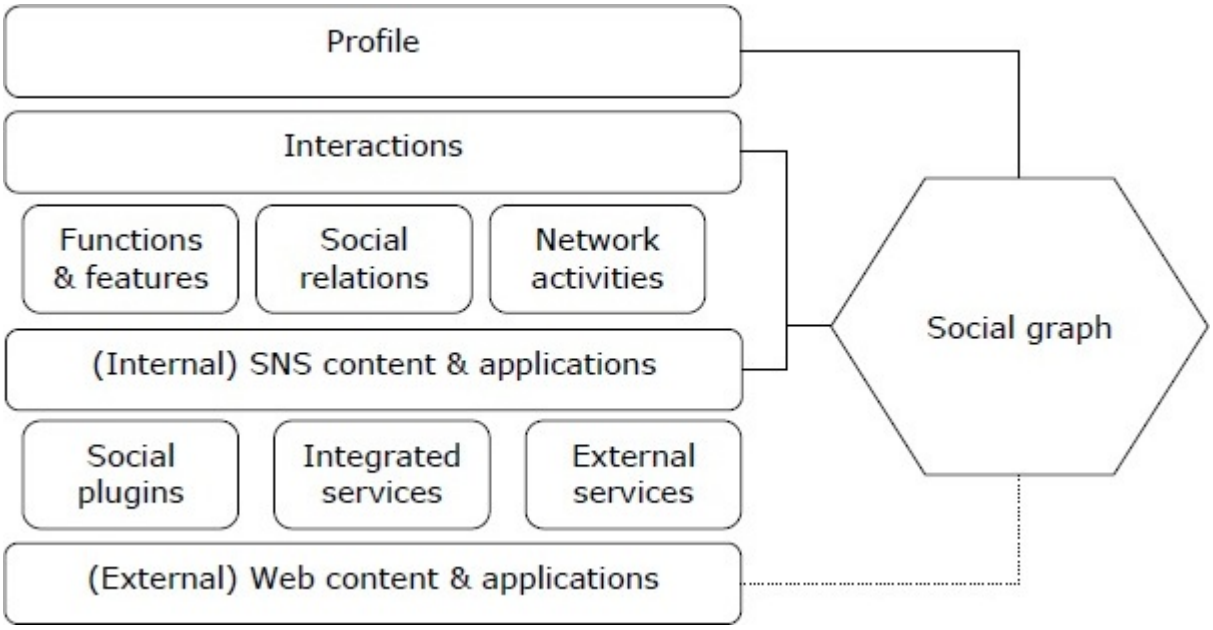
The rapid expansion of SNS revitalized McLuhan's (McLuhan 1964) "the media is the message": merely using social media entails that information is disclosed within the network. Even if a user does not actively post information in his profile, the sheer presence of the profile is information that becomes processed in the SNS environment. With its networking character, SNS environments have a self-amplifying dynamic inherent in its design: the number of users is likely to grow if networking among them increases. Even if a user would intend so – the very mechanisms of SNS make it relatively difficult to remain in traditional modes of interaction, i.e. one-to-one relations. The networked environments inherently enable and stimulate one-to-many relations and interactions from the individual user's point of view. This enables a variety of new interaction modes among users (one-to-one, one-to-many and few-to-few, many-to-many) and between users and software agents (searching; proposals based on semantic algorithms). In addition, the integration of

[57] Facebook seems to have reached a billion users http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html Google+ about 500 million user http://techcrunch.com/2012/12/06/google-shares-numbers-more-than-500m-upgraded-235m-active-across-google-135m-in-the-stream/

external applications (such as micro-blogs) increases the density of communication among those not present in the same place.

Despite of the many different SNS, most of these systems are similar regarding their basic structure and functionality. The very idea remains: to enable (dynamic) relations between different entities. The implementation of this idea consists of many different components. Figure 11 shows a simplified model of the main building blocks of a typical SNS structure.

Figure 11: Main building blocks of a typical SNS structure, Source: Strauß/Nentwich (2013a)



The user profile plays a particular role as it represents the main access point to all the SNS functionality. Profiles can be seen as enhanced calling cards of individuals (or in several SNS also organizations and groups) with two core functions always present: identity management and contact management (Richter/Koch 2007). A user profile maps—more or less publicly accessible—the contacts of a person and enable access to further members on various paths, i.e. networking. Via their profile, users are linkable to others and visible inside (and outside) the network environment. Usually, a profile contains the following (pre-structured) information: Contact information (e.g. address, e-mail, phone, website)

- Personal information (e.g. date of birth, interests)
- Pictures of users and other photos
- Status messages (micro-blogging on current events etc., indications regarding one's professional and personal relationship status etc.)
- Tracking of user activities (e.g. messages regarding changes of the profile, the joining of groups etc.)
- Record of contacts, affiliation to groups, etc.

This information is usually visible to other members of the SNS. The degree of visibility depends on the particular settings of the SNS environment. To some extent, users can define in their SNS accounts which data should be visible to others (e.g. all members of the

SNS or only certain contacts/friends). From a user's point of view, the profile is at the core of the SNS. It provides central access to the wide array of interactions offered within the SNS environment. In the centre are the social relations, i.e. the user's circle of contacts, groups, etc.; different internal functions and features stimulate further interaction; the network itself provides tools to automatically inform about activities in the domains a user is related to. These interactions generate new content and via applications the user can also proactively include content into the network (e.g. by posting, sharing, etc.). Although strongly interrelated, there are two content and application layers that can be distinguished: the internal one within the SNS environment and the external one crossing the border to the outside Web via external services and social plugins. Each of these building blocks generates large amounts of information that is processed further in the SNS environment and to some extent fed into the social graph.
These structural aspects shape the functionality of SNS environments. Considering the major characteristics of SNS from a wider perspective, the SNS functionality consists of the following core features (Cachia 2008, 3):

Table 6: Core features of SNS

Feature	Description
Presentation of oneself	Via the profile as main entry point in most SNS and their starting pages, users can present themselves and content they want to share to other peers.
Externalisation of data	The display of connections, i.e. the list of contacts, serves two functions as it allows users to view their networks and at the same time present to share it with others.
New ways for community formation	As SNS enable novel forms of interaction with a variety of features, people have multiple ways to connect from person to person as well as via digital objects in embedded applications, tags etc., i.e. via user-generated content. The array of connections extends also to non-personal entities.
Bottom-up activities	In line with the new possibilities for community building, networking effects are stimulated and individuals have enhanced options to share interests, ideas and collaborate.
Ease of use	The relative simplicity of SNS allows people with basic Internet skills to create an online presence without web design or programming skills and mostly without additional costs.
Reorganisation of the Web environment	SNS created new access points to Web services that are to some extent separated from the outside Web. In this regard SNS foster a centralization of Web environments.

5.2.1. Network effects

As the term implies, networking and interactions among users within a specific virtual environment is a core feature of SNS. While SNS are a recent phenomenon they refer to classical studies about social interactions and networking such as Milgram's exploration of

the "small world problem" (Milgram 1967), stating that every person knows every other person worldwide over six degrees of contacts. These theoretical assumptions reflect in contemporary SNS although the small world theory was criticized by several scholars. For instance by Kleinfeld (Kleinfeld 2002), who pointed out some biases in different studies on the small world problem, e.g. regarding the selection of samples and that the experiments conducted often failed to prove the six degrees hypothesis. "*Rather than living in a 'small, small world' we may live in a world that looks a lot like a bowl of lumpy oatmeal, with many small worlds loosely connected and perhaps some small worlds not connected at all. Milgram's 'small world' theory could be viewed as the 'strong' form of the small world phenomenon, for which we have little empirical evidence. The 'lumpy oatmeal' theory, that we live in a world with many small worlds possibly, but not necessarily connected, might be viewed as the 'weak' form of the small world phenomenon, for which we do have evidence*" (Kleinfeld 2002, 65). Despite of this critical view, there are also some recent studies that examined the small world hypothesis in the context of Internet communication: e.g. Leskovec and Horvitz (Leskovec and Horvitz 2008) analysed 240 Mio. Instant-messenger accounts and came to similar results: every user knows every other user over approx. 6,6 knots. However, while some mathematical studies reveal even less than six degrees, this might not correspond with societal reality: "[W]e may live in a world where everyone is connected by a short chain of acquaintances, but it is hard for most people to find these connections" (Kleinfeld 2002, 66).

A further classical theory that SNS are related to is the theory of "the strength of weak ties". This theory deals with the different forms of connections in a social network. In his classical work, Granovetter (Granovetter 1973) identified the dimensions of time, emotional intensity, intimacy, and reciprocity as factors shaping the strength of a tie. Strong ties refer to close relations as between friends and relatives. As these connections are built on a certain amount of trust they are stabilizing factors for the consistency of a network. Weak ties are more loose connections, but they have strong influence on the growth of a social network. With their bridging function across different network domains or nodes, a network can expand. Via weak ties, content (or more general) information can be distributed more widely and traverse greater social distance than via strong ties (ibid). Hence, contacts that are loosely bound to other contacts are expected to have a wider network and thus might also benefit from extended access to information (Heidemann 2010).

The strength of weak ties is well demonstrated by the success of the micro-blogging service Twitter: the aim of this service is to provide a simple way to distribute information across the network. The more followers exist, the more likely it becomes that information (the tweet) reaches into other networks or communities. Opposed to that, information distributed through strong ties "is much more likely to be limited to a few cliques than that going via weak ones; bridges will not be crossed" (Granovetter 1973, 1366). However, if ties are too weak, this might have negative effects on the perceived reliability and trustworthiness of a contact. As a consequence, relations might become what Granovetter (Granovetter 1973, 1361) calls "absent ties", defined as "ties without substantial significance" or even a "lack of any relationship". Hence, strong ties are essential for the stability of a network and, in their relation to weak ties, also ensure a fluid information flow.

5.2.2. Network relations and the social graph

The theoretical concepts outlined above, i.e. the six degrees of separation and the strength of weak ties also contribute to the development of social graphs. Social network analysis makes use of graph theory: a social graph is an attempt to deal with the complexity of social network environments. The general aim is to identify the number of actors and their relations among each other in the network (Nextmedia CSA 2010). The relevance of an actor depends not least on the number of relations to other actors. Central actors with a high number of relations represent nodes. In general, social graphs allow to model real-world interaction and enable deeper insights into user behaviour. This does not merely incorporate relations between human entities but already addresses also digital objects, i.e. content related to a human entity. The social graph is a dynamic way of modelling relations and thus different types can be distinguished; e.g. regarding the context of the analysis. Jin et al. (Jin et al. 2013) identify the following four different types of social graphs:

1. *Friendship* graph to map the relations among users
2. *Interaction* graph to visualize the interactions of users
3. *Latent* graph to show latent forms of interactions such as profile visiting
4. *Following* graph to reveal the distribution of followers/followees e.g. in micro-blogging.

SNS provide rich environments as regards information on social relations and interactions. Hence, most SNS utilize social graphs to analyse their networks but some also introduce it as part of their functionality available for users. For instance, Facebook offers a particular search in the social graph that addresses aspects of the semantic web: it allows, e.g. to search for persons with particular interests, places they have visited, pictures a user likes, etc.[58] In addition, there is also a standardized application programming interface (API) for developers available (i.e. the open graph), which enables web pages from the outside web environment to be interconnected with the social graph. The integration of social plugins into web pages is the most common practice to establish such a connection between the SNS and other Web environments.

5.2.3. Embedded services and the role of social plugins

Besides the internal SNS features, many applications from external (third party) providers are embedded in the SNS environment that can be accessed by users, so-called "apps". Most SNS offer standardized programming interfaces for developers (API) to integrate a variety of apps. The range of available apps is broad but most are entertainment related (such as social games like Farmville, quizzes, puzzles, applications for music, shopping, travelling, etc.).[59] The development and integration of apps is not least determined by commercial interests and targeted advertising.

So-called "social plugins" are particular forms of embedded services: they are standardized applications to foster interactivity between users and their content by establishing a connection between an SNS and other Web environments. The most prominent social plugins are Facebook's "like", "share", "follow" and "send" buttons, which are included in

[58] See https://de-de.facebook.com/about/graphsearch
[59] A variety of apps is available e.g. in Facebook's App Center https://www.facebook.com/appcenter.

many Web sites. Via these features, users can share content with others and reveal their opinions on particular content. These data is inter alia used for advertising and enables a significant extension of the SNS environment as it provides deeper insights into user behaviour referring to social search (e.g. Biermann 2010). The functionality of social plugins is relatively simple but sophisticated: a plugin establishes a direct connection with one or more servers of the original SNS environment. The SNS (e.g. Facebook) then traces every interaction with this social plugin such as clicking a like button or commenting a post, etc. If the individual interacting via a social plugin is a member of the SNS, this information feeds into his profile data. If the user is not a SNS member, the information is still collected and likely to be stored in a separate profile for non-members including identifiable data from the user's machine. Thus, social plugins gather large amounts of information about individual user interactions also in the Web outside the SNS. This includes inter alia what one likes, with whom one shares what, which comments one posts on particular content, which websites and services one uses, etc. In short, a very detailed picture of individual usage patterns on the Internet.

5.3. Societal impacts

Various studies deal with usage and impact of SNS, covering sociological aspects (e.g. Ellison et al. 2007; Wanhoff 2011; Röll 2010; Steinfield et al. 2008), psychological issues such as Internet addiction (e.g. Valkenburg et al. 2006; Livingstone 2008) and commercial aspects, such as the business models of SNS and related companies, including data mining for marketing and other purposes (e.g. Elmer 2004; Häusler 2007; Fraser/Dutta 2008) as well as academic usage (e.g. Nentwich/König 2012). Some of the studies focus on usage and non-usage as well as usage patterns in particular (e.g. Hargittai 2007), often times with a particular focus on young users (e.g. Amanda/Mary 2007). Many studies on SNS focus on privacy and trust (e.g. Fuchs 2009; Gross/Acquisti 2005; Biermann 2010; Ferdig et al. 2008; Lewis et al. 2008; Barnes 2006; Cain et al. 2009; Dwyer et al. 2007). Opposed to those critical aspects, there is a variety of positive effects such as stimulating social learning, enabling new modes of participation, strengthening community building, development of social capital and empowerment (e.g. Wimmer 2009; Pratchett et al. 2009; Heidemann 2010; Hoffman 2009).

However, in the reality of common SNS usage these effects occur only partially. While some of the envisioned effects are observable in particular contexts, every-day-usage practices of most users seems to follow similar mechanisms than in the analogue world; i.e. communication and exchange with other individuals. Studies on user behaviour and motivational aspects for SNS usage correspond to this assumption: The main reason is staying in touch, maintaining contact and relations with friends, relatives and acquaintances. Publishing and generating content such as sharing photos, music, likes etc. is an essential part of SNS usage patterns. A further aspect concerns the entertainment factor. The content in SNS environments (e.g. videos, photos, games etc.) often has an entertainment value for users. "*Many people spend time surfing the online social networks browsing through the content in similar fashion as people watch television*" (Rantamäki 2008). However, the content differs from traditional media such as radio or television as users do not merely redistribute but also create content themselves or put existing content into completely new contexts. This additional value of SNS is one aspect for its popularity.

The user generated content is also precious for the economic aspects of SNS as it provides high value for different kinds of business models. In this respect, SNS are both in itself a business model and enable further economic activities. Large SNS, such as Facebook are, so far, a viable business model, successful even at the stock markets. The core value of the business models is mostly the substantial data available in SNS. This data give deep insights into user interests and behavior. Thus it has high commercial value e.g. for personalized advertising, market analysis etc. SNS access is usually for free in this model to attract a maximum amount of users, but users have to allow analyzing their data. Therefore this has been labeled the "service-for-profile model" (Elmer 2004; Rogers 2009). Mostly the data is also sold to third parties such as data marketeers. Beside this basic model, several other funding approaches exist as Nentwich/König (Nentwich/König 2012) observed: Some SNS charge fees for premium functions (e.g. Xing), such as specific services, or enriched profiles for commercial users. In some specific SNS (e.g. science-specific) there are a several other funding approaches based on subsidies or donations. Besides the dominating service-for-profile model that earns criticism for lacking data protection and privacy issues alternative models based on crowdfunding to gather donations exist (e.g. Diaspora)[60].

The fact that entertainment aspects are present in SNS does not narrow the given effects of SNS but underlines that the context of usage plays a crucial role in this regard. The rather simple assumption that the more specific a usage context is given in an SNS the more likely are effects in the scope of this context. Examples in this regard are given in the scientific use of SNS. Nentwich and König (Nentwich/König 2012) provide a deeper analysis of SNS in the context of science and research.

As the case of sixdegrees shows, not every SNS from the early days survived in the tides of web evolution. Most prominent is the fall of Friendster, which encountered serious problems ending up in a collapse. The main reason for this collapse was a lack of functionality to handle different groups of contacts and the possibility to distinguish e.g. between close friends, colleagues and others as not every user wanted to grant all contacts the same access to its profiles. But exactly this was the case in the Friendster environment. As a consequence, the dropout rates increased. A further related reason was an increasing abuse of the network by spammers and "Fakesters" that exploited the network functionality for advertising and spam (Boyd 2007). This leads to social collisions and decreasing trust of users in the providers. Recent scandals on large-scale surveillance of Web activities contribute drastically to decrease trust on wider societal level.

5.3.1. SNS between the public and the private sphere

With the occurrence of SNS, questions on the relationship between the public and the private sphere reappeared. According to Habermas' (Habermas 1989) classical work, the public sphere is an essential part of deliberative democracy that intermediates between citizens and political decision makers. From a more general view, the public sphere is "*an open field of communicative exchange. It is made up of communication flows and discourses which allow for the diffusion of intersubjective meaning and understanding*" (Trenz 2008, 2). With its inherent deliberative quality it is not merely some form of public

[60] http://joindiaspora.com

communication but an element that transforms public communication into public opinion (Frazer 2007; Trenz 2008). The development of this deliberative quality is linked to the private sphere, i.e. those spaces and domains where individuals have the ability to be and act free and without interference from others. Hence, domains where privacy is factual and people are able "*to engage in worthwhile activities that they would otherwise find difficult or impossible*" (Solove 2006, 484). In this respect, the relation between the private and the public sphere is complementary: individuals develop their opinions in their private sphere; and, by communicating and interacting with other individuals the public sphere takes shape (Habermas 1989). It is vital that enough open space exists for both spheres to develop where individuals can meet, share thoughts, discuss their opinions, exchange ideas etc. without interference. Otherwise, the deliberative quality and transformative capacity as essential parts of democratic will formation might diminish. In the analogue world, different kinds of public spaces provide room for both spheres to converge. But where are SNS environments to be located in the interplay between the public and the private sphere? At first glance, SNS environments appear as public spaces, i.e. "*non-domestic physical sites that are distinguished by their relative accessibility* […]"(Humphreys 2010, 2). For Boyd (Boyd 2007b), SNS can be seen similar as "*mediated publics*" and "yet *another form of public space*". However, there are significant differences between SNS and traditional public spaces: As SNS access usually demands user authentication, it represents a specific space on the Internet, which is to some extent separated from others – a form of semi-public space. One distinguishing factor is the visibility of interactions: Considering a common public square in the analogue world, the behaviour, movements and interactions of individuals are generally visible to others nearby; however, there is usually no systematic monitoring of interactions and communication content. Thus, this visibility is rather volatile and with different varying levels of privacy. In an SNS environment, social relations and interactions *including* the content are explicitly observable (and observed). This observability is given because the relations between personal (friends, contacts, etc.) and non-personal entities (interests, content used, shared, linked, liked, produced, etc.) are part of the information processed (Strauß/Nentwich 2013).

The public sphere should not be (mis-)understood as a single space of public deliberation, but as a "*communicative network where different publics partially overlap*" (Nanz 2007, 19). In the last few years, social media grew wider into traditional mass media and visibly affects public discourse. In this regard, SNS are a sparkling example for a novel, digital representation of the public sphere. It is hardly applicable to analyse whether the vast amount of heterogeneous partial publics being active in SNS environments mirrors and influences public communication in general. However, a certain impact of activism in SNS for instance on public discourse is evident as outlined in the next section.

5.3.2. Capability for political participation

SNS provide a variety of options to strengthen relations between individuals as well as institutions. The assumed potential for democratic processes includes for instance political action, campaigning, participation, establishing links between public sector and civil society and fostering the relationship between citizens and government etc. (CLG 2008). There are several studies on the effects of ICT and social media for political participation in the field of e-participation (OECD 2007; Levine 2002; Macintosh 2003; Baringhorst 2009; Lindner et

al. 2011). Assumed effects are inter alia increasing political engagement due to the ICT-induced networking culture, enhanced social capital building and stimulation of active citizenship. For instance, Kann et al. (Kann et al. 2007) postulate that Internet communication created a new culture of political participation by fostering citizen involvement, openness, political information and ideas and facilitating mobilization and campaigning. Social media inter alia was used extensively for political campaigning during the US elections in 2008 (Smith 2009). SNS in general reflect the societal need to communicate and socialize with other individuals. Their modalities correspond to the need to share lively experiences and connect with others. In this regard, SNS usage can be seen as "*a way of sustaining communication and continued sharing of experience and learning*" (CLG 2008, 6). Blogging, citizen journalism, publishing critical videos on public events or politics or similar contribute to public discourse as different opinions may stimulate interest in debate (OECD 2007). However, while some evidence exists on such effects in specific cases, the related expectations relativize as political participation is not reducible to technical means. "*A common fallacy is that the deployment of ICT for participatory approaches will directly lead to, e.g., more transparency, increased engagement, community empowerment and, as a consequence, to fostering the quality of deliberation on political issues*" (Lindner et al. 2011, 111). Hence, the expectations that ICTs and social media improve democratic processes in general are mostly overestimated. Having the opportunity to publish does not automatically imply that your voice will be heard in the public sphere (Lindner 2007).

Expectations that a general SNS such as Facebook entails positive effects on civic engagement and democracy is likely to be misleading as the mechanisms of democracy are complex and not reducible to the online world. A major reason is that a general network per se has no such intended context (such as stimulating participation) but in its broadest sense simply connecting people. While this surely is a sine qua non for participation it is not a sufficient factor for determining participation. This does not neglect the mobilizing power of social media. A prominent example for this power is given by the **Arab Spring revolutions**, where SNS where important tools to support activists and had significant political impact. While the political will to engage in these movements is bound to the particular individual and thus no result of ICT, these channels can catalyse existing political engagement by stimulating mobilization. The networking structure of SNS provided ideal means to support activists in organising and coordinating protest movements and raise their outreach: in 2011, "*millions of Facebook and Twitter users in Tunesia and Egypt formed a social grid massively parallel that sustained the revolutionary waves in Tunis and Cairo's main streets and suburbs as well as in the secondary towns of the countryside*" (Benkirane 2012). The networking nature of SNS made it possible not only to organize, but also to mutually learn as protesters shared their experiences, spread news, sympathy and support with others over the networks. These learning effects in real time also contributed to the success of activists (Skinner 2012). In this regard, social media channels served as catalysts: they "*accelerated local reactions, synchronized different levels and intensities of uprisings and permitted the coverage of events through real-time footage directed to global opinion*" (Skinner 2012). However, the same technologies that supported the democratization process were used for control and repression of citizens by the authoritarian governments of the region. Hence, the role of social media for political

participation is to some extent an ambivalent one. "*Social networks and new media can transform information sharing into creative ways of knowledge production. But they can also be used for control and manipulation of citizens*" (Skinner 2012). It depends not least on the political-administrative system or regime and the cultural context of SNS usage. As Dahlgren (Dahlgren 2013) puts it: "*Democracy will not be saved by media technologies; social media can make an important difference in this regard, but they can also function to exacerbate democracy's difficulties. Ultimately only citizens can revitalise and extend democracy; that is our only realistic option*". While the role of social media for political participation is ambivalent it bears manifold potential for knowledge production as described in the next section.

5.3.3. SNS-linked knowledge production

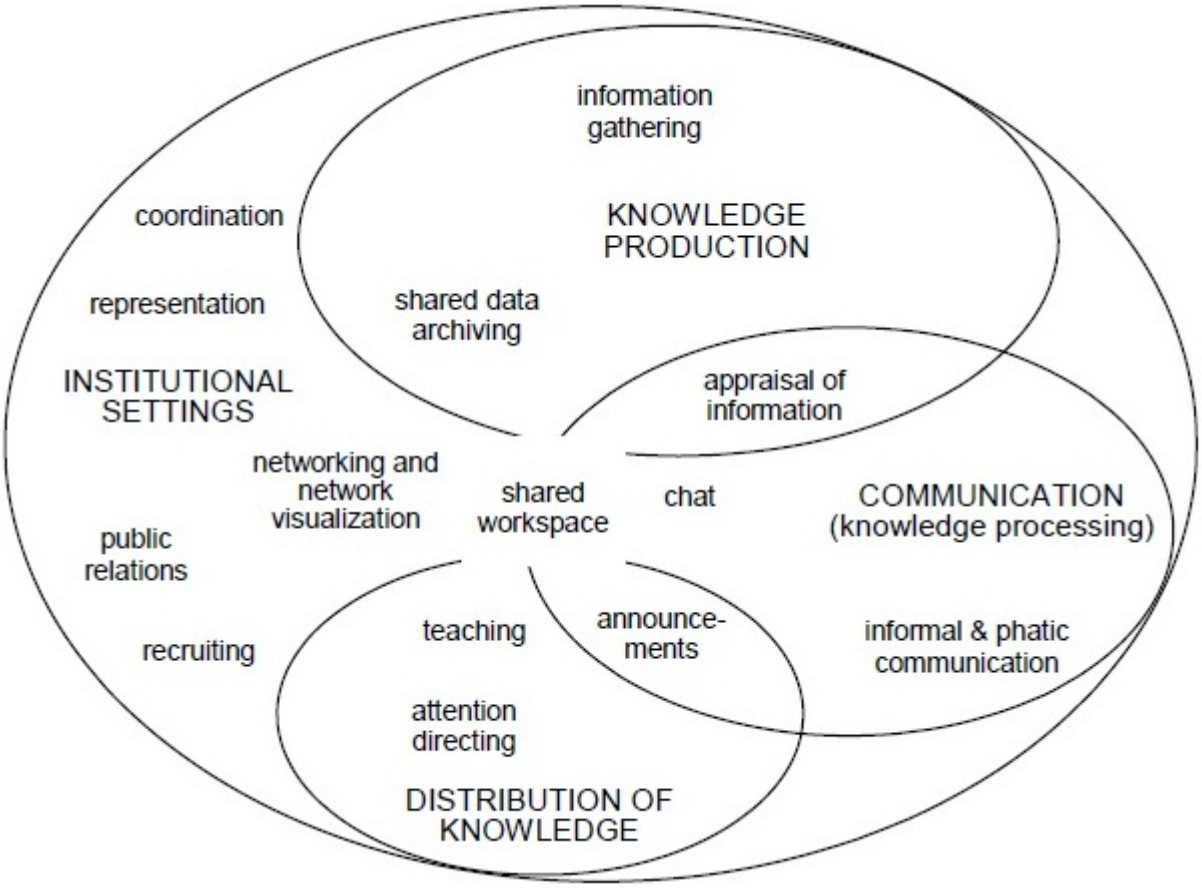
To provide an advanced and encompassing platform for easy and informal communication in various forms is obviously the prime functionality of SNS. However, many of the tools available in SNS may also serve other purposes, in particular supporting the production of new knowledge. A non-linear model of how knowledge is produced distinguishes between four interlinked areas (Nentwich 2003, 23ff.): (1) the institutional settings, i.e. the framework in which knowledge production takes place, including the technical equipment, (2) knowledge production in the narrow sense, i.e. information gathering, data production, data-processing and -analysis, data management, (3) knowledge processing, i.e. knowledge representation, discourse, cooperation and evaluation, and finally (4) knowledge distribution, i.e. publication, teaching, and implementation (see Figure 8). In all four areas information technology in general, and new social media, in particular SNS, have an impact. While this has been shown with regard to activities in the field of science and research under the label of "cyberscience" (Nentwich/König 2012; Nentwich 2003), this is also applicable in other areas of knowledge production, such as in the software industry or in the consultancy business.

When it comes to the specific role of SNS in knowledge production, the core observation is that the various functions of directing attention (from the "Like" button to user ratings, from user tagging to automated recommender systems) contribute to acquiring information, particularly with regard to documents, literature, news items etc. Groupware-like collaboration tools available in some SNS like shared data or file archives or collaborative text editors, support working groups in their data management etc. Of vast importance is how the knowledge is processed, i.e. how it is elaborated, refined, tested, and evaluated it through communication and discourse in expert circles (and beyond). The various channels offered by SNS enable quick and informal, synchronous and asynchronous ways of exchanging thoughts about the new knowledge *in nuce*. It is this easiness of communication within SNS that offers the potential of a faster turn-around of knowledge.

An important asset of SNS as compared to previous and parallel tools supporting knowledge production is its potential to include not only many more, but also a greater variety of actors, data-providers, and experts in the process. A particular strength of SNS is their potentially wide user base. Whatever the specialty, whatever the topic, it is likely that the huge networks represented in SNS will come up with one or more individuals that have the right expertise, practical knowledge or represent a needed point of view. Hence SNS, as a specific digital infrastructure, may play a role in the so-called crowdsourcing.

Crowdsourcing is usually defined[61] as the practice of obtaining knowledge (services, ideas, or content) by soliciting contributions from a large group of people, and especially from an online community, rather than from traditional employees or suppliers. Wikipedia, a very important producer of a knowledge resource, is the most prominent example in that respect and can be labeled a *proto*-SNS (as regular users have their individual profiles and communicate mainly through the Wikipedia-specific internal communication channels).

Figure 12: Knowledge production, Source: Nentwich 2003, 24



5.4. Privacy Implications

Sharing personal information plays an essential role in the very design of SNS as every form of social interaction needs a certain amount of information about the parties involved. On the one hand, the wide range of new possibilities for sharing and creating content supports community building and collective actions; on the other hand, it further stresses informational privacy and the users controllability over his/her personal information in several ways (and not least due to complex modes of data processing that refer to distributed computing in the cloud). Or in other words: the distinction between personal information and user content diminishes further within social networks. Thus, privacy, trust, and proper handling of personal information are crucial aspects of SNS. In this regard there are potential conflicts between users' intentions to share personal information and the way this information is used by the SNS (e.g. behavioural targeting and processing of user

[61] http://www.merriam-webster.com/dictionary/crowdsourcing.

data for commercial interests). These issues are not least affected by the interplay between privacy awareness, different usage patterns and features supported by the SNS.

5.4.1. User perceptions on information disclosure and privacy

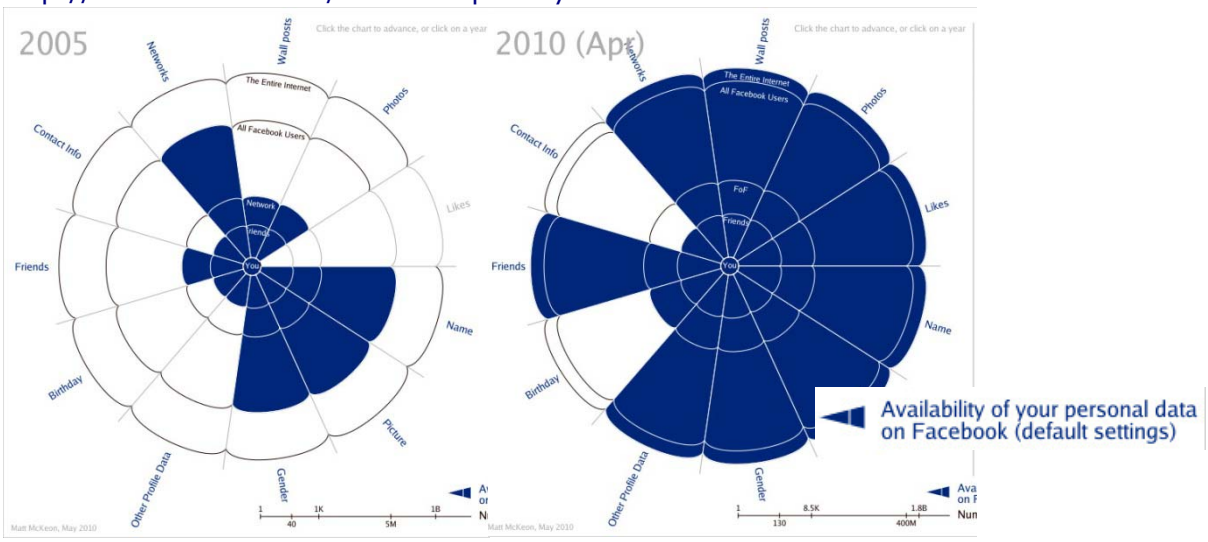
It is evident that users share vast amounts of personal information in SNS. A number of studies explore what information users reveal (Acquisti/Gross 2006; Barnes 2006; Fuchs 2009; Leenes 2010). Lack of privacy awareness is surely an important issue in this regard. However, the problem seems to be more complex as disclosing information does not necessarily imply that SNS users do not care about their privacy. On the contrary, users who are well aware of the privacy problems of their SNS usage are seemingly not a minority. According to a critical study exploring the perceptions of SNS users on advantages and disadvantages of SNS, for the majority of the respondents (55.7 %), a main threat is "political, economic, or personal surveillance as a result of data abuse, data forwarding, or a lack of data protection"; for 23 % the disclosure of personal affairs is problematic; about 8 % see the danger of job-related disadvantages if current or potential employers access profiles, 6.6 % are concerned about advertising or spam. At the same time, respondents named maintaining existing contacts (59.1 %) and establishing new contacts (29.8 %) as the main benefits of SNS (Fuchs 2009). Hence, the majority of the participants seem to perceive that the advantages of SNS are somewhat coupled with risks regarding surveillance and loss of privacy. A special Eurobarometer survey (TNS 2011) displays similar results. About 50 % of the European citizens perceive that disclosing personal information is hardly avoidable on the Internet. Social media has an essential share in this regard. Among SNS users, the two main reasons for disclosure are to gain access to a service (61 %) and to connect with others (52 %). Also half of the SNS users were already in a situation where they had to reveal more personal information than service usage would require. Over 70 % are (very or fairly) concerned about such cases. More than 50 % of the internet users are concerned about profiling activities although the question was linked to positive effects such as gaining free services. One could argue that users need more awareness of their own responsibility for handling personal information. Awareness-raising in this regard is without any doubt an important issue. However, it does not seem to be a sufficient measure: three-quarters of the European Internet users seem to be somewhat aware of this and at the same time see a demand for more responsible treatment of their information by online sites. Among SNS users, 75 % perceive a need for more control of their personal information (TNS 2011). Hence, there seems to be awareness of privacy problems related to SNS usage, but users perceive a lack of control over their personal information flows. In other words: the concept of informational self-determination is not sufficiently incorporated in SNS.

5.4.2. Complexity of privacy settings and user preferences

The privacy settings of SNS provide a certain amount of control over personal information. Users can customize the settings based on their preferences and to some extent determine which information should be visible and accessible to others. However, there are many critical aspects in this regard. The way privacy is handled in SNS environments seems to have shifted towards a "disclosure-by-default" paradigm (Strauß/Nentwich 2013). The

changes in Facebook's privacy policy[62] underline this shift. In 2005, availability to most information was limited at least to the list of contacts and only some to members. As Figure 10[63] shows, the default settings have significantly changed until 2010. What was once protected by the standard privacy configuration is now accessible by default. SNS users who keep this standard setting disclose practically all information in their profiles, their contacts, their photos, and their preferences (e.g. "likes"). While at least the widest circle of disclosure was limited to members, this information is now visible not merely to friends or all SNS members, but also to entities in the Web outside the SNS environment.

Figure 13: Facebook's privacy setting over time, Source: Matt McKeon 2010 http://mattmckeon.com/facebook-privacy



One could argue that users can at least change their privacy settings and do not have to keep the default settings. However, this argument has limits: the complexity of the settings complicates the users' ability to customize their preferences. Furthermore, the amount of privacy-awareness differs widely among users. Surely a complete lack of privacy settings would worsen the problem. However, the options available to reduce information disclosure such as reducing profile visibility are rather "*a quick fix (…) than a systematic approach to protecting privacy*" (Debatin/Lovejoy 2009, 103). Facebook's privacy policy also raised concerns of the European Commission. In 2009, the Commission released a set of principles for safer social networking recommending inter alia to "*[e]nable and encourage users to employ a safe approach to personal information and privacy*" (EC 2009). However, these principles were limited to enhance protection of minors. The Article 29 Working Party put more emphasis on the importance of privacy settings: "*SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties*" (Article 29 Data Protection Working Party 2009). As Facebook changed its settings in December 2009 (a few days after the release of the Working Party's opinion), in a letter to Facebook the Working Party underlined its opinion

[62] Recently in 2013, Facebook again changed its settings, According to the New York Times, "Facebook's new policies make clear that users are required to grant the company wide permission to use their personal information in advertising as a condition of using the service." http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html.

[63] This visualization is only an extract and does not cover the full range of personal information disclosed.

and called the fundamental changes at the cost of users privacy "unacceptable" (Article 29 Data Protection Working Party 2010). This issue underlines the problem of fluid privacy settings. As the default settings changed significantly over time and SNS rapidly introduce new features, this problem is further exacerbated (e.g. the users' settings can be undermined by new settings or features). A recent study reveals that although users seem to be more aware of customizing their privacy settings, confusing changes of these lead to unintended disclosure.[64] Furthermore, in many cases, the terms of use allow the SNS to process the users' personal data including third parties. In addition, most third party applications have specific terms of use. Some require the users' consent to process personal data, others automatically collect these data. As services are embedded, data from these also flow back into the SNS environment. Even if a user customizes her profile according to her very own perception of privacy, problems remain as: due to the usage policy of most SNS (e.g. Facebook), users give consent on the disclosure of their personal information. Finally, despite of the privacy settings, the SNS serves as centralized repository holding detailed information about the individual user.[65] This information is also attractive for a variety of observers in the public and the private sector. SNS provide ideal environments for large-scale profiling which "*builds on combining two strands of information to create an expectation of individual users' future preferences, wishes and behaviours"* (Van der Berg 2011, 187). These two streams of information are "the totality of past behaviours and choices of a single individual" and "*the collective behaviours of a large group of people, with respect to one single choice or purchase*" (Van der Berg 2011, 188). Many business models ground on these data e.g. social marketing, behavioural advertising or specific monitoring of social media in order to predict new trends. An example is "Mass Relevance" which claims to aggregate SNS content in real-time.[66] In the public sector, large-scale surveillance of Internet communication by security authorities and intelligence agencies is heavily evident since the revelations of the PRISM and Tempora projects.[67] These incidents drastically highlight the urgent need for a reconsideration and revitalization of privacy and scrutiny as public values in contemporary society (Strauß 2014 forthcoming). SNS quickly expanded worldwide not least due to its contribution to stimulate the societal need to communicate and exchange with others. Communication is also a matter of trust, which is seriously harmed by the recent scandals that caused significant loss of trust in private and public institutions among citizens.[68] Trust is a core aspect of democratic societies that grounds on reciprocity. Without such, negative impacts are likely to increase further. The dimension of collateral damage is yet unforeseeable and cannot be easily fixed. But it is obvious that measures are needed to improve privacy protection to repair the massive loss of trust.

[64] http://allfacebook.com/carnegie-mellon-facebook-privacy-study_b112298.

[65] In the case of Facebook these and other privacy problems are currently part of law suit going on in Europe, known under the label "Europe vs. Facebook". The related platform http://www.europe-v-facebook.org/EN/en.html provides detailed information on what data is collected and processed by Facebook (http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html).

[66] For further examples see http://www.insidefacebook.com/category/social-media-monitoring/

[67] Cf. http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet-7000016565/ http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[68] http://www.dailymail.co.uk/sciencetech/article-2423713/Facebook-users-committing-virtual-identity-suicide-quitting-site-droves-privacy-addiction-fears.html, and lack of trust among internet users in government institutions http://www.bitkom.org/de/presse/8477_76831.aspx

5.4.3. Personal vs. non-personal data and identifiable information

According to the European Data Protection Directive (95/46/EC)[69], personal data represents information that relates to an identified or identifiable natural person (or data subject). In case of anonymous or anonymised information, i.e. information that does enable identification of the data subject, protection principles do not apply. At first glance, this is reasonable. However, the role and meaning of identifiable information has significantly changed. A possible distinction of identifiable information is between person-specific data referring directly to one's identity (e.g. name, date of birth, etc.) and explicitly entered by a user; and technology-specific data referring to one's technical devices (e.g. IP-, or MAC-address, web browser identifiers, etc.) processed during a user-session without direct user interaction (Strauß 2011). In general, the variety of data collected and processed can be distinguished in *explicit data*, i.e. information directly related to service usage which a user uploads to a digital environment (e.g. profile details, interests, photos, etc.), and *implicit data*, i.e., information that is processed automatically in the system without direct involvement of the individual (e.g. browser data, interactions, content, web sites visited, profiling, etc.). Whether processed information is personal or non-personal is increasingly difficult to determine. Contemporary and emerging information processing, particularly as regards SNS and other networked environments, vividly demonstrate that the distinction between personal and non-personal data diminishes. This heavily strains "unlinkability", which is a crucial requirement for the technical implementation of informational self-determination. Unlinkability prevents from privacy-infringing linkage of separated information, i.e. that different contexts stored in different repositories become merged into one central profile. This linkage is possible due to unique identifiers. The effectiveness of unlinkability suffers from increasing options to create identifiers. In digital environments, every form of interaction creates a certain amount of traces. This is obvious in the case of personal data, but also non-personal data are traceable leading to one's identity. With increasing amounts of data linkable to a person his or her "identity shadow" (Strauß 2011) expands, entailing, new options to re-identify an individual by gathering quasi-identifiers from these data. As "context is everything" (Leenes 2010) in an SNS environment that processes vast amounts of personal information with rich context information, there are several options to apply de-anonymisation techniques (Wondracek et al. 2010). These aspects cannot be protected by current SNS privacy settings. A further aspect is information disclosed to other contacts that also undermine privacy settings: "*leaking graph information enables transitive loss: 'insecure friends' profiles can be correlated to a user with a private profile*" (Bonneau et al. 2009, 6). Hence, even if information would be protected by the privacy settings (which is not the case as outlined), the effectiveness of this protection would depend also on the settings of the contacts a user is related to.

The increasing relevance of social plugins and embedded services feeds the array of context information and further undermines informational self-determination. Users mostly have to give consent if they want to use an app. Furthermore, those third parties providing the services extract and gather personal information from the SNS to analyse user

[69] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML At current stage, the reform process for a new European Privacy Framework is still going on.

behaviour (e.g. for targeted advertising), also without the users' consent.[70] Also this practice of data gathering is manifold as vice versa the SNS itself absorbs data also from the outside Web and traces user behaviour also in contexts that are usually not related to SNS usage. With the social graph and developments towards "social search", the mapping of personal relations extends towards a mapping of user information, preferences, behaviour, activities, social relationships, etc. In this regard, SNS dig deep in the identity and behavioural patterns of users. The already existing conflict between users intentions to share information, for instance with a view to socialising, and how this information is treated by the SNS intensifies. A certain amount of user control is essential for the effectiveness of privacy protection, not least regarding this "privacy-sociality trade-off" (Leenes 2010). However, all these (de-) and (re-)contextualisation aspects elaborated above make informational self-determination a rather tricky task to cope with.

5.4.4. Privacy types and SNS usage

Privacy is to be understood as a multidimensional concept consisting of different types and dimensions. Clarke (2006)distinguishes four major types: privacy of the person, privacy of personal behaviour, privacy of social communications and privacy of personal data. Finn et al. (Finn et al. 2013) propose an extended taxonomy of "seven types of privacy" by complementing additional dimensions to Clarke's approach, privacy of

- the *person* encompasses the protection of body functions and characteristics, such as biometrics or genetic codes;
- *behaviour and action* addresses the "ability to behave in public, semi-public or one's private space without having actions monitored or controlled by others"; this involves "sensitive issues such as sexual preferences and habits, political activities and religious practices" (ibid);
- *communication* includes the ability to communicate freely via different media and without interception including the avoidance of different forms of wiretapping and surveillance of communication;
- *data and image* addresses the protection of data from automatic disclosure to other individuals and organizations; individuals should have "*a substantial degree of control*" over their data and its usage (Clarke 2006); image is a particular "*form of personal data can be mined for biometric data and used to identify, monitor and/or track individuals as they move about public or semi-public space*" (Clarke 2006);
- *thoughts and feelings* involves an individuals' freedom to think and feel whatever he/she likes to without restriction; this type differs from behaviour as thoughts do not necessarily translate into behaviour;
- *location and space* encompasses one's right to move free from interference in private, public or semi-public space without being identified, tracked or monitored;
- *association (including group privacy)* addresses one's right to associate with whomever he/she wants without being monitored. This also includes groupings or profiles over which one has no control (e.g. involvement in discussion groups) (Clark 2006).

[70] E.g. popular apps and games such as Farmville and others undermine the privacy settings and submit data to advertisers. According to the Wallstreet Journal, Facebook IDs of users were sent to at least 25 different companies. Wallstreet Journal Oct. 17 2010
http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

This taxonomy allows to grasp more systematically to what extend a technology affects privacy. Strauß and Nentwich (Strauß and Nentwich 2013) explored which privacy types are affected by common and emerging SNS usage, which refers to the rapid development of social networks and upcoming trends. They found that the main types currently affected are privacy of communication, data and image as well as privacy of association. As communication and interaction is at its very core, SNS gather extensive arrays of information in this regard; these and other data are accessible and per default disclosed to others, including images and photos; privacy of association also affected as the list of contacts is visible. Furthermore, the related profiles can undermine the privacy of other contacts. As the relations and interactions in SNS include personal as well as non-personal entities (i.e. content) related information this gives some insights into behaviour and action (e.g. contributions in discussions, postings, interests, etc.) and even thoughts and feelings: Some SNS features try to seduce users by revealing information in this regard. For instance in Facebook, users are asked "How are you feeling?", "What are you doing?" and similar. Hence, to some extent, also these privacy types are affected at present. The on-going diffusion and further expansion of the SNS universe makes it likely that privacy impacts increase affecting additional types of privacy. Three main trends can be identified in this regard (Strauß and Nentwich 2013):

1) Social plugins and the social graph aiming at gaining deeper insights into users' identity and behavioural patterns and perceptions also outside the SNS environment.
2) Face recognition and biometrics, which develop quickly and begin to reach into SNS contexts (Power 2011) affect the privacy of the person. For instance, Facebook supports photo tagging to link persons and their profiles; Google is the owner of patent for "facial recognition with social network aiding"[71]; these developments link the appearance of a person in both the physical and the virtual world.
3) Mobile social media usage significantly increases: the amount of mobile data processed doubled from 2011 to 2012 (Ericsson 2012); with location-based services and mobile apps, access to SNS via mobile devices (such as smart phones, tablet PCs, etc.) becomes more attractive. According to ComScore (Comscore 2012), mobile SNS access rates increased over 70 % from 2010 to 2011. Hence, also privacy of location and space becomes affected further.

5.4.5. Privacy-by-design

One of the core privacy problems of SNS is the prevailing paradigm to disclose information by default which pervades SNS environments. Related is the second core problem that identifiable information increases due to diminishing boundaries between personal and non-personal data. Thus, in order to cope with current and upcoming privacy challenges, a shift of this paradigm is necessary towards privacy-by-design and privacy-by-default schemes. As the term implies, privacy-by-design encompasses approaches to embed privacy and data protection into the very design, operation and management of technologies. Realizing privacy-by-design grounds on seven foundational principles (Cavoukian 2009):

- *Proactive not reactive*; preventative not remedial, i.e. privacy is to be proactively implemented before, not after a risk or breach occurs.

[71] https://www.informationweek.com/internet/google/google-seeks-social-networking-face-reco/229218484

- *Privacy as the default setting*, i.e. privacy as built-in feature without requiring users action to customize settings.
- *Privacy embedded into design*, i.e. as integral part of systems and practices without diminishing functionality
- *Full functionality* – positive-sum, not zero-sum, i.e. without constructed trade-offs such as privacy vs. security but embracing multiple functionalities
- *End-to-end life-cycle protection*, i.e. a "cradle-to-grave lifecycle management of personal information" beginning already with the first information processed including a deletion at the end of the process
- *Visibility and transparency*, i.e. data processing needs to be understandable and controllable to scrutinize proper handling of information
- *User-centricity*, respect for user privacy, i.e. incorporating the user as a central part of the system and empowering their active role in privacy protection.

Islam and Iannella (Islam and Ianella 2012) analysed the privacy-friendly SNS Diaspora regarding its implementation of these principles. Diaspora[72] is a privacy-aware, decentralized, distributed social network aiming at replacing centralized SNS that failed in protecting privacy. Its architecture thus differs from common SNS: it is decentralized consisting of so-called "pods", i.e. private servers where user accounts (seeds) are hosted. Users can store and control their data via these pods. They can choose whether to manage their own servers or use a public pod. In general, the system provide higher amount of user control. Islam and Iannella (Islam and Ianella 2012) found that some principles are well addressed, in particular that the network is proactive, as it provides flexible options for users to control their data; and that visibility and transparency are high as the system is open source and users can setup their own SNS. While privacy-by-default is implemented, data security seems to be in the first place. Hence, functionality is only partially given and they conclude that some features are more related to security-by-design such as encryption features for securing user content. Diaspora is still in its beginnings with only a few users compared to global players but seems to bear some potential to improve SNS privacy.

As Diaspora exemplifies, there exist some promising technical means available for enhancing privacy-by-design which is a *sine qua non* to cope with the main privacy challenges. In general, the number of privacy tools that aim at supporting users in their informational self-determination increases: e.g. browser plugins or add-ons to prevent user tracking by third-parties, different kinds of advertisement blockers, or blockers of social plugins (e.g. Ghostery, Adblock+, Facebookblocker). Similar tools also exist as apps for SNS environments (e.g. privacyfix.com). These measures are without any doubt essential to foster privacy protection. However, from a wider societal perspective, they are often prophylactic and not sufficient to cope with existing privacy and data protection problems. One important aspect is that the employment of such technological means is currently in the responsibility of the individual. This depends not least on his or her amount of privacy awareness. This contributes to another form of digital divide: a sort of **privacy divide** (Papacharissi 2010), where users with privacy awareness and capabilities to protect their data are separated from users with less awareness and/or less media and privacy literacy.

[72] http://www.diasporial.com; https://joindiaspora.com; https://diasporafoundation.org

Users have without any doubt high responsibility to protect their data and privacy, but they cannot be the only ones in charge. Hence, instead of providing users with a cumbersome and sometimes diffuse tool-box to take care for their privacy, privacy-by-design needs to be improved on several levels accordantly. As regards SNS, this implies to enforce the implementation of privacy mechanisms in design and architecture of SNS in a more effective way than it is currently the case. Relevant factors in this regard are:

- Encryption of content
- Unlinkability of personal identifiable information
- Pseudonymity and options for anonymous usage
- Decentralization of personal data
- Transparency and accountability of SNS environments and providers

Content encryption is an essential aspect to improve the protection of several privacy types. Currently, this is widely the exception than the norm: most information is available online as plain text. Integrating encryption functionality as standard into the SNS environments would significantly contribute to protect the privacy of the user and to effectively secure from unintended information disclosure. The problem of increasing personal identifiable information can also be addressed with encryption, referring to the concept of unlinkability of personal information which is a major requirement for the implementation of informational self-determination. Unlinkability is essential to prevent from *"privacy-destroying linkage and aggregation of identity information across data contexts"* (Rundle et al. 2008). Options to use pseudonyms instead of unique identities, for instance by surrogating identifiers or parts of a user ID with random values supports to avoid linkage with users' identities. Pixelating techniques could be used by default to anonymize and remove the relation of a photo to a specific person; also in order to avoid automatic face recognition. Currently, most SNS represent centralized repositories containing massive amounts of personal information. As the example of Diaspora shows, there is also the option of a decentralized architecture. This also supports privacy and security and thus should be fostered. The integration of features enabling SNS users to view their own profile from different angles could support transparency and awareness, for instance by differentiating between how a user profile is presented to contacts, other users or the outside web, together with options to change the modes of presentation. A similar demand is given as regards system designs: these should be widely open to public scrutiny and verifiable as regards their handling of personal information. The use of open standards can contribute to enhance transparency and accountability of SNS.

These potential measures should not be misunderstood as merely technical means but should be supported by accordant policy actions such as:

- Enforce content encryption as standard
- Foster anonymity and pseudonymity
- Strengthen freedom of information and transparency
- Raise awareness for privacy and transparency
- Stimulate innovation for privacy by design
- Strengthen the role of Data Protection Authorities to improve checks and balances

As described above, setting privacy as the default is a core aspect to foster privacy-by-design principles. Several valuable approaches including technical and organisational means in the field of privacy-by-design exist. Innovations in this domain thus need to be stimulated and put forward on larger scale to cope with the privacy challenges. In this regard, the on-going reform of the European data protection legislation can play an important role. As contemporary privacy suffers from *"the imbalanced control over personal information and increasing information asymmetries between the data controller and the individual whose data are processed"* (Strauß 2013), there seems to be a policy vacuum in the currently effective legislation. Observing the on-going reform process, the European Commission seems to be well aware of this vacuum: The current proposal encompasses several relevant issues to support and promote privacy-by-design such as particular norms on data protection by design and by default, a strengthened role of privacy impact assessments, the obligatory creation of data protection officers in companies above a specific size, and the stimulation of economic incentives for privacy-by-design through data protection seals (such as the EuroPriSe seal[73]). In addition, the draft contains several suggestions to improve transparency of data processing, e.g. an obligation for data controllers "*to explicitly inform the data subject on the legitimate interests pursued*" by processing of personal data, the highlighting of purpose limitation and consent, the obligation to notify about data breaches, the provision to individuals of access to data concerning him or herself, the right not to be subject to profiling by means of automated processing as well as the right to be forgotten (COM 2012/11/EC). To cope with contemporary privacy problems related to SNS and beyond demands an effective privacy framework and as next steps improved measures for its practical implementation.

[73] https://www.european-privacy-seal.eu.

6. CONCLUSIONS AND POLICY OPTIONS

6.1. Main findings and concluding remarks

From technological point of view Cloud Computing is more an evolution of existing technologies within the field of distributed computing. Basically it allows the dynamically adapted usage, i.e. need based, of IT resources over a network. First concepts appeared already in the early 1960s, but after some difficult developments in the late 1990s it gained more and more importance in the last decade. Basically, it allows the dynamically adapted, i.e. need based, usage of IT resources over a network. The main difference to previous offers such as Grid Computing is the broadness enabled by different deployment and service models as well as the usability through web interfaces. This is enabled by the application of two main technological features, service orientation in form of web services and multi-tenancy in form of virtualization, as well as a specific three layered architecture. In addition, Cloud Computing demands several technological requirements. Another important aspect is the further evolution of revenue models such as "pay-as-you-go". The underlying idea, in particular for companies, is to turn investments into operational expenses. Altogether, it can lead to new, maybe disruptive changes in business models, but, as shown, the situation is still in a flux. That is also reflected by the fact that the definition, functionalities and characteristics are still not fully settled. There is no universally accepted definition, but the definition of NIST has prevailed in practice. It defines Cloud Computing as *"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."* Similar to the plethora of definitions, there is also a growing number of service, delivery and revenue models. In particular the service and delivery models have become an object of marketing. The same situation can be found in case of the delivery models, where besides the typical delivery models of public, private or hybrid clouds many new terms emerged.

However, a market exists already and it is growing at a high rate. At the moment the market for public Cloud offers grew by nearly 20% per year. For example IDC states that the market grew from 40 bn. $ in 2012 to 47.7 bn. $ in 2013. Also other market segments like Cloud-related IT services or markets for private Clouds show a strong growth. Therefore, it will become an independent and important segment of the software and IT services market in the next years. The common view is that in respect of the different services models the market for the SaaS model will stay the biggest one in the future. Regarding the regional development the US is the biggest market for Cloud Computing at the moment. At the moment, Europe is the second biggest market behind the US and followed by Japan, but it is characterized by smaller growth rates than many other regions, in particular emerging markets like China or India. Typical offers are addressing enterprise administration applications, not industrial ones, as well as consumer-oriented applications. In the last year the number as well as the complexity of offers grew. Consequently the landscape of providers is becoming more differentiated ranging from big, integrated providers (e.g. Amazon, Google) and specialists (e.g. Salesforce, Terremark) to the new group of cloud-born companies (e.g. Dropbox). It is obvious that most of the big and well-known providers are of US origin, which underlines their dominance in the IT industry.

Normally they operate globally. Some of them even have data centres in Europe. Europe still lags behind in the adoption and usage, but the picture might be a little bit more differentiated as drawn by some authors. With regard to the adoption level the differences might be not as big as stated, but for example SMEs in the US adopt it faster. More obvious are the differences in the usage patterns, which show that the usage is less sophisticated in Europe. This means that in particular businesses as well as public services use more and more advanced services.

The history of contemporary SNS is relatively short but turbulent. In practically no time, the variety of applications available and accordingly the user rates increased enormously: big players such as Facebook today count almost one billion users. In their very beginnings, SNS started as niche applications, already in the late 1980s and early 1990s with a first impetus from early web communities and interest groups. The first messaging services appearing during the 1990s created options to connect with other Web users and create contact lists. Few years later, sixdegrees.com, the first profile-based SNS combined different features for self-presentation, managing contacts, and messaging. The user profile today is standard in contemporary SNS and part of their core architecture as profiles are the main entry points to access all functionalities of SNS. The profile-based SNS expedited further developments and facilitated the occurrence of different community-focussed SNS. With increasing usage rates, business-related SNS and SNS devoted to particular interest groups appeared (e.g. the music-focussed MySpace was the most popular site during the early 2000s). After Facebook entered the global stage (in 2003), a broad spectrum of social media services (such as YouTube, Twitter, etc.) became available and SNS became part of the mainstream. Entailed is an on-going trend towards the integration of services and applications, transforming SNS into platforms for a broad spectrum of different features expanding also to the outside Web. Major drivers in this regard are social plugins and social graphs that link SNS and other web environments. This can affect the shape of the World Wide Web in general.

The networking structure of SNS provides a variety of new modes of interactions. The basic functionality of SNS to some extent grounds on classical theories in the field of network analysis: for instance Milgram's (1967) "small world problem", addressing the "six degrees of separation", i.e. that every person globally can be related over six degrees to any other, and Granovetter's (1973) hypothesis of the "strength of weak ties", claiming that loose connections have a strong impact on network expansion as they function as bridges across different network nodes. The growth of SNS environments is coined by these concepts and the variety of types of content available across SNS environments. The design of SNS, primarily their networking structure, contributes much to people connecting worldwide for a variety of purposes. Around the most important reasons for usage, to stay in touch with others, manifold different motivations and usage patterns mirror societal heterogeneity. With their low-threshold options to establish, modulate and extend various network-based relations, SNS highlight and foster the effects of many-to-many interactions. The effects of usage vary, but refer to general networking effects such as the strength of weak ties. To some extended traditional network effects are boosted by enhanced interactivity. In this regard, self-amplifying dynamics are inherent in SNS design: the number of users is likely to grow if interaction among them increases. This significantly contributes to enhanced

options for widespread distribution of information in no time among large numbers of users, groups and communities locally and globally.

The analysis has shown that Cloud Computing and SNS bear potentials for Europe. In particular Cloud Computing offers potentials for economic growth and employment. This is based on the expectation that Cloud Computing and the underlying idea of flexibly usage and payment lead to cost reductions and productivity growths in businesses and public administrations. The span of estimated cost savings reaches from 10 to 30%, but as already mentioned there is only little literature that deals with real cases. So there is a need for further evaluation in practice. Additionally, the question of the total cost of ownership (TCO), which also includes costs for migration and termination, has not yet been answered. In case of consumers, cost savings are seen as less important. Beyond that other positive impacts are growing mobility and flexibility. In the medium to long term, productivity gains are seen as positive impacts, in particular for businesses and public administrations. In the medium to long term other positive impacts like flexibility, mobility or new innovative offers are seen as more important. In the latter case the question is if and how it will happen. Apart from that, another often controversially discussed impact is the professionalization of security management (back up, security, etc.) which comes along with cloud offers and could be a benefit for consumers and SMEs. For consumers factors like convenience are seen as the main impact. All of these impacts are also considered as main drivers for the adoption of Cloud Computing, but there are two points to consider about these possible potentials.

Based on the positive direct impacts, several studies conclude that Cloud Computing enables significant productivity growth that will impact overall growth and employment positively. However, only a very limited number of the analyses tried to determine the size of these effects for Europe or at least for some of the EU member states. In these cases, all studies forecast a significant positive impact on employment and the creation of new business opportunities, which goes along with an overall economic growth. But for two reasons these results have to be interpreted with caution beside the normal challenges of all types of forecasts. Firstly, the underlying calculations are based on estimated cost savings. This is fair due to the lack of empirical values, but normally such estimations tend to be quite optimistic, particularly in early stages of a technology. Secondly, the analyses partly neglect input-output relations and effects, i.e. the fact that job creation in one sector may lead to job destruction in another. The relevance of these points is underlined by some recent literature on the impact of IT in general on employment and growth. This research shows that even realised productivity gains do not automatically lead to the creation of highly-skilled employment. In the worst case, it could even have the opposite effect. This review is not aimed at dismissing the positive expectations and potentials associated with Cloud Computing as a whole, but it is aimed at raising awareness for the fact that these potentials are not exploited automatically. Exploiting them requires that all obstacles are removed as well as that the estimated cost savings can be realized to a certain extent. Moreover, the analysis also showed that beyond addressing obstacles and challenges specific framework conditions like education or infrastructure are required to turn productivity gains into growth of employment.

In case of SNS, the new modes of interactions combined with the self-amplifying dynamic a broad spectrum of positive effects. This significantly contributes to enhanced options for widespread distribution of information in no time among large numbers of users, groups and communities locally and globally. This particular strength supports a variety of positive effects such as stimulating social learning, enabling new modes of participation, strengthening community building, developing social capital and enhancing political empowerment. However, as the case of the Arab Spring Revolutions highlights, the role of SNS for political participation is often ambivalent. The same social media channels that supported activists and democratic movements have been used by authoritarian regimes for control and repression. Hence, without individuals using social media for democratic means this potential lies idle. The many different interactive tools available in SNS also foster the production of new knowledge. This feeds the participatory capacity of SNS as well as knowledge production, particularly in scientific contexts. The large amount of content available via SNS can contribute to mutual learning among users and present valuable sources for various kinds of business models.

Beside the positive impacts, the analysis shows that both technologies also go along with negative impacts. In particular both bear risk for information security, control of data and privacy. In Cloud Computing, there is the risk to lose control over data or that the confidentiality of data is breached as well as the risk that the data is not available when needed, which has impacts for all user types from business, public administration or consumers. For consumers in particular, there is the risk of sacrificing privacy because many advertisement-based or freemium Cloud services like web-based mail services rely on the analysis and reuse of user data. This is underlined by the analysis on SNS, where one major problem is the lacking distinction between user information, interactions, and content. An essential concept that becomes increasingly strained is informational self-determination. SNS highlight that the array of different digital contexts, in which personal information flows through, keeps expanding. Recent innovations, such as the increasing role of social plugins and the social graph, amplify this expansion. As a result, informational self-determination becomes even more complicated as information processing and analysis is in most cases unrecognized at least by the individual users. And even if recognized, the options for users to control their privacy are limited and not sufficient, so that there is need to address privacy protection as a shared responsibility among all stakeholders involved. Cloud Computing also bears further risks. Further risks can arise if a transfer of data is problematic either because data cannot be deleted or technical problems make it difficult. The problem of data portability and beyond that of migration or usage of different providers is even a bigger challenge for businesses and public administrations, because in the worst case vendor lock-in can eventually lead to higher instead of lower costs. Beyond that there are possible negative impacts caused by a lack of availability or even by a loss of data. Finally there there is a widespread fear that Cloud Computing providers and foreign governments abuse data. The effects of the US Patriot Act, the Foreign Intelligence Surveillance Act, and the National Security Letters have been widely discussed in the media. All of these impacts were also identified as barriers for the adoption.

Not surprisingly, Cloud Computing will impact the IT markets and industry itself. According to different market researchers, it can be stated that the share of Cloud Computing in the

overall market for software and IT services will grew from 3 to 5% at the moment to a range of 10 to 20% in the next 5 to 10 years. This fast growth leads to a growing market share, which will impact other traditional market segments. While markets will change, the structure of the industry will not change significantly as it seems today, i.e. the dominance of US-based providers will continue. Nevertheless, the current developments may provide an opportunity for Europe.

These results and recent developments such as the revealing large-scale surveillance of individuals on a global level underline that information security as well as data protection and privacy are challenges that need to be understood and addressed. Moreover recent events like the disclosure of information on large-scale, global mass surveillance by some states or the growing number of cybercriminal activities and its global nature, underline the need to address the challenges of governance. Most recent information security threats in the context of Cloud Computing are directed at the confidentiality of data by unauthorised access from in- or outside. This can be addressed by a reliable, highly secure computer base, which would require secure and open soft- and hardware. Another way to address this challenge could be the use of encryption, which requires that encryption standards are not compromised. Further encryption methods that can be used in Cloud Computing (e.g. homomorphic encryption) or ins SNS (e.g. content encryption) are only in early stages. An alternative would be to explore the possibility of using large, mass-manufactured devices using tamper-detecting membranes. While these countermeasures against a loss of confidentiality also address threats to integrity, threats to availability can be addressed with various existing means, but not entirely, e.g. regarding network outages. As shown, Cloud Computing also challenges the existing data protection regime in Europe by for core problems: 1. The problem of jurisdiction and applicability; 2. The problem of defining roles and responsibilities; 3. The problem of worldwide and continuous data transfer; and, 4. The lack of a binding European interpretation mechanism. The analysis of the regulation draft, which was released by the commission, shows that it addresses these challenges by an clarification and expansion of scope as well as of the distribution of roles and responsibilities. Furthermore it envisages a revamp of the rules allowing international transfers of data; and institutes a number of novel interpretation mechanisms, which will allow it to be bindingly interpreted at European level. It seems important to continue this way to adjust the data protection regime to current and future emerging technologies and developments. Finally it also introduces several novel features (e.g. right to be forgotten, data portability or data protection by design and default), which are also relevant for SNS. Here measures should not least trigger a shift of the prevailing disclosure-by-default paradigm towards a setting where privacy-by-design and privacy-by-default are the leading principles. This is particularly salient in the face of the recent scandals. They highlight urgency for a revitalization of privacy – a concept that is strongly connected to the need to recover the individuals' trust in the system. They also show the governance of Cloud 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. The proposed regulation seeks to provide means for the enforcement of European privacy policy in international markets. Currently, it seems that this approach has support in the European Parliament. 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. The benefits of greater enforceability are obvious. 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. On the other hand, with this approach Europe moves one step closer to the strong-arm style of diplomacy. Maintaining this course may well lead to ripples in the EU-US relationship. And while "Europeanisation" of cloud governance may be preferable to other tendencies of Member State actions, which point towards nationalisation, there are real risks of a global polarization that may spill from matters of ICT governance into other areas. One pathway forward may be a true internationalization of governance structures underlying the functioning of the Internet. Tackling this challenge may contribute to a sea change in ICT governance and a global step forward towards the realization of the liberating potentials of a neutral, open Internet.

Finally the further analyses of drivers and barriers as well as the previous results show that in case of Cloud Computing two other challenges need to be addressed: Legal uncertainty as well as the competitiveness of markets, which includes also suitable framework conditions, and a few technological challenges. Though the market development shows that there is already a vivid Cloud business, the contractual aspects of it is only in an early stage of development with many legal uncertainties. In particular in the business context, the analysis shows that choice of law and applicability of EU law are also in areas beside data protection and third-party access a main concern, because often it is either circumvented by Cloud providers or the EU law itself bears some uncertainties like in the case of IPR. Other important aspects are understandable and standardised contract documents like Acceptable Use Policies (AUP) or Service Level Contracts. This is in particular relevant for smaller companies as well as consumers. Another point is 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. Here new ways of certification and trustmarks are needed. The case of contract termination underpins the fact that different challenges can amplify each other. Together with standardisation and interoperability issues it can be used to create vendor lock-in, which is a barrier for the market competitiveness. Both need to be addressed by clarification and the support for interoperable frameworks.

Other aspects show that market fragmentation, though not Cloud-specific, as well as the lack of innovative companies form barriers to the competitiveness of Europe. The first point refers to a broad set of issues all dealing with challenges to cross-border activities in Europe. There are still issues that need to be addressed to enforce the creation of a single market for digital services, which needs to be completed for a competitive European Cloud market. The second point refers to the lack of fast growing European enterprises becoming global player. As shown by many analyses over the last decade, there is a 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 the focus of the discussion. This includes challenges for procurement as well for financing the founding and growth of companies, that can be addressed. Moreover, the analysis also shows that

exploiting the full potentials of Cloud Computing also requires efforts regarding human capital as well as to reconsider the broadband development in Europe. The first underlines that skilled personnel is fundamental for both providers as well as their users to exploit the potentials of Cloud Computing and related other emerging technologies like Big Data.The latter is important, because it enables more and more digital business, which will lead to a strong increase in the demand for a suitable network infrastructure. Consequently, it is necessary to develop network infrastructures in a way that enables the realization of the potentials. Questions arising from it concern 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. Finally technological challenges such as data management and scalability, which are important for Cloud as enabler for Big Data and other emerging technologies, need to be addressed because the amount of data being processed is growing constantly and as the majority of Web applications are designed to be driven by traditional database software and porting them to utilize alternative data stores is often not feasible

Overall this analysis of impacts and challenges underlines that action is necessary to address these issues. Though there are positive effects for citizens and businesses, they will possibly not adopt these technologies as long as these risks exist. As a consequence positive economic and societal potentials at large cannot be realized. In particular the recent disclosures on the practices of the NSA and similar institutions as well as the behavior of some private sector actors have potential to undermine the trust into these technologies; not to mention the possible cybercriminal activities around it. Normally, a situation like this is then often coined by the contradiction of interests, but also the IT and internet , in particular the US based one as shown by their open letter claiming for more global surveillance governance[74], started to realize that trustworthiness is in the long run a critical factor for their business. This situation offers new opportunities for Europe and creates some reasons to take action in Europe now. The first one is the need for a holistic approach. The analysis shows that neither more technological solutions nor more regulations nor new governance structures will solve the problems alone. Only a combination of strong security, modern and appropriate privacy regime, fair legal environment and improved governance structures will assure that potentials for misuse can be minimized. The second reason to take action is that this would Europe allow to use the chance to gain more importance and influence in the global discussion on the principles of modern digital life and economy for two points. The exploitation potentials could strengthen the European competiveness overall and in particular in the digital economy and society. Secondly this would enable Europe to have a more active and influential role in the international discussions and decisions on the underlying principles. Finally, strongly related to the second reason, it also offers a chance to boost the European ICT and in particular industry which is lagging behind by addressing weaknesses, while making Europe to a trustworthy partner for data.

6.2. Suggestions for policy options

The overall conclusions show that – due to the circumstances such as the NSA affair – at the moment, there is a unique chance to achieve multiple Cloud Computing related goals

[74] See http://97.74.205.113/.

simultaneously. There are no contradictions in assuring European citizens secure, privacy aware, legally certain and fair use of Cloud Computing and SNS and in increasing the competitiveness of European ICT industries. Moreover it is possible to exploit the potential of Cloud Computing and SNS to the benefit of both the European economy and society at large.

Consequently the aim of the last step of the project was to prioritize the identified policy measures. This process was threefold. A first step was to identify guiding ideas based on the unique chance described above, while reviewing and analyzing the different policy measures described and evaluated in the previous chapters. This was based on the overall idea to ensure that European citizens and businesses can use Cloud Computing and SNS without having difficulties with security, privacy or further legal uncertainties and thereby create a competitive advantage for the European ICT industries as an attractive, reliable and secure location for business. The policy options were grouped into four thematic blocks (described in detail below):

- **Make security a commodity**
- **Establish privacy as a location advantage**
- **Build a trustworthy environment for digital business and living**
- **Create an inspiring ecosystem for ICT industries**

In a second step, the results of the review of the different measures were used to identify complementarities and possibilities to combine measures. This was aimed at reducing the number of measures as well as to detect interrelations that could influence the successful implementation of the different measures. Moreover, it could also lead to the identification of new measures resulting from this analysis. It also included mapping of all measures to the thematic blocks named before. Based on these results the last step was the selection of the most promising measures that form a coherent and consistent set of options for European policy makers. The guiding principle for this selection was that the selected options should address relevant specific challenges and be measurable, acceptable (for all stakeholders), realistic and time-depended.

Overall this approach led to the following set of 16 policy options.

Make security a commodity

At the moment IT security is sometimes difficult. Solutions can be hacked, even if, e.g. a powerful crypto system has been used, or they sometimes they are inconvenient to use for normal users. Therefore it is necessary to support the development of highly secure IT solutions, which are easy to use and which can be adopted by all businesses, both big and small, as well as by all citizens.

1. **Support the development of open and secure software and hardware and encryption methods:** The development of secure open soft- and hardware, which does not contain any backdoors, potential for zero-day exploits, etc., as well as of encryption methods, for instance content or homomorphic encryption, should be explored. For practical usability, it should be compatible with existing software and easy to understand. The latter could be realized using, for instance, virtualization. This should initially be supported by means such as research funding. In addition, the

development of these highly secure soft- and hardware could additionally be encouraged, for instance, by (pre-commercial) procurement policies or by making it mandatory in some sectors.

2. **Encourage the use of checklists and certifications:** To address the day-to-day risks of Cloud Computing, the use of checklists for keeping systems secure could be encouraged, as should the use of sufficient backups, etc. The use of comprehensive security policies could be certified. Breaches should at least be reported to the certifying institution. In the medium run, certification could show the use of secure computers or secure virtualisation.
3. **Assess the economic viability of large hardware security modules:** To allow confidential processing of data in the Cloud, it could be estimated what such processing in remote tamper-resistant modules would cost when applied on a large scale. This is regarded to be more expensive, but the concrete cost penalty is unknown.
4. **Initiate a dialogue on the structure and governance of the Future Internet:** A high-level dialogue with Internet infrastructure organizations such as ICANN, IANA, IETF and others about the future infrastructure of the Internet and the internationalization of its governance should be established.

Establish privacy as a location advantage

For a long time, European data protection standards were seen as a disadvantage for digital business. Recent developments, as well as changing requirements for emerging technologies and a growing digitalization of all spheres, underpin the necessity of modern privacy rules. By modernizing the data protection regime Europe could not only ensure a better protection of citizens, but also serve as a model for emerging markets, which could be attracted to increase their exchange with Europe. Moreover Europe could underpin this function as an example for modern and appropriate privacy regime by addressing a fair and secure governance and proposing a structure of an open Internet at a global level.

1. **Proceed with the modernization of data protection:** Support, and if possible expediate, the current process of data protection reform, in particular the clarification of data protection principles relating to cloud computing. This includes the support of the choice of a Regulation as the legal instrument, the strengthening of pre-existing individual rights in the Regulation, the range of new rights offering further control to the data subject (e. g. portability, deletion), as well as the range of novel obligations for the data controller and the accountability principle
2. **Establish the principles of security and privacy by design:** Look further into ways of developing and promoting architectures for Cloud Computing and SNS designed from the beginning to a high level of security as well as privacy by design[75] rather than only by trust or legislation.
3. **Support the creation of a European Data Protection Board:** Support European level consistency and interpretation mechanisms and the creation of a European Data Protection Board.
4. **Ensure the extraterritorial application of European data protection law:** Leave the safe harbor agreement and explore and implement options to ensure the

[75] "Privacy by design" could mean to use, e.g. pseudonyms of attribute-based credentials (showing e.g. that somebody is of a certain age).

extraterritorial application of European data protection law as foreseen in the current draft of the regulation.

Build a trustworthy environment for digital business and living

Digital life of citizens and business needs legal certainty to ensure new ideas are taken up. Since many emerging technologies in ICT create both new chances and new challenges, there is need to continually review existing legislation and to adjust it if necessary. Only if people have trust in legal certainty, they will adopt and use new technologies and exploit their potential for the economy and society as a whole.

1. **Stipulate the setting of minimum requirements for contracts:** Support proposals to stipulate minimum requirements regarding changes to the provisions of contracts, the notification of such changes and remedies for those clients for whom changes are materially significant.
2. **Support the standardization of Acceptable Use Policies and Service Level Agreements:** Encourage standardization of Acceptable Use Policies and Service Level Agreements as well as support proposals for model clauses and the language for both.
3. **Eliminate jurisdictional uncertainty:** Consider support for proposals that address issues relating to jurisdictional uncertainty. This may include supporting initiatives to stipulate compliance with EU law, minimum requirements regarding the disclosures to a third country and obligatory use of Mutual Legal Assistance Treaties.
4. **Support the development of certifications:** Support proposals for the development of EU cloud-specific certification, which are meaningful, e.g. in regard to privacy contains automatic information of DPA in case of any access by others. Promote their use through the adoption by public sector organizations within the EU.

Create an inspiring ecosystem for ICT industries

A crucial precondition for a competitive ICT industry is an inspiring ecosystem. This is illustrated by examples in other regions (Silicon Valley, Israel) or other industries (cars, machine equipment). Such ecosystems contain many components. Of particular importance is support for innovative and fast growing companies as well as the provision of sufficient framework conditions.

1. **Encourage the creation of European market players:** Support the creation of new disruptive developments in technology and business models such as really secure platforms for mobile devices or business exploiting the potentials of the Cloud and SNS ecosystem.
2. **Support standardization and interoperability:** Support the efforts for standardization and interoperability in Cloud Computing and SNS to enable a vivid European market. This is aimed at preventing the misuse of market power for setting de facto standards for example in the field of data portability as well as corrupting encryption standards. Possible ways to achieve this could the adoption in public services or strengthening of the role of European bodies like ENISA or ETSI.
3. **Empower people across all strata of society:** Empower people by supporting the appropriate education of a sufficient number of people, users as well as developers. The first refers to both technological knowledge and to knowledge as to the potentials and risks of emerging technologies such as Cloud Computing and SNS. The latter refers to the support of the integration of groups less represented in the ICT and related industries such as women, elderly people or people with less formal education.

4. **Reconsider current broadband strategies:** Review the progress and methods of the different EU member states and elsewhere. Possible examples are Sweden or Japan. Based on this identify and adopt best practices. This includes addressing the problem of financing infrastructures ensuring an appropriate balance of interests for all stakeholders. Furthermore, increased competition between fixed, licensed and unlicensed communications would be supportive.

ANNEX A: 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.

ANNEX B: SUMMARY OF THE WORKSHOP

The workshop "The Potentials of Cloud Computing for Europe" which was held on 2 October 2013 as part of the 5th European Innovation Summit at the EP was part of this project. It aimed at discussing the potentials in general and the key findings of the ETAG project team in particular with both recognized experts and the public.

Programme

10.00 Welcome address by António Fernando Correia De Campos MEP, STOA chairman
10.10 Introduction to the projects and review of socio-economic potentials of Cloud Computing; Dr. Arnd Weber, KIT-ITAS
10.25 EU data protection strategy for the Cloud; Caspar Bowden, independent privacy researcher
10.40 Challenges of Cloud Computing – a consumer perspective; Chiara Giovannini, ANEC
10.55 Challenges of Cloud Computing – a business perspective; Dr. Theo Lynn, Dublin City University / Irish Centre for Cloud Computing and Commerce
11.10 Future competitiveness of the EU ICT sector in emerging ICT technologies; Prof. Dr. Reinhilde Veugelers, KU Leuven / Bruegel
11.25 EU Cloud Computing Strategy; Jorge Gasos, European Commission DG Connect
11.40 Roundtable discussion with Members of Parliament, experts and auditorium
12.30 End of workshop after closing remarks

After a welcome address by the member of the EP and STOA chairman António Fernando Correia De Campos, Dr. Arnd Weber from the Institute for Technology Assessment and Systems Analysis of the Karlsruhe Institute of Technology introduced the research project. Among the invited experts were Chiara Giovannini from ANEC, the independent privacy researcher Caspar Bowden, Dr. Theo Lynn from the Dublin City University's Irish Centre for Cloud Computing and Commerce, Prof. Dr. Reinhilde Veugelers from KU Leuven and Dr. Jorge Gasos from the European Commission's Directorate General Connect. Comparisons of the current states in Europe and the US as well as deliberations on the interactions among the two economic regions played key roles during the lively discussions at the workshop. The advantages of US Cloud providers in terms of economies of scale and the lack of resources for non-R&D innovation and public procurement in Europe were addressed as well as challenges related to information security and data protection. In this respect, the spying practices of US agencies made public by Edward Snowden, risks resulting from backdoors in software and hardware, and deficiencies concerning the legal situation were brought up.

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.
- Acquisti, A. and Gross, R. (2006): Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, in: Danezis, G. and Golle, P. (Eds): PET 2006, Heidelberg Springer, 36-58.
- Agrawal, D.; Abbadi, A. E.; Antony, S.; and Das, S. (2010): Data Management Challenges in Cloud Computing Infrastructures, in: *Databases in Networked Information Systems, 6th International Workshop, DNIS 2010*, volume 5999, of *Lecture Notes in Computer Science*, 1-10, 2010.
- 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.
- Amanda, L. and Mary, M.(2007): Social networking websites and teens: an overview: Pew Internet and American Life Project <http://apo.org.au/?q=node/16749>.
- Amazon (2013b): Case Studies. Retrieved from https://aws.amazon.com/en/solutions/case-studies/, 07/23/2013.
- Anandasivam, A./Buschek, S/Buyya, R. (2009): A Heuristic Approach for Capacity Control in Clouds, in: Proceedings of 2009 IEEE Conference on Commerce and Enterprise Computing, Los Alamitos, 90—97.
- and the Future Internet Public-Private Partnership, Brussels.
- Article 29 Data Protection Working Party (2007): Opinion 4/2007 on the concept of personal data: WP 136.
- Article 29 Data Protection Working Party (2009): Opinion 5/2009 on online social networking <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf >.
- Article 29 Data Protection Working Party (2009): Opinion 5/2009 on online social networking <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf >.
- Article 29 Data Protection Working Party (2010): European data protection group faults Facebook for privacy setting change (Press release, 12 May) <http://ec.europa.eu/justice/policies/privacy/news/docs/pr_12_05_10_en.pdf>.
- 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.
- Auffray, Christophe (2012): Cloud Andromède : un projet sinon rien pour Dassault Systèmes, in:: ZDNet, April 2, 2012 (http://www.zdnet.fr/actualites/cloud-andromede-un-projet-sinon-rien-pour-dassault-systemes-39770291.htm).
- 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.
- Baringhorst, S. (2009): Introduction. Political Campaigning in Changing Media Cultures - Typological and Historical Approaches, in: Baringhorst, S., Kneip, V. and Niesyto, J. (Eds): Political Campaigning on the Web, Bielefeld, 9-30.
- Barnes, S. B. (2006): A privacy paradox: Social networking in the United States, First Monday 11(6).
- 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/).
- Baun, C. et al. (2011): Cloud Computing – Web-Based Dynamic IT Services. Springer.
- BBC (2013): Child abuse sites on Tor compromised by malware. 5 August 2013. http://www.bbc.co.uk/news/technology-23573048 .
- Becker, Georg; Regazzoni, Francesco; Paar, Christof; Burleson, Wayne (2013): Stealthy Dopant-Level Hardware Trojans. CHES 2013. http://people.umass.edu/gbecker/BeckerChes13.pdf .
- Benkirane, R. (2012): The Alchemy of Revolution: The Role of Social Networks and New Media in the Arab Spring. GCSP Policy Paper, No. 2012/7, edited by Geneva Center for Security Policy.
- Biermann, K. (2010): Facebook, bing und Skype vernetzen sich, Zeit Online, 15.10. <http://www.zeit.de/digital/internet/2010-10/facebook-bing-skype>.
- 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.
- Bloomberg (2012): IDC Forecasts Public IT Cloud Services, (http://www.bloomberg.com/article/2012-09-11/avwhMWO4XHw4.html).
- 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.
- Bohn, R. B./Liu, F./Tong, J./Mao, J./Messina, J.V./Badger, M.L./Leaf, D.M (2011): NIST Cloud Computing Reference Architecture, Washington, D.C. (NIST SP - 500-292).
- Bonneau, J., Anderson, J., Anderson, R. and Stajano, F. (2009): Eight friends are enough: Social graphs approximation via public listings, in: SNS 2009, 13-18 <http://www.cl.cam.ac.uk/~rja14/Papers/8_friends_paper.pdf>.
- Borgmann, M./Hahn, T./Herfert, M./Kunz, T./Richter, M./Viebeg, U./Vowé, S. (2012):On the Security of Cloud Storage Services, Darmstadt (SIT Technical Report SIT-TR-2012-001)
- Borja, Florence (2012): Cloud Computing in Europe Lagging Behind, in: Cloud Times, September 12, 2012, (http://cloudtimes.org/2012/09/11/cloud-computing-europe/).
- Bowden, C. (2013c): The US surveillance programmes and their impacts on EU citizen's fundamental rights; European Parliament, Policy Department C – Citizen's Rights and Constitutional Affairs; PE 474-405. Available at: http://www.europarl.europa.eu/studies
- Bowden, Caspar (2013a): The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights. Briefing Note. Brussels.

- Bowden, Caspar (2013b): Cloud computing, mass-surveillance and Data Protection. Presentation given at STOA, Brussels, Oct. 2, 2013.
- Boyd, D. M. and Ellison, N. B. (2007): Social Network Sites: Definition, History, and Scholarship, Journal of computer-Mediated Communication 13(1), 11 <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.
- Bradshaw, S./Millard, C./Walden, I. (2010): Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper 63. (http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1662374_code468680.pdf?abstractid=1662374&mirid=1).
- 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.
- 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.
- Business wire(2013): NTT Com Security Survey http://www.businesswire.com/news/home/20131015006209/en/NTT-Security-Survey-North-American-Businesses-Lead.
- Cachia, R. (2008): Social Computing: Study on the Use and Impact of Online Social Networking. IPTS Exploratory Research on the Socio-economic Impact of Social Computing: JRC Scientific and Technical Reports - Institute for Prospective Technological Studies (IPTS) - European Commission <http://ftp.jrc.es/EURdoc/JRC48650.pdf >.
- Cain, J., Scott, D. R. and Akers, P. (2009): Pharmacy Students' Facebook Activity and Opinions Regarding Accountability and E-Professionalism, American Journal of Pharmaceutical Education 73(6), Artikel 104 <http://www.ajpe.org/aj7306/aj7306104/aj7306104.pdf>.
- Carr, N. G. (2005): The end of corporate computing, in: MIT Sloan Management Review, 46(3), 67—73.
- Castillo Vera (2013a): Draft Report on unleashing the potential of cloud computing in Europe (2013/2063(INI)). Committee on Industry, Research and Energy. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-506.114&format=PDF&language=EN&secondRef=01 10/27/2013 .
- Castillo Vera (2013b): Amendments 1 - 62. Draft report on unleashing the potential of cloud computing in Europe (2013/2063(INI)). Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-516.774+01+DOC+PDF+V0//EN&language=EN 10/27/2013 .
- Castro (2013): How Much Will PRISM Cost the U.S. Cloud Computing Industry? ITIF, August 2013 (http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry).
- Cattaneo, Gabriella/Kolding, Marianne/Bradshaw, David/Folco, Guiliana (2012a): Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up. D2 – Interim Report, Brussels (Smart 2011/0045).
- Cattaneo, Gabriella/Kolding, Marianne/Bradshaw, David/Folco, Guiliana (2012b): Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely

Barriers to Take-up. D2 – Interim Report Statistical Annex, Brussels (Smart 2011/0045).
- Cattaneo, Gabriella/Kolding, Marianne/Bradshaw, David/Folco, Guiliana (2012c): Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up. D3 – Final Report, Brussels (Smart 2011/0045).
- Cattedu (2011): Security and Resilience in Governmental Clouds. Making an informed decision. ENISA.
- Cattedu and Hogben (2009b): An SME perspective on Cloud Computing - Survey. ENISA.
- Cavoukian, A. (2009): Privacy by Design … Take the Challenge'; in series: Information and Privacy Commissioner of Ontario, Canada <http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf>.
- 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.
- Chellappa, R.K. (1997): Intermediaries in Cloud-Computing: A New Computing Paradigm, INFORMS Annual Meeting, Dallas, TX, October 26-29, 1997.
- Clarke, R. C. (2006): What's 'Privacy'? <http://www.rogerclarke.com/DV/Privacy.html>.
- CLG (Communities and Local Government) (2008): Online social networks research report, London: Communities and local government publications.
- Cloud Industry Forum (2012): USA Cloud Adoption & Trends 2012, High Wycombe.
- Colt (2011): European CIO Cloud Survey, London (http://www.colt.net/cdnucm/groups/public/@cdn/@public/documents/generalcontent/cdnp_005990.pdf).
- ComScore (2012): More than Half of People that Access Social Networks on their Smartphone do so on a Near Daily Basis. comScore data mine (February 29) <http://www.comscoredatamine.com/2012/02/more-than-half-of-people-that-access-social-networks-on-their-smartphone-do-so-on-a-near-daily-basis>.
- 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.
- CPNI (2012): National Infrastructure Protection. Emerging Technologies. April 2012. http://www.cpni.gov.uk/documents/publications/2012/2012014-national_infrastructure_protection_emerging_technologies.pdf?epslanguage=en-gb .
- Cusumano, M. (2004): The business of software, Cambridge/Mass.
- Dahlgren, P. (2013): Do social media enhance democratic participation? - The importance and difficulty of being realistic. Policy Paper No. 4/2013, edited by Rosa Luxemburg Stiftung Berlin <http://www.rosalux.de/fileadmin/rls_uploads/pdfs/Standpunkte/policy_paper/PolicyPaper_04-2013.pdf >.
- Darpa (2012): Information Innovation Office. Access 17.3.2012. http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_%28CRASH%29.aspx .
- Das, Sudipto; Divyakant Agrawal, and Amr El Abbadi (2010): G-Store: a scalable data store for transactional multi key access in the cloud, in: *Proceedings of the 1st ACM symposium on Cloud computing* (SoCC '10). New York, NY, 163-174.

- Dasilva, N. (2013). *Q&A on European data protection reform.* Background note, European Parliament. Available at: http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform
- Debatin, B. and Lovejoy, J. P. (2009): Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, Journal of Computer-Mediated Communication 15.
- Dignan, Larry (2011): Cloud computing market: $241 billion in 2020, in: ZDNet, April 22, 2011, (http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702).
- Dignan, Larry (2012): Oracle, Ellison and fun with cloud computing sound bites, in: ZDNet, May 31, 2012. (http://www.zdnet.com/blog/btl/oracle-ellison-and-fun-with-cloud-computing-sound-bites/78720).
- DIW (2010): Economic implications of Cloud Computing, Berlin.
- 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.
- Durkee, David (2010): Why Cloud Computing Will Never Be Free, in: ommunications of the ACM, 53(5), 62-69.
- Dwyer, C., Hiltz, S. and Passerini, K. (2007): Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, in: Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09 - 12 2007: Association for Information Systems <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.148.9388&rep=rep1&type=pdf>.
- Ecorys (2010): The competiveness of EU SME's in the ICT service sector. Rotterdam.
- Ecorys et al.(2009): The competiveness of EU SME's in the ICT service sector, Rotterdam.
- 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.
- Ellison, N. B. and Boyd, D. (2013): Sociality through Social Network Sites, in: Dutton, W. H. (Ed.): The Oxford Handbook of Internet Studies, Oxford: Oxford University Press, 151-172.
- Ellison, N. B., Steinfield, C. and Lampe, C. (2007): The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites, Journal of Computer-Mediated Communication 12, 1143-1168 <http://www.mvirtual.com.br/midiaedu/artigos_online/facebook.pdf>.
- Elmer, G. (2004): Profiling Machines, Cambridge, MA: MIT Press.
- Elsner, Jens; Weber, Arnd (2013): Using the lower UHF bands for Commons & Events. Paper presented at ITS Europe, Florence 2013 (http://www.econstor.eu/dspace/handle/10419/72523).
- Endeshaw, A. (2001): "The Legal Significance of Trustmarks." In Information & Communications Technology Law, vol. 10(2), pp 203-230.

- Ericsson (2012): Ericsson Mobility Report - on the pulse of the networked society <http://www.ericsson.com/ericsson-mobility-report>.
- ESA (2009): European Software Industry: looking for a competitive advantage. European Software Association. Brussels.
- Esteves Rui (2011): A taxonomic analysis of cloud computing, Lisbon (http://idpcc.dcti.iscte.pt/docs/Papers_1st_Doctoral_Workshop_15-6-2011/RuiEsteves.pdf).
- 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. (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. (2011a): 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 (2011a): 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 (2009): Safer Social networking principles <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf>.
- 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 (2012a): Impact Assessment Accompanying the General Data Protection Regulation: SEC (2012) 72 final.
- European Commission (2012b): 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 (2012c): Unleashing the Potential of Cloud Computing in Europe: COM(2012) 529 final.
- European Commission (2013): Digital Agenda Scoreboard 2013, Brussels.
- European Commission (EC) (2011) *Cloud Computing: Public Consultation Report.* Information Society and Media Directorate-General. Converged Networks and Services, Software & Service Architectures and Infrastructures**.** Brussels, 5th December 2011.
- European Commission Decision (2013): Horizon 2020, Work Program 2014-2015. Brussels, C (2013)8631 of 10 December 2013.
- European Commission. (2012): A European Consumer Agenda - Boosting confidence and growth, COM 2012/225/EC, Brussels.
- European Council (2013): European Council , 24/25 October 2013 Conclusions, EUCO 169/13.
- 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 (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.
- Ferdig, R. E., Dawson, K., Black, E. W., Black, N. M. P. and Thompson, L. A. (2008): Medical students' and residents' use of online social networking tools: Implications for teaching professionalism in medical education, First Monday 13(9) <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2161/2026>.
- 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.
- Finn, R. L., Wright, D. and Friedewald, M. (2013): Seven Types of Privacy, in: S. Gutwirth et al. (Ed.): European Data Protection: Coming of Age, Dordrecht: Springer Science+Business Media < http://works.bepress.com/michael_friedewald/60>.
- Forrester (2012): Personal Cloud Services Emerge To Orchestrate Our Mobile Computing Lives, Cambridge/Mass.
- Fransman, M. (2011): The evolving ICT industry in Asia and the implications for Europe, Sevilla.
- Fraser, M. and Dutta, S. (2008): Throwing Sheep in the Boardroom: How Online Social Networking Will Transform Your Life, Work and World Hoboken et al.: Wiley.
- Frazer, N. (2007): Transnationalising the Public Sphere: On the Legitimacy and Efficacy of Public Opinion in a Post-Westphalian World, Theory, Culture and Society 24, 7-30.
- Fuchs, C. (2009): Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance, Salzburg/Wien: ICT&S Center (University of Salzburg), Forschungsgruppe Unified Theory of Information <http://twinic.com/duploads/0000/0509/ICT_Use_-_MySpace_Facebook_2008.pdf >.
- Garfinkel, S. (1999): Garfinkel, Simson (1999). Abelson, Hal, ed. *Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT*. MIT Press.
- Gartner (2008): Hype Cycle for emerging technologies, Stamford (http://www.gartner.com/it/page.jsp?id=739613).
- Gartner (2009): Gartner Highlights Five Attributes of Cloud Computing Stamford, (http://www.gartner.com/it/page.jsp?id=1035013).
- Gartner (2012): Gartner Says Cloud Adoption in Europe Will Trail U.S. by At Least Two Years, May 31, 2012, Egham (http://www.gartner.com/it/page.jsp?id=2032215).
- 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 (2013a): Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion; (http://www.gartner.com/newsroom/id/2352816).
- Gartner (2013b): Forecast: Public Cloud Services, Worldwide, 2011-2017, 3Q13 Update; (https://www.gartner.com/doc/2598217).

- Giron, Frederic et al. (2009): The European Software and Software Based Services Industry, Brüssel.
- 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.
- Goodman, R. (2013): Is the Draft UN Resolution on the Right to Privacy a Trojan Horse for Libertarians? Justsecurity.org, December 4, 2013.
- Granovetter, M. S. (1973): The Strength of Weak Ties, American Journal of Sociology 78(6), 1360-1380.
- Grawrock, D. (2006): The Intel Safer Computing Initiative. Intel Press.
- Greenwald and MacAskill (2013): NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 07/07/2013.
- Greif, B. (2012): Reporter ohne Grenzen stuft zwölf Staaten als Feinde des Internets ein.
- Gross, R. and Acquisti, A. (2005): Information Revelation and Privacy in Online Social Networks (The Facebook case), in: Atluri, V., De Capitani di Vimercati, S. and al. (Eds): Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES 2005, Alexandria, VA, USA, November 7: ACM Press, 71-80.
- Guardian (2013a): Revealed: how US and UK spy agencies defeat internet privacy and security. 6.9.2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security .
- Guardian (2013b). XKeyscore presentation from 2008 – read in full. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation .
- Guardian (2013c): (Snowden documents). http://s3.documentcloud.org/documents/784159/sigintenabling-clean-1.pdf .
- Guardian (2013e): Edward Snowden revelations prompt UN investigation into surveillance. http://www.theguardian.com/world/2013/dec/02/edward-snowden-un-investigation-surveillance .
- Guardian (2103d): NSA Files: Decoded. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 .
- Habermas, J. (1989): The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society (original work: "Strukturwandel der Öffentlichkeit 1962, Hermann Luchterhand Verlag), Cambridge MA: The MIT Press.
- Hargittai, E. (2007): Whose Space? Differences Among Users and Non-Users of Social Network Sites, Journal of Computer-Mediated Communication 13(1), 276–297 <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00396.x/pdf>.
- Harmon, R./Demirkan, H./Hefley, B./Auseklies, N. (2009): Pricing Strategies for Information Technology Services: A Value-Based Approach, in: Proceedings of 42nd Hawaii International Conference on System Sciences, 1—10.
- Häusler, S. (2007): Soziale Netzwerke im Internet. Entwicklung, Formen und Potenziale zu kommerzieller Nutzung, Saarbrücken: VDM Verlag Dr. Müller.
- Hazlett, Thomas (2013): Conference: Daddy, What's a Broadcast Television Network? Nov. 15, 2013. http://iep.gmu.edu/conference-daddy-whats-a-broadcast-television-network/ .

- Heidemann, J. (2010): Online Social Networks – Ein sozialer und technischer Überblick., Informaktik-Spektrum 33 (2010), 262-271.
- Heiser, G. (2013): Protecting eGovernment Against Attacks (White Paper). In: Jacobi et al. 2013a .
- Henschen (2012): Salesforce.com Revenues Surge, But Should You Ignore Losses? ; (http://www.informationweek.com/applications/salesforcecom-revenues-surge-but-should-you-ignore-losses/d/d-id/1107539?).
- Hoefer, C.N./ Karagiannis, G. (2010): Taxonomy of cloud computing services, in: IEEE Globecom 2010 Workshop on Enabling the Future Service-Oriented Internet Proceedings, (http://eprints.eemcs.utwente.nl/19203/01/05700157.pdf).
- Hoffman, E. S. (2009): Evaluating Social Network Tools for Distance Learning, TCC 2009 Proceedings, 92-100.
- 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. (2012b): 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.
- 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.*
- Hoorens et al. (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.
- Hoorens et al. (2012): Towards a competitive European Internet industry. A socio-economic analysis of the European Internet industry
- Humphreys, L. (2010): Mobile social networks and urban public space, New Media Society, 1-16 <http://www.asc.upenn.edu/news/2010/Humphreys_journal.pdf>.
- 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).
- IDC (2013a): IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation: (http://www.idc.com/getdoc.jsp?containerId=prUS24298013).
- IDC (2013b): IDC MarketScape: Worldwide Cloud Professional Services 2013 Vendor Analysis (http://idcdocserv.com/242401e_IBM).
- IDC (2013c): IDC Forecasts Worldwide Spending on Hosted Private Cloud Services to Surpass $24 Billion in 2016; (http://www.idc.com/getdoc.jsp?containerId=prUS23972413).
- IETF 88, (2013): *Hardening the Internet*. Presentation for IETF 88 Technical Plenary. Available at https://datatracker.ietf.org/meeting/88/materials.html#wg-plenaryw
- Islam, M. B. and Iannella, R. (2012): Privacy by Design: Does it matter for social networks?, in: B. Crispo et al. (Ed.): Privacy and Identity Management for Life IFIP Advances in Information and Communication Technology Berlin/Heidelberg: Springer, 207-220 <http://link.springer.com/chapter/10.1007/978-3-642-31668-5_16>.
- Jacobi, A.; Folker, M.; Kool, L.; Munnichs, G.; Weber, A. (2012): Security of eGovernment Systems. Case Study Report; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Security%20of%20eGovernment%20-%20Case%20Study.pdf .

- Jacobi, A.; Jensen, M.; Kool, L.; Munnichs, G.; Weber, A. (2013b): Security of eGovernment Systems. Policy Options Assessment and Project Conclusions; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Security%20of%20eGovernment%20Final%20Report.pdf .
- 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.
- Jin, L., Chen, Y., Wang, T., Hui, P. and Vasilakos, A. V. (2013): Understanding user behavior in online social networks: a survey, IEEE Communications Magazine September.
- Johnson (2013); Silicon Vally: NSA spying cloud prove costly to bay Area and other businesses, experts say; (http://www.siliconvalley.com/news/ci_24437687/nsa-spying-could-prove-costly-bay-area-and?source=most_viewed#).
- Kalenda, Florian/Pößneck, Lutz (2011) : Bericht: "Bundes-Cloud" für deutsche Firmen und Behörden in Planung, , in : ZDnet, December 19, 2011, (http://www.zdnet.de/41558883/bericht-bundes-cloud-fuer-deutsche-firmen-und-behoerden-in-planung/).
- Kann, M. E., Berry, J., Gant, C. and Zager, P. (2007): The Internet and youth political participation, First Monday 12(8).
- Kelly (2011): IBM: Cloud Computing to Contribute $7 Billion in Revenue by 2015 ; (http://www.ciozone.com/index.php/Cloud-Computing/IBM-Cloud-Computing-to-Contribute-$7-Billion-in-Revenue-By-2015.html).
- Khajeh-Hosseini, A./Sommerville, I./Sriram, I. (2010): Research Challenges for Enterprise Cloud Computing. ArXiv preprint (http://arxiv.org/abs/1001.3257).
- Kleinfeld, J. S. (2002): The small world problem, Society 39(2), 61-66 <http://www.stat.cmu.edu/~fienberg/Stat36-835/Kleinfeld_SWP.pdf>.
- 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 (2013a): Break through the cloud adoption barriers -KPMG cloud-service-providers-survey.
- KPMG (2013b):The-cloud-takes-shape – Global cloud survey: the implementation challenge.
- 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.
- 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.

- Kuhlmann, D., Weber, A. (2009): The Evolution of the OpenTC Architecture Illustrated via its Proof-of-Concept-Prototypes. OpenTC Final Report. Bristol, Karlsruhe, http://www.opentc.net/ .
- Kundra, Vivek (2011): Federal Cloud Computing Strategy, Washington, D.C. .
- 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.
- LaMonica, Martin (2005): Utility Computing: IT-Services demnächst aus der Steckdose?, in: ZDNet, July 25, 2005, (http://www.zdnet.de/39135103/utility-computing-it-services-demnaechst-aus-der-steckdose/).
- Laugesen, Nicolai S. (2011): Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements, Copenhagen.
- Layo, Irmee (2012): Gartner: 'Personal Cloud' to Replace Traditional Business IT Solutions by 2014 in: Cloud Times, March 22, 2012, (http://cloudtimes.org/2012/03/22/personal-computers-will-be-traded-for-personal-cloud-by-2014/).
- Leenes, R. (Ed.) (2010): Context is everthing: sociality and privacy in Online Social Network Sites, Heidelberg/Berlin/New York: Springer.
- 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).
- Leskovec, J. and Horvitz, E. (2008): Worldwide buzz: Planetary-scale views on a large instant-messaging network, in: Proceedings of the 17th international conference on World Wide Web, April 21-25, Beijing, 915-924.
- Levine, P. (2002): Can the Internet save democracy? Toward an on-line commons, in: Hayduk, R. and Mattson, K. (Eds): Democracy's moment: Reforming the American political systems, New York, 121-137.
- Lewis, K., Kaufman, J. and Christakis, N. (2008): The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network, Journal of Computer-Mediated Communication 14(1).
- Lindner, R. (2007): Politischer Wandel durch digitale Netzwerkkommunikation?, Wiesbaden.
- Lindner, R., Beckert, B., Aichholzer, G., Strauß, S. and Hennen, L. (2011): E-public, e-participation and e-voting in Europe - prospects and challenges; Final Report, commissioned by: Science and Technology Options Assessment (STOA)/European Parliament, Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung,.
- Livingstone, S. (2008): Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression, New media & society 10(3), 393-411 <http://eprints.lse.ac.uk/27072/1/Taking_risky_opportunities_in_youthful_content_creation_%28LSERO%29.pdf>.
- 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.

- Macintosh, A. (2003): Using Information and Communication Technologies to Enhance Citizen Engagement in the Policy Process, in: OECD (Ed.): Promise and Problems of E-Democracy. Challenges of Online Citizen Engagement, Paris, 19-142.
- Mack, D., Behler, A., Roberts, B. and Rimland, E. (2007): Reaching Students with Facebook: Data and Best Practices, Electronic Journal of Academic and Special Librarianship 8(2) <http://southernlibrarianship.icaap.org/content/v08n02/mack_d01.html>.
- Marston, Sean et al. (2011): Cloud Computing – the business perspective, in: Decision Support Systems 51 (2), 176–189.
- Maxwell, W., Wolf, W. (2012): *A global reality: Governmental Access to Data in the Cloud. Maxwell_Revised Go*vernment 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/ .
- McDonagh, M. (2012): "Review of the Regulatory and Legal Environment for Cloud Computing in the EU" Irish Centre for Cloud Computing and Commerce.
- McLuhan, M. (1964): Understanding Media. The Extensions of Man, London: Routledge & Kegan Paul.
- Mell, P./Grance, T. (2011): The NIST definition of cloud computing. Recommendations of the National Institute of Standards and Technology, Washington, D.C. (NIST Special Publication 800-145).
- Mell, P./Grance,T. (2009): Draft NIST Working Definition of Cloud Computing, Washington, D.C. (http://csrc.nist.gov/groups/SNS/cloud-computing/ .
- 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.
- Milgram, S. (1967): The small world problem., Psychology Today 2(1), 60-67.
- Montalbano, Elizabeth (2012) GSA Moving USA.gov, Data.gov To Public Cloud, in: InformationWeek, January 25, 2012, (http://www.informationweek.com/government/cloud-saas/gsa-moving-usagov-datagov-to-public-clou/232500473).
- Montevideo Statement (2013): *On the Future of Internet Cooperation*. Common statement by AFRINIC, ARIN, APNIC, IAB, ICANN, IETF, ISOC, LACNIC, RIPE NCC, and W3C. Available at http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm
- Mowery, David (1996) (Hrsg.): The international Computer Software Industry, Oxford.
- Nanz, P. (2007): Multiple Voices: An Interdiscursive Concept of the European Public Sphere, in: Fossum, J. E., Schlesinger, P. and Kvaerk, G. (Eds): Public Sphere and Civil Society? Transformations of the European Union. ARENA Report No 2, 11-28 <http://www.arena.uio.no/cidel/Reports/702.pdf.>.
- Nentwich, M. (2003): Cyberscience: Research in the Age of the Internet, Vienna: Austrian Academy of Sciences Press <http://hw.oeaw.ac.at/3188-7>.
- Nentwich, M. and König, R. (2012): Cyberscience 2.0. Research in the Age of Digital Social Networks; in series: Interactiva, Vol. 11, edited by Bieber, C., Leggewie, C. and Lobin, H., Fankfurt/New York: Campus <http://www.campus.de/wissenschaft/kulturwissenschaften/Kommunikation+und+Medien.40449.html/Cyberscience+2.0.98243.html>.
- Nessi (2008): A NESSI Position Paper: European Software Strategy. Brussels.

- Nextmedia CSA (2010): Social Networks Overview: Current Trends and Research Challenges. European Commission Information Society and Media.
- Nielsen, N. (2013): *EU questions decade-old US data agreement*, EUObserver.com. http://euobserver.com/justice/120919, 07/22/2013.
- O´Gara (2012): Rackspace Cloud Revenues Up 69%; http://cloudcomputing.sys-con.com/node/2328228.
- OECD (2007): Participative Web and User-Created Content. Web 2.0, Wikis and social networking: Organisation for economic co-operation and development <http://akgul.bilkent.edu.tr/oecd/9307031E.pdf>.
- OECD (2011): Demand Side Innovation Policy: Theory and Practice in OECD Countries", Paris.
- Osterwalder, A. (2004): The Business Model Ontology - A Proposition In A Design Science.
- Papacharissi, Z. (2010): Privacy as luxury commodity, First Monday, 8 <http://firstmonday.org/ojs/index.php/fm/article/view/3075/2581>.
- 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.
- Plummer, Daryl/Bittman, Thomas J. (2009): Five Refining Attributes of Public and Private Cloud Computing, Stamford.
- Power, R. (2011): Face recognition and social media meet in the shadows, CSO Online, August 01 <http://www.csoonline.com/article/686959/face-recognition-and-social-media-meet-in-the-shadows>.
- Pratchett, L., Durose, C., Lowndes, V., Smith, G., Stoker, G. and Wales, C. (2009): Empowering communities to influence local decision making. Evidence-based lessons for policy makers and practioners.
- PwC (2012): The speed of life. Storing Entertainment Content in the Cloud, los Angeles.
- Qian, L./Luo, Z./Du, Y./Guo, L. (2009): Cloud Computing: An Overview, in: Proceedings of 1st International Conference on Cloud Computing Conference, 626—631.
- Rajala, R. & Westerlund, M. (2007): Business models - a new perspective on firms' assets and capabilities - Observations from the Finnish software industry, in: Entrepreneurship and Innovation, 8(2), 115—125.
- Rajala, R./Rossi, M. Tuunainen, V. K. (2003): A framework for analyzing software business models, in: Proceedings of the European Conference on Information Systems, Naples.
- Rantamäki, J. (2008): Perceived user value of social networking <http://www.cse.hut.fi/en/publications/B/1/papers/Rantamaki_final.pdf>.
- 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.
- Reuters (2013): U.S. overhauling intelligence access to try to prevent another Snowden. Jul 19, 2013. http://www.reuters.com/article/2013/07/18/us-usa-security-snowden-intelligence-idUSBRE96H18F20130718 .
- Richter, A. and Koch, M. (2007): Social Software – Status quo und Zukunft; Technischer Bericht, No. 2007-01, Februar 2007, München: Fakultät für Informatik,

Universität der Bundeswehr München <http://www.unibw.de/wow5_3/forschung/social_software>.
- Ried, Stefan et al. (2011): Sizing The Cloud: Understanding And Quantifying The Future Of Cloud Computing – Extracts, Cambridge, MA (online available at: - http://de.scribd.com/doc/83423660/Extrait-Etude-Forrester-Sizing-the-Cloud).
- Rogers, R. (2009): Zur Frage der Vergoogelung. Hin zu einer unkritisierbaren Maschine?, in: Becker, K. and Stalder, F. (Eds): Deep Search. Politik des Suchens jenseits von Google, Innsbruck: Studienverlag, 193-206.
- Röll, F. J. (2010): Social Network Sites. Digitale Jugendkulturen, in: Hugger, K.-U. (Ed.): VS Verlag für Sozialwissenschaften, 209-224 <http://dx.doi.org/10.1007/978-3-531-91908-9_12>.
- Rossbach, C./Welz, B (2011): Survival of the fittest. Wie Europa in der Cloud eine führende Rolle übernehmen kann, München.
- Rüdiger, A. (2012): Hybrid Cloud kommt durch die Hintertür, in: ZDNet.de, December 14, 2012, (http://www.computerwoche.de/a/hybrid-cloud-kommt-durch-die-hintertuer,2519861).
- Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., Guimarares, M. T. M. and Trevithick, P. (2008): At a crossroads: "Personhood" and digital identity in the information society, No. JT03241547: OECD <http://www.oecd.org/dataoecd/31/6/40204773.doc>.
- Sandgren, Patrik; Mölleryd, Bengt (2013): How liberalised is the optical fibre broadband market? The case of Sweden. Paper presented at ITS Europe, Florence .
- Schief, M./Buxmann, P. (2012): Business Models in the Software Industry. Proceedings of the 45th Hawaii International Conference on System Sciences, 3328–3337.
- Schleife, K. et al. et al. (2012): Wachstumshemmnisse für kleinere und mittlere Unternehmen am Beispiel der IT-Branche, Berlin.
- Schmidt, J. (2009): Das neue Netz. Merkmale, Praktiken und Folgen des Web 2.0, Konstanz: UVK.
- 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 (2013d): Take Back the Internet . Crypto-Gram Sept. 15, 2013 .
- Schneier, Bruce (2013e): Air gaps. https://www.schneier.com/blog/archives/2013/10/air_gaps.html .
- Schneier, Bruce (2013f): Why It's Important to Publish Theo NSA Programs. Crypto-Gram Oct. 15, 2013 .
- Schofield, Jack (2012): Personal cloud to replace PC by 2014, says Gartner, in: ZDNet, March 13, 2012, (http://www.zdnet.com/personal-cloud-to-replace-pc-by-2014-says-gartner-4010025617/).
- 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./Neidecker-Lutz, B. (2010): The Future of Cloud Computing. Opportunities for European Cloud Computing beyond 2010, Brussels.

- Schubert, L./Jeffrey, K. (2012): Advances in Cloud Computing. Report from the Cloud Computing Expert Working Group, Brussels.
- 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.
- Shumow, Dan; Ferguson, Niels (2007): On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng. http://rump2007.cr.yp.to/15-shumow.pdf .
- Skinner, J. (2012): Social Media and Revolution: The Arab Spring and the Occupy Movement as Seen Through Three Information Studies Paradigms. Working Papers on Information Systems <http://sprouts.aisnet.org/11-169>.
- Smith, David M./Plummer, Daryl C./ Cearley, David W. (2009): The What, Why, and When of Cloud Computing, Stamford.
- Snowden, Edward (2013): Eight things we learned. 18 June 2013. http://www.theguardian.com/world/2013/jun/18/edward-snowden-live-q-and-a-eight-things .
- Solove, D. (2006): A taxonomy of privacy, University of Pennsylvania Law Review 154 (3), 477-560.
- SpiceWorks (2012): State of SMB IT 2H 2012, Austin.
- Steinfield, C., Ellison, N. B. and Lampe, C. (2008): Social capital, self-esteem, and use of online socialnetworksites: A longitudinal analysis, Journal of Applied Developmental Psychology 29(6), 434–445.
- Steinmueller (2004): The European Software sectoral system of innovations. In: Malerba, F. (ed.): Sectoral Systems of Innovations, Cambridge, 193-241.
- Strauß, S. (2011): The Limits of Control - (Governmental) Identity Management from a Privacy Perspective, in: Fischer-Hübner, S. (Ed.): Privacy and Identity Management for Life, 206-218.
- Strauß, S. (2013): Digital identities and the upcoming EU privacy reform - a future-proof approach?, LSE Media Policy Project Blog, London School of Economics and Political Science <http://blogs.lse.ac.uk/mediapolicyproject/2013/05/08/digital-identities-and-the-upcoming-eu-privacy-reform-a-future-proof-approach/ >.
- Strauß, S. (2014): forthcoming, Towards a taxonomy of social and economic costs of surveillance., in: Wright, D. and Kreissl, R. (Eds): Surveillance in Europe: Routledge.
- Strauß, S. and Nentwich, M. (2013): Social network sites, privacy and the blurring boundary between public and private spaces, Science and Public Policy (6), doi: 10.1093/scipol/sct072 <http://spp.oxfordjournals.org/content/early/2013/10/10/scipol.sct072.full>.
- 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.
- TNS (2011): Attitudes on Data Protection and Electronic Identity in the European Union (Special Eurobarometer 359), Brussels.
- Trenz, H. J. (2008): In search of the European Public Sphere. Between Normative Overstretch and Empirical Disenchantment. RECON Online Working Paper.
- 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.

- U.S. Senate (2003): Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters. Treaty Doc. 108-27. U.S. Government. Available at: http://www.charitableplanning.com/document/1886119
- UN (2013): *The Right to Privacy in the Digitial Age*; UN General Assembly, Third Committee. A/C.3/68/L.45. Available at http://justsecurity.org/wp-content/uploads/2013/12/Draft-UN-Resolution-Right-to-Privacy.pdf.
- Valkenburg, P. M., Peter, J. and Schouten, A. P. (2006): Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem CyberPsychology & Behavior 9(5), 584-590.
- Van der Berg, B. (2011): The uncanny valley everywhere? On privacy perception and expectation management, in: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G. (Eds): Privacy and identity management for life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School: Springer, 178-191.
- 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.
- Veugelers, R. et al. (2012): Lessons for ICT Innovative Industries. Three Experts' Positions on Financing, IPR and Industrial Ecosystems, Seville.
- Villalón, C. (2013): *Opinion of Advocate General Cruz Villalón delivered on 12 December 2013– Case C-239/12*; Court of Justice of the European Union. Available at http://edri.org/wp-content/uploads/2013/12/C-293-12-AGOP-1.pdf
- Violino, Bob (2011): Cloud computing thunders into the government in: Government Health IT, June 2, 2011, (http://www.govhealthit.com/news/cloud-computing-thunders-government).
- Vogel, W. (2009): Eventually Consistent, in: Communications of the ACM, 52(1), 40-44.
- Wanhoff, T. (2011): Wa(h)re Freunde - Wie sich unsere Beziehungen in sozialen Online-Netzwerken verändern, Heidelberg: Spektrum Akademischer Verlag.
- Weber, Arnd; Haas, Michael; Scuka, Daniel (2011): Mobile Service Innovation: A European Failure. Telecommunications Policy, Volume 35, Issue 5, June 2011, 469-480.
- Weber, Arnd; Weber, Dirk (2012): Verifizierte Virtualisierung für mehr Sicherheit und Komfort. Datenschutz und Datensicherheit 1/2012, 43-47.
- Weber, Matthias et al. (2010): Cloud Computing –Was Entscheider wissen müssen, Berlin.
- WEF (2011): Advancing Cloud Computing: What to do now? Priorities for Industry and Government. World Economic Forum in partnership with Accenture.
- Weigelt, Matthew (2012): What the end of Apps.gov teaches, in: FWC.com, December 5, 2012 (http://fcw.com/articles/2012/12/05/apps-gov-lessons.aspx).
- Weinhardt, C./Anandasivam, A./Blau, B./Borissov, N./Meini, T./Michalk, W./Stosser, J. (2009b): Cloud Computing - A Classification, Business Models, and Research Directions, in: Business Models & Information Systems Engineering, 1(5), 391—399.
- Weinhardt, C./Anandasivam, A./Blau, B./Stößer, J. (2009a): Business Models in the Service World, in: IEEE IT Professional, 11(2), 28—33.
- Wessner, Charles (2008): Assessment of the Small Business Innovation Research Program, Washington, D.C.
- Wimmer, J. (2009): The Publics behind Political Web Campaigning. The Digital Transformation of 'Classic' Counter-Public Spheres, in: Baringhorst, S., Kneip, V. and Niesyto, J. (Eds): Political Campaigning on the Web, Bielefeld: transcript, 31-51.

- Woloszynowicz, M. (2011): The Economics of Dropbox. http://www.w2lessons.com/2011/04/economics-of-dropbox.html, 07/23/2013.
- Wondracek, G., Holz, T., Kirda, E. and Kruegel, C. (2010): A Practical Attack to De-Anonymize Social Network Users; Technical report: iSecLab <http://tinyurl.com/yccfqqd>.
- Wyld, David C. (2010): the cloudy future of Government IT: Cloud Computing and public sector around the world, in: International Journal of Web & Semantic Technology 1(1), 1(1), January 2010.
- Yang, H./Tate, M. (2012): A Descriptive Literature Review and Classification of Cloud Computing Research, in: Communications of the Association for Information Systems, 31(Article 2).
- Yeo, C. S./Venugopal, S./Chu, X./Buyya, R. (2009): Automatic metered pricing for a utility computing service, in: Future Generation Computer Systems, 26 (8), 1368-1380.
- Youseff, L./Butrico, M./Da Silva, D. (2008): Toward a Unified Ontology of Cloud Computing, in: Proceedings of 2008 IEEE Grid Computing Environments Workshop, Los Alamitos, 1—10.
- Zhang, Q./Cheng, L./Boutaba, R. (2010): Cloud computing: state-of-the-art and research challenges, in: Journal of Internet Services and Applications, 1(1), 7—18.
- 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.