EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

CLOUD COMPUTING

STUDY

EN

2012

CLOUD COMPUTING

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

CLOUD COMPUTING

STUDY

Abstract

Cloud computing is a new model of computing that could bring substantial benefits to consumers, businesses and administrations, while also creating new risks and challenges. This study provides an overview on cloud computing and how it relates to EU consumer protection and the EU digital single market goals. It demonstrates that cloud computing could induce savings and facilitate innovative online services. However, it finds that barriers to take-up of cloud computing are manifold. It concludes that in order to seize the benefits of cloud computing, priority actions for EU policymakers are addressing legislation-related gaps, improving terms and conditions for users, tackling stakeholder security concerns, encouraging the public sector cloud, and promoting further research and development in cloud computing.

IP/A/IMCO/ST/2011-18
PE 475.104

May 2012
EN

This document was requested by the European Parliament's Committee on Internal Market and Consumer Protection.

AUTHORS

Civic Consulting
Potsdamer Str. 150
DE-10783 Berlin

Dr Frank Alleweldt and Dr Senda Kara (Directors)
Anna Fielder (Lead author and coordination)
Ian Brown (Contributing author)
Verena Weber (Second reader)
Nicholas McSpedden-Brown (Research)

RESPONSIBLE ADMINISTRATOR

Mariusz Maciejewski
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: mariusz.maciejewski@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its newsletter please write to:
Poldep-Economy-Science@europarl.europa.eu

Manuscript completed in April 2012

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

GLOSSARY OF TERMS

Authentication	Verification of the identity or attributes of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.[a]
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[a]
Cloud pricing models/service models	*Consumption-based pricing model*: A pricing model whereby the service provider charges its customers based on the amount of the service the customer consumes, rather than a time-based fee. For example, a cloud storage provider might charge per gigabyte of information stored. *Subscription-based pricing model*: A pricing model that lets customers pay a fee to use the service for a particular time period, often used for software services.[b]
Cloud provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals, usually for a fee.[b]
Cloud standards	Cloud standards are an agreed-upon approach to ensure interoperability, so a customer can take tools, applications, virtual images, and more, and use them in another cloud environment with minor rework. Portability lets customers take one application or instance running on one vendor's implementation and deploy it on another vendor's implementation.[b] See also *Interoperability* and *Portability.*
Cloud storage	A service that allows customers to save data by transferring it over the Internet or another network to an offsite storage system maintained by a third party.[b]
Community cloud	A cloud set up by a group of organisations that have agreed shared security, privacy and other requirements for a custom cloud they operate together. The size and number of the organisations, amongst other factors, determines the scale of demand, and hence cost savings they can obtain overall.[b]
Data centre	A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.[c]
Elastic computing	The ability to dynamically provision and de-provision processing, memory, and storage resources to meet demands of peak usage without worrying about capacity planning and engineering for peak usage. See also *On-demand service.*[b]
Federation	The practice of managing consistency and access controls when two or more independent geographically distributed clouds share either authentication, files, computing resources, command and control, or access to storage resources.[d]

Hybrid cloud	A cloud that combines a public cloud and private cloud, with sensitive applications and data in a private cloud and more generic systems and processes in a public cloud, and which are often bound together by standardised or proprietary technology that enables data and application portability.[g] See also *Private cloud* and *Public cloud.*
Infrastructure as a Service (IaaS)	A service allowing the consumer to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).[a]
Lock-in	Dependency on a particular cloud vendor and difficulty moving from one cloud vendor to another due to lack of standardised protocols, APIs, data structures (schema), and service models.[b]
On-demand service	A model by which a customer can purchase cloud services as needed; for instance, if customers need to utilise additional servers for the duration of a project, they can do so and then drop back to the previous level after the project is completed.[b]
Personal cloud	A small server in a home or small business network that can be accessed over the Internet. Designed for storing and sharing personal content, personal clouds enable viewing and streaming from any Internet-connected personal computer and quite often from major smartphones. Although personal clouds function in a similar manner to any private cloud set up in a company, their primary feature is easy installation for the average personal computer user.[e]
Platform as a Service (PaaS)	A service allowing the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.[a]
Portability	The ability to move applications and data from one cloud provider to another.[b] See also *Lock-in*.
Private cloud	A cloud that is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.[a]
Privacy by design	An understanding of privacy whereby privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.[h]
Public cloud	A cloud that is made available to the general public or a large industry group and is owned by an organisation selling cloud services.[a]
Resource pooling	The bringing together of a provider's computing resources in order to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.[a]

Security	Refers here to information security, meaning protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide: (A) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) Confidentiality, which means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (C) Availability, which means ensuring timely and reliable access to and use of information.[f]
Service level agreement (SLA)	A contractual agreement by which a service provider defines the level of service, responsibilities, priorities, and guarantees regarding availability, performance, and other aspects of the service.[b]
Software as a Service (SaaS)	A service allowing the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[a]
Virtualisation	The creation of a virtual version of a hardware platform, operating system, a storage device or network resources. The usual goal of virtualisation is to centralise administrative tasks while improving scalability and workloads.[c]

Sources:

a) US National Institute for Standards and Technology (NIST),
b) http://cloudtimes.org/glossary/
c) Wikipedia
d) Cisco
e) http://www.clubcloud.org/blog/-/blogs/your-guide-to-personal-cloud
f) Title III of the US E-Government Act, entitled the Federal Information Security Management Act of 2002
g) Microsoft
h) European Commission, A Digital Agenda for Europe, EUC, 26/8/2010, COM(2010) 245 final/2.

EXECUTIVE SUMMARY

Background

- This study presents the results of research conducted by Civic Consulting between October 2011 and March 2012. Its purpose, as requested by the European Parliament's terms of reference, is to provide an overview on cloud computing, and how it relates to EU consumer protection and the EU digital single market goals.

What is Cloud Computing?

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction, according to a widely accepted definition of the US National Institute for Standards and Technology (NIST).

- The most substantial economic impact of cloud technology could come in the cost savings and increased competitiveness of IT services available to public and private organisations, as well as opportunities leading to new services. Because of demand aggregation, bulk purchasing of power and hardware, and reduced per-unit labour costs cloud providers can make substantial savings on their running costs, and pass these on to their customers. Businesses can use cloud technologies for IT provision, thereby using equipment better, being more flexible, being faster, and having less capital expenditure. For consumers, cloud technologies are making information and online content more accessible and more interactive.

- The main types of clouds are public clouds, private clouds, and hybrid clouds; the main types of services offered by such clouds are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Such cloud services can be provided from data centres located anywhere in the world, which has significant policy implications.

Use and Potential Benefits of Cloud Computing

- The cloud is used differently by different users: consumers typically use it for email, file storage, content and information sharing, payment services and music and video streaming. Businesses use it mainly for basic office tools, collaboration, project management, and the design of custom applications. Administrations use the cloud in largely the same ways as businesses, in addition to innovating in the quality of services, they provide to citizens through e-government solutions.

- Surveys show that most online *consumers* use cloud computing in the form of webmail services, with a little less using online applications for sharing content. The main benefits of the cloud for consumers relate to convenience, flexibility, reduced costs, ease of use, the ability to share content, improved access to information and online content, automatic maintenance and updating, and potentially better security.

- *Businesses* stand to benefit most by avoiding capital expenditure for IT, and being able to scale IT resources; this implies lower barriers to entry, bringing new products to market more quickly, and can help the creation of innovative SMEs. Businesses can also work together more effectively thanks to project management and collaboration cloud services. Furthermore, businesses with innovative ideas can use cloud providers' infrastructure to design custom applications and provide original services and products to consumers, businesses and administrations.

- The same cost-saving benefits for businesses also apply to *governments*, but governments can also benefit from cloud technologies by increasing the quality and innovation within e-government services they provide to citizens and businesses - services that could reduce citizens' and businesses' administrative burdens. There are already examples of public administrations, both locally and nationally, which have either adopted or are planning to adopt cloud-based services, and increasingly governments are developing comprehensive cloud computing strategies.

Risks Related to Cloud Computing

- The biggest perceived barriers for both consumer and SME take-up of cloud computing are lack of privacy, data security, provider lock-in, lack of standardisation, and jurisdictional issues relating to applicable law and law enforcement access to data.

- Potential general data security risks arising from cloud computing relate to: an increase in threats to data confidentiality due to the concentration of data on common cloud infrastructure; the loss of IT control and governance by organisations using cloud services; and an increased risk of data interception in authentication and transmission procedures.

- Transparency is often lacking in providers' provisions concerning data security, in particular a lack of data integrity guarantees combined with disclaimers of liability clauses in contracts; a lack of standards regarding data control and security; and often unclear and incomplete information concerning security and privacy on cloud providers' websites.

- Multiple approaches exist to tackle these vulnerabilities, such as differentiation of the level of security needed by sensitivity of data or use of a 'private cloud' managed by the organisation itself or a provider. Additional data security assurance could also be provided through a form of audit and certification systems of cloud services providers.

- The main challenges surrounding the legal issues regarding privacy relate to: ambiguities as to the role of the cloud service provider; uncertainty regarding applicability of EU laws; the need for more effective data protection; uncertainty regarding laws governing international data transfers, and the lack of universality in data protection legislation.

- Law-abiding consumers or business users storing their data in the cloud may well be affected by compulsory orders for disclosure, without notification, as in a public or shared cloud authorities may seize the servers or computers containing personal information of the guilty and innocent alike; this is compounded by a lack of standards in providers' 'thresholds' of disclosure.

Challenges Related to Achieving a Digital Single Market

- Fragmentation of the digital single market along geographical borders due to differing legal frameworks may restrict or slow down the development of EU-wide cloud-computing based services, for example those dependent on intellectual property rights (music, films, books).

- Rights and responsibilities in the cloud are not yet clear due to lack of transparency or difficulties in finding information, problems with contracts, the complexities of many jurisdictions or the fact that for each legal issue - data protection, contracts, consumer protection or criminal law - the jurisdiction may differ. There also gaps in the relevant legislation when applied to cloud computing.

- Cloud providers' contracts often disclaim liability, contain inappropriate or illegal clauses and lack certain key pieces of information such as the location of data centres. In particular, service contracts offered to SMEs are rigid, with little room for negotiation. A majority of interviewed stakeholders agree there is a need for standardised contracts, with specific requirements regarding safety, security and reliability.

- Standardisation efforts for cloud services are proliferating. However, even if consumers would greatly benefit from interoperable cloud services, support for interoperable standards from industry is mixed, with some industry players fearing that early standardisation could stifle innovation.

Cloud Computing in the Future

- In the short term, it is uncertain whether there will be significant changes in the types of cloud services offered. However, their availability and capacity are likely to continue to increase, as economies of scale drive ever-larger data centres, which will continue to migrate towards sites with cheaper energy.

- While some services are likely to move to the public cloud given the potential cost savings, other services will still remain in a private environment, because there remain many instances where the intelligent use of small scale solutions is as efficient, or even more efficient than large scale ones.

- Issues such as security and privacy could slow down development because if business users or public authorities do not have the confidence or the evidence that public clouds can be trusted, they are unlikely to take up the cloud model. But lack of competition, mainly due to insufficient interoperability, could be one of the biggest hurdles to overcome in cloud computing development.

- An important future challenge will be in identifying the areas where cloud computing development could be coordinated on the European level to avoid duplication and waste. This would mean tackling essential standards issues to achieve interoperability, ensuring effective competition between providers, by addressing for example vertical integration of service providers or enabling better public procurement for cloud services to encourage new market entrants, and coordinate both European and national cloud computing initiatives.

- Connectivity will gain in importance, since the increased usage of cloud services will result in customer dependency on the availability of high-speed broadband, (including wireless 4G mobile networks or other available technologies); upload speeds in particular may become an important factor. Cloud services accessed through mobile devices would be facilitated by EU-wide access to Internet without complicated or costly roaming arrangements.

- Due to jurisdictional problems, in practice European consumers are unlikely to be able to seek redress from cloud services providers in other jurisdictions. Providing adequate means for redress is necessary for the future in the consumer services area, since there is a strong asymmetry of powers between consumers and providers of cloud services.

INTRODUCTION

Some have likened the onset of cloud computing to the industrial revolution, in terms of providing means for the mass production of certain goods and services, or even the 'fifth utility' (after water, gas, electricity and telephony). Others have remained sceptical, and see it as little more than a marketing tool promoting new models of organisation without a significant change in technology.

The EU has an ambitious Digital Agenda leading up to 2020, which sets out over 100 concrete activities to achieve a strong and competitive European digital single market, and as such is considered an important part of the EU's overall growth strategy. Within this Agenda, the technology model called 'cloud computing' has been gaining in importance due to its expected macroeconomic benefits, such as helping start-up small businesses enter the market, which could foster innovative new online applications and save administrations taxpayers' money on ICT (Information and Communication Technologies) provision. A Commission Communication containing a Cloud Computing Strategy is postponed from its original data and now due in summer 2012.

This study presents the results of research conducted by Civic Consulting between October 2011 and March 2012. Its purpose, as requested by the European Parliament's terms of reference, is to provide a broad overview on cloud computing, and how it relates to EU consumer protection and the EU digital single market goals. Specifically it sets out to answer these questions:

- What is cloud computing and what are its benefits for consumers, businesses and administrations now and in the future?
- What are the risks related to cloud computing for these stakeholders, as well as the main internal market and consumer policy challenges now and in the future?
- What are the future cloud computing trends and foreseen future benefits and risks?
- What actions may be necessary to address highlighted risks and challenges?

To address these questions adequately in the short time available, we reviewed the relevant literature, targeting in particular research and policy works covering European aspects, as well as other media since this is a fast evolving subject; and we carried out 18 structured face-to-face or by phone interviews with relevant European officials, consumer representatives, national public administrations, and cloud providers and industry representatives (for a list of organisations, see Annex 2). The insights provided by these interviews have been crucial for the understanding of this complex technology model, what it can offer, and what it cannot.

One of the challenges in covering any aspect of cloud computing is that there is still debate about exactly what it is and its definition, and indeed whether it is a new paradigm or just an old technology promoted in a new form. Some definitions can be so broad as to cover the whole of the online Internet world and therefore all its related issues and policy challenges. Therefore, we have adopted one of the most widely accepted definitions of cloud computing provided by the US National Institute of Standardisation and Technology (NIST) and have endeavoured to focus on the benefits and risks that are the most relevant to this technology model, according to this definition. Even so, the subject is complex and broad, and has synergies with many areas of the EU digital single market, from intellectual property issues to broadband penetration and the so-called Internet of Things, the suggested evolution of the internet into a network of interconnected objects operating independently.

The report is structured as follows: Section 2 provides an overview of cloud computing with its projected impact, the main types of cloud and its main uses; Section 3 provides a more detailed breakdown of how consumers, businesses and administrations are using cloud computing and the benefits they stand to draw from it; Section 4 analyses the potential risks related to cloud computing for all stakeholder groups; Section 5 examines the challenges that remain to achieving a single market in cloud computing; Section 6 provides an overview of the future of cloud computing; and Section 7 concludes with key policy recommendations to be considered by EU policymakers for the development of cloud computing in Europe.

1 AN OVERVIEW OF CLOUD COMPUTING

KEY FINDINGS

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction, according to a widely accepted definition of the US National Institute for Standards and Technology (NIST).
- The most substantial economic impact of cloud technology could come in the cost savings and increased competitiveness of IT services available to public and private organisations, as well as opportunities leading to new services. Because of demand aggregation, bulk purchasing of power and hardware, and reduced per-unit labour costs cloud providers can make substantial savings on their running costs, and pass these on to their customers. Businesses can use cloud technologies for IT provision, thereby using equipment better, being more flexible, being faster, and having less capital expenditure. For consumers, cloud technologies are making information and online content more accessible and more interactive.
- The main types of cloud are public clouds, private clouds, and hybrid clouds; the main types of services offered by such clouds are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Such cloud services can be provided from data centres located anywhere in the world, which has significant policy implications.
- The cloud is used differently by different users: consumers typically use it for email, file storage, content and information sharing, payment services and music and video streaming. Businesses use it mainly for basic office tools, collaboration, project management, and the design of custom applications. Administrations use the cloud in largely the same ways as businesses, in addition to innovating in the quality of services they provide to citizens through e-government solutions.

The following sections provide an overview of cloud computing. We first ask: 'What is cloud computing?, before outlining the main current uses of cloud technology by consumers, businesses and public authorities.

1.1 What is cloud computing?

1.1.1 The definition of cloud computing

'Cloud computing' is a rather vague term with a multitude of meanings, from the more specific to ones so broad as to encompass virtually the whole of the Internet. One of the clearer and more widely accepted definitions comes from the US National Institute for Standards and Technology:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".*[1]

One of the consumer organisations interviewed suggested a consumer-centred definition:

> *"Cloud computing is … when you use services, or storage, not at your own computer but somewhere else in the Internet, which is not in one data centre but is spread all over the Internet. As a user you don't know where your data is or where the services are which you are using. So …, cloud computing is Facebook, it is webmail, it is online storage and it is when you use software which is not running on your computer but in the Internet."*

Some have likened the onset of cloud computing to the Industrial Revolution, in terms of providing means for the mass production of certain goods and services, or even the 'fifth utility' (after water, gas, electricity and telephony).[2] They see that cloud computing will herald a revolutionary paradigm shift in terms of "increased productivity, job creation, business development and competitive advantage" that it brings about, and could even be "one of the most important ways that European economies can revive and emerge from the economic crisis."[3]

At the same time, some people are sceptical about the cloud 'hype', if not the technology itself, and see it as little more than a marketing tool promoting new modes of organisation without a significant change in technology. Widely quoted is Oracle's CEO Larry Ellison, who voiced his frustration with the term:

> *"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. . . . I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads….."*[4]

---

1 NIST, Mell, P. & Grance, T., *The NIST Definition of Cloud Computing*, 2011., p.2 at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2 See e.g. Price, M., *Pinning Down the Cloud*, Wall Street Journal, 14 Feb 2011 at http://online.wsj.com/article/SB10001424052748704739504576067461795827534.html; and Wyld, D. C., *Cloud Computing: Is it the Fifth Utility?*, 2009 at http://computersight.com/computers/cloud-computing-is-it-the-fifth-utility/.

3 See CEBR, *The Cloud Dividend: Part One - The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and the UK*, 2010, available at http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf.

4 Ellison, L., *Speech at Oracle OpenWorld 2008*, September 25, 2008.

This scepticism was reflected by one of our interviewees, a European official who predicted that "the bubble will burst soon" and continued: "we're back to the future. We're back to the mainframe [computer] with VT100 terminal on the other side. In the second half of the 1990s they wanted to launch … Network Computing, and it has been a total failure. … It's some kind of marketing tool used at the moment, and I think abused, that's why I think it's going to burst."

In spite of these disagreements, there is a general consensus that this remote computing 'cloud' of resources represents a new way of delivering computing services, not a new technology[5] - although there are continuing technical developments that improve the efficiency and security of these systems. Substantial cloud research and development by European businesses and universities is being funded under the EU's Seventh Framework Programme.[6]

International Data Corporation (IDC) estimates the global market for cloud services at 44.2 billion US Dollar (34 billion Euro) in 2013, with the European market worth just over 6 billion Euro.[7] Many providers are headquartered in the US, and include the computing giants Google, Microsoft and Amazon. Europe-based cloud providers include Cloud4Com in the Czech Republic, City Cloud in Sweden, and Germany's MESH and Zimory. An industry representative told a recent conference that North America-based providers are currently strongest, with 56% of market, against 25% in Western Europe. This gap is predicted to narrow to 50% against 29% by 2014.[8]

Cloud architecture has the potential to reduce the number of data centres for large organisations. Figure 1 below shows how successfully IBM was able to consolidate its data centres into cloud architecture, compared to the US Federal Government.

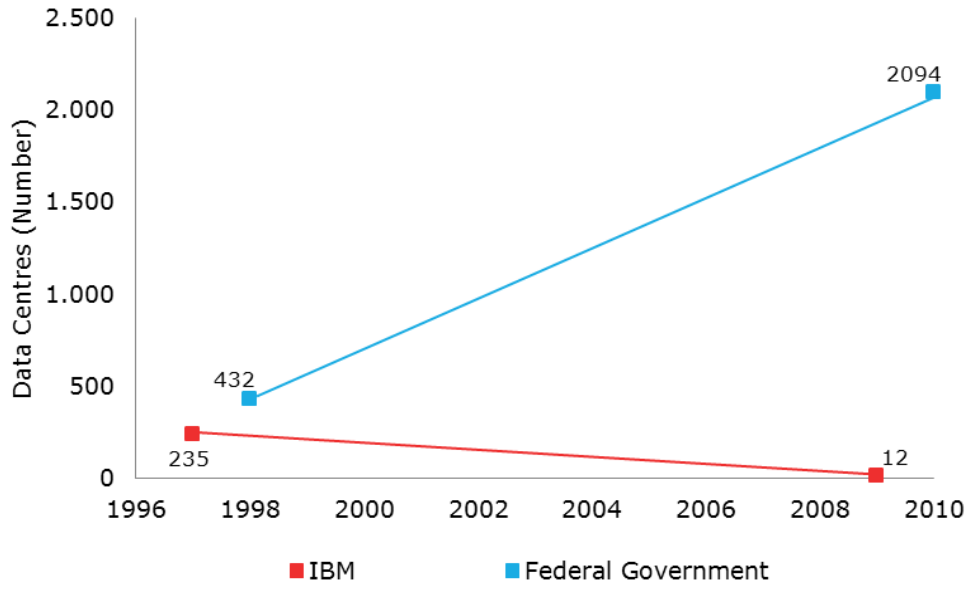
[5] ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009, p.4.

[6] See for example the Software & Service Architectures and Infrastructures theme under ICT research at http://cordis.europa.eu/fp7/ict/ssai/.

[7] IDC, Gens, F., Mahowald, R. P. & Villars, R. L., *IDC Cloud Computing 2010 - An IDC Update*, 2009, Doc # TB20090929; IDC, Bradshaw, D., *Western European Software-as-a-Service Forecast, 2009-2013*, 2009, Doc # LT02R9, 2009. Note that this figure refers only to 'Software-as-a-Service' cloud services in Europe.

[8] Moisés Navarro Marín, Director of Cloud Strategy and Services at Telefónica, in Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011, p.5.

Figure 1: IBM data centre rationalisation and US Federal Government expansion



Source: Renda, S., *US "Cloud First" Policy Insights, EC-ETSI Standards in the Cloud Workshop*, 2011.

In addition, a substantial economic impact of cloud technology could come in the cost savings and increased competitiveness of IT services available to other public and private organisations. This is because *cloud providers* can make substantial savings on their running costs, and pass these on to their customers. They can cut their energy costs by siting data centres in areas of cheap electricity with high bulk purchase discounts; they can increasingly automate system administration with the same number of technical staff covering much higher numbers of servers; and they can standardise system procurement to a limited number of hardware and software platforms, and so obtain bulk discounts.[9] *Businesses* can use cloud technologies for IT provision, thereby "using equipment better, being more flexible, being faster, having less capital expenditure, [and instead having] more running expenditure, [which is] bearable expenditure", as one interviewed European official put it. A representative of a consumer organisation emphasised that there are also a lot of potential benefits for *consumers*, because "the cloud is making information more accessible and more interactive [with] cost savings for tax payers and consumer".

The potential benefits of cloud computing, and related risks and challenges, are discussed in more detail in Section 4 below.

[9] Microsoft, Harms, R. & Yamartino, M., *The Economics of the Cloud*, Microsoft whitepaper, 2010, p.3.

1.1.2 How cloud computing works

The cloud has emerged out of global computing infrastructure built by major companies such as Google, Amazon, Microsoft and eBay and initially used to run their own businesses. Having built massive data centres in multiple countries with very high-speed connections into the global Internet, they spotted the revenue potential in offering surplus data storage and computing services to other companies. Some of these data centres can hold upwards of one hundred thousand servers.

Each of these computing servers runs operating system software that can present multiple 'virtualised' environments to customers, who can run their own software applications without them interfering with other concurrently-running programs on the same server. Companies such as IBM, HP and Citrix sell systems that efficiently manage this virtualisation process and provide additional reliability and security features. For example, HP's 'CloudSystem Matrix' systems allow programs to be automatically transferred from a failing machine to one that can take on the extra load.[10] Data centres can also store customer data on request. Customers can request the computing and storage resources they need at any given moment on a pay-per-use basis.

1.1.3 Main types of clouds

The best-known cloud services are so-called 'public clouds', based on global networks of data centres offering pay-per-use services to the general public or a large industry group. This is where the greatest cost savings are to be found, thanks to demand aggregation, bulk purchasing of power and hardware, and reduced per-unit labour costs. Certain services may even be provided for free by public cloud providers, to attract custo

Companies and administrations can build their own 'private clouds', based on their existing computing hardware. This is often the first step in a company's move from existing IT systems towards public cloud services. While a private cloud does not generally provide as great cost savings as a public cloud, it might be suitable for organisations with sensitive data they do not want to send outside their own systems.

The significance of cost differences between different types of clouds is illustrated by Microsoft's cloud costing model, which suggests that private clouds are extremely expensive with a small installed base of fewer than 100 servers, since they have none of the supply or demand-side scale advantages of public clouds. At around 1,000 servers a private cloud brings greater benefits, although reportedly still at a 10-fold premium over public cloud services.[11] It also requires companies to invest up-front in the necessary computing hardware and software.

In between public and private models are 'hybrid clouds', where some computation and storage is done in the public cloud and some on private systems. This allows more sensitive data to be processed in-house while less sensitive data goes to cheaper public cloud servers.

[10] HP, *Transform data center economics and meet dynamic business needs: The business case for the HP CloudSystem Matrix*, 2011, p.9.

[11] Microsoft, Harms, R. & Yamartino, M., *The Economics of the Cloud*, Microsoft whitepaper, 2010, p.16.

A further model is that of 'community clouds'[12], set up by groups of organisations that have agreed on shared security, privacy and other requirements for a custom cloud they operate together. The size and number of the organisations, amongst other factors, determines the scale of demand, and hence cost savings they can obtain.

1.1.4 Classification of cloud services

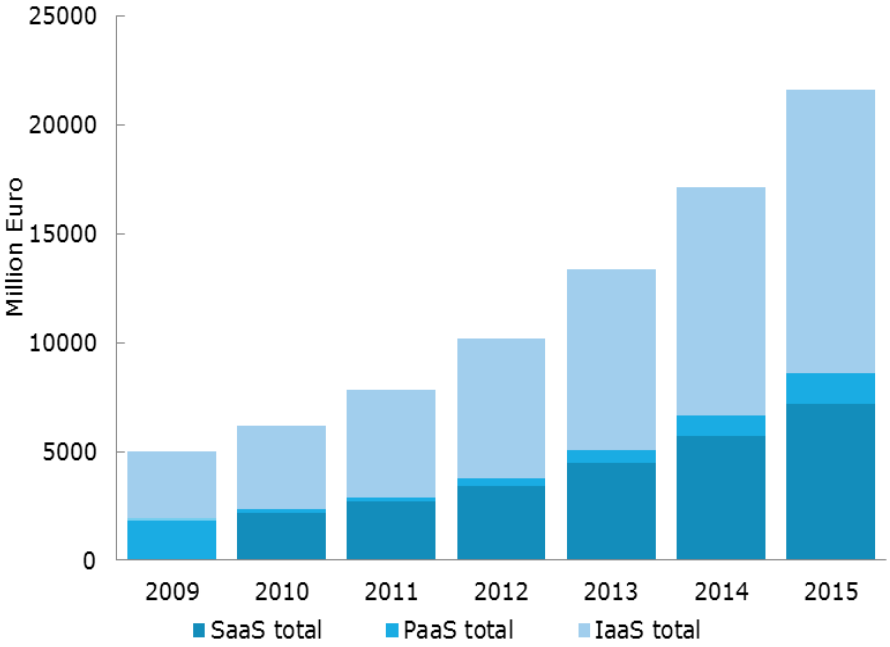
Cloud systems are typically classified according to the services they provide. The main types[13] are:

- *Storage as a Service* - this allows customers to store and share data remotely. Examples include Dropbox, Box.net, Amazon Scalable Storage Service (S3), Iron Mountain, EMC Atmos Online, Google Cloud Storage, and Microsoft's SQL Azure.
- *Software as a Service (SaaS)* - this provides a complete remote software environment to customers, for example for email, word processing, customer relationship management, and many other types of applications. Examples include Google Docs, Calendar and Gmail, Zimbra, Spotify, Salesforce.com, Microsoft Office 365, and SAP Business by Design.
- *Platform as a Service (PaaS)* - this enables software developers to build custom applications on clouds, taking advantage of the cloud ability to automatically provide additional computing and storage resources when required. Examples of PaaS include IBM Websphere, Force.com, Springsource, Morphlabs, Google App Engine, Microsoft Windows Azure, and Amazon Elastic Beanstalk.
- *Infrastructure as a Service (IaaS)* - gives software developers direct control over the computing and storage resources being provided by a cloud. This provides greater flexibility, at the cost of greater complexity to take advantage of all of the cloud's services. Examples include Amazon's Elastic Compute Cloud, Zimory, Elastichosts, and VMWare's vCloud Express.

[12] For more details on types of clouds see European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010, pp. 9-11.

[13] For more details the classification of cloud services see Ibid, pp. 9-11.

Figure 2: Estimated value of different categories of cloud services across the EU (Storage as a Service is included in the IaaS total)



Source: Pierre Audoin Consultants, *PAC's Cloud Computing Worldwide by countries datamart 2012*, 2011, reproduced with permission (Data from 2012 to 2015 are predictions).

Underpinning all cloud services are the infrastructure providers (IaaS providers). Public cloud providers, such as Amazon, Google and Microsoft, are often large enterprises – they need deep pockets to build the necessary data centres and global connectivity. These providers also need specialised hardware and software expertise, and security expertise and resources to defend against constant physical and electronic attacks.[14] Private infrastructure (including that "inside" hybrid and community clouds) can be managed by smaller companies and associations, depending on its scale.

Platform (or PaaS) providers add "middleware" software to infrastructure to make it easier for software developers to program. In particular, they make it easier for software to scale from a low to high level of resource usage on-demand, and to manage client billing. The infrastructure providers themselves typically have platform offerings. Other notable organisations with a specific platform specialisation include IBM, Force.com, and Facebook. The complexity of developing and maintaining these platforms will tend to favour larger companies over SMEs as platform providers.

[14] Armbrust, M., et al., *Above the Clouds: A Berkeley View of Cloud Computing*, 2009, p.5.

Software developers (SaaS providers) can take advantage of cloud infrastructure and platforms to create the services that are generally accessed directly by customers. The cloud platforms should make it easy for small companies to enter this market. For example, SlideShare, which allows millions of users to share and comment on PowerPoint presentations, was started up using cloud services by a husband-and-wife team.[15] Infrastructure and platform providers themselves also often offer services developed on their own clouds. Examples include Microsoft's Office 365, Google Docs, and Amazon's e-commerce store. An interesting example of the potential for integrating services between different providers comes from Box.com, which allows customers to edit files in its storage cloud using Google Docs. The company's Box Innovation Network encourages other software suppliers to provide additional services on its storage platform, and is investing up to 2 million USD (1.6 million EUR) in software companies to support this development.[16]

Users generally access cloud services using their web browser, or applications downloaded onto their PC, tablet or smartphone.

1.1.5 Geographical location of data centres

The biggest cloud policy implications come from the fact that cloud servers can be located geographically anywhere in the world, inside or outside the EU. Global cloud providers wish to be able to seamlessly move and replicate data between their servers, in order to take advantage of lightly-loaded servers in different time zones, the availability of cheap power (especially fluctuating renewable resources), and to improve performance and resilience.

However, some of their customers may wish to ensure their data remains within the EU, especially for data protection and security reasons. Major cloud providers have European infrastructure (e.g. Microsoft in Dublin and Amsterdam; Amazon in Dublin; Rackspace in London and Slough, UK[17]) and allow customers to buy EU-specific cloud resources. An even more geographically-bounded example is the French *Andromède* initiative, which will be funded by a public-private partnership between the French state and several communication companies. All of the *Andromède* servers will be located in Europe; Microsoft and Atos will offer Office 365 services hosted entirely in France.[18]

[15] India Knowledge@Wharton, *SlideShare's Rashmi Sinha: 'We Wanted to Reach Millions'*, 24 August 2010, at http://knowledge.wharton.upenn.edu/india/article.cfm?articleid=4515.

[16] Yeh, C., *Box Innovation Network: Innovation in Enterprise Software is Possible*, 2011, at http://blog.box.com/2011/11/box-innovation-network-innovation-in-enterprise-software-is-possible/.

[17] Information gathered during our interviews.

[18] See Telecompaper, *France to form Andromede cloud computing Joint Venture in November*, 2011, at http://www.telecompaper.com/news/france-to-form-andromede-cloud-computing-jv-in-november/ ; Telecompaper, *Dassault Systemes pulls out of cloud project*, 2011, at http://www.telecompaper.com/news/dassault-systemes-pulls-out-of-andromede-cloud-project/.

1.2 How is the 'cloud' used?

The following sections give some examples of current uses of cloud computing according to its definition and specific characteristics outlined above. It is important to note that the cloud computing paradigm is closely related to others in the area loosely called 'Future Internet'[19], and in particular to that of services provided over the internet. Therefore, there can be confusion between the two, for example when it comes to e-government service provisioning. As explained in the expert group report on the future of cloud computing carried out for the European Commission:

> *"Clouds can be regarded as an enabler for enhanced features of large scale service provisioning. Much research was vested into providing base capabilities for services provisioning - accordingly, capabilities that overlap with cloud system features can be easily exploited for cloud infrastructures*".[20]

Cloud services used by consumers

A wide range of consumer services are offered using cloud technology. Payment providers such as PayPal are offering transaction services that allow customers to make payments through mobile applications on their smartphones.[21] Flickr, Picasa, YouTube and Facebook allow users to share photos and videos with friends. Yahoo!, Microsoft and Google support hundreds of millions of email users. Dropbox and Box.com allow users to store and share files. Apple's iCloud includes all these features, along with a music locker service that allows users to access their music collection from any of their devices.

As recorded by surveys, webmail is still by far the most widely used 'cloud' application;[22] other popular applications such as the massive video sharing and storage site YouTube or photo-sharing Picasa and Flickr have been around for some time, long before the 'cloud' terminology became fashionable. More recent innovations in the world of entertainment applications include the music streaming and sharing site Spotify and video-renting site Netflix. These services opened to consumers instant access to large libraries with musical and cinematographic resources.

There is disagreement on whether social networking sites, notably Facebook, are cloud applications, including among those we interviewed - some say yes, some say definitely not.[23] From a consumer policy perspective whether it is or it isn't defined as such matters little. One of the interviewed European officials explained that he considers Facebook a cloud, but this was relevant "only for the guys running the Facebook

---

[19] 'Future Internet' is a general term for research activities on new architectures for the Internet. It refers to the general movement of many activities and services online – such as business, content creation and sharing, education, shopping, networking and communication - and the changes required in the Internet to facilitate this movement.

[20] European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010, p. 16. Also see here for further information on related concepts such as the "Internet of services" and "Internet of Things".

[21] Perez, J. C., *PayPal to open app store for developers*, IDG News Service, 2010, at http://www.pcworld.com/businesscenter/article/190193/paypal_to_open_app_store_for_developers.html

[22] Ipsos OTX MediaCT, *Head in the clouds? Cloud computing and consumers*, Free year-round insights, Technology Edition #2, June issue, 2011, at http://www.ipsos.com/mediact/sites/ipsos.com.mediact/files/pdf/Head%20in%20the%20clouds.pdf. Data applies only to the United States.

[23] See also e.g. "Is Facebook a cloud?" at http://www.focus.com/questions/facebook-cloud/, where technology experts do not agree either.

infrastructure. For the end user, it's completely irrelevant if it is. It's only relevant in the sense that services may be more accessible. But users will never see it as such."

More classic cloud-based services, which can be used both by individuals and organisations, include storage services, office software, project collaboration tools and file back-up (Carbonite or Basecamp), services for mobile device-independent access to content (iCloud), as well as a multiplicity of innovations, e.g. apps for traffic and navigation. Not all succeed: for example Google Health, a personal health data storage locker and sharing site, has recently closed down due to lack of mass take up.[24]

More details regarding selected cloud based services targeted at consumers are presented in the following table:

Table 1: Examples of popular consumer-focused cloud services

	Website address	Description of service on website	Examples of usage
Amazon Cloud Drive	https://www.amazon.com/clouddrive/learnmore	"Amazon Cloud Drive is your personal hard drive in the cloud. Store your music, videos, photos, and documents on Amazon's secure servers. All you need is a web browser to upload, download, and access your files from any computer." "You'll never lose your files from a hard drive crash or a lost or stolen laptop."	Storage purposes
Apple iCloud	www.icloud.com	"iCloud stores your music, photos, documents, and more and wirelessly pushes them to all your devices. Automatic, effortless, and seamless — it just works." "iCloud automatically and securely stores your content so it's always available to your iPhone, iPad, iPod touch, Mac or PC. It gives you access to your music, apps, latest photos and more from whichever device you happen to be using. And it keeps your email, contacts and calendars up to date across all your devices. No syncing required. No management required. In fact, no anything required. iCloud does it all for you."	'Device' cloud, i.e. with a device-centric view of cloud storage.
Dropbox	https://www.dropbox.com/	"Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website. Dropbox also makes it super easy to share with others, whether you're a student or professional, parent or grandparent. Even if you accidentally spill a latte on your laptop, have no fear! You can relax knowing that Dropbox always has you covered, and none of your stuff will ever be lost."	Storage purposes

[24] See http://www.google.com/intl/en-GB/health/about.

	Website address	Description of service on website	Examples of usage
Evernote	http://www.evernote.com/	"Evernote makes it easy to remember things big and small from your everyday life using your computer, phone, tablet and the web… With Evernote, all of your notes, web clips, files and images are made available on every device and computer you use… Share your notes and collaborate on projects with friends, colleagues and classmates."	Note-taking and note-sharing purposes
Google Apps	http://www.google.com/apps/intl/en/business/index.html	Google Apps allows users to "Get custom email like hikingfan@your-group.com.[Gmail]; Create websites and group wikis. [Google Sites]; Organize your schedule and share events with friends; [Google Calendar] Share online documents, presentations, and spreadsheets [Google Docs]."	'App' cloud, for storage, collaboration and sharing purposes
Microsoft Skydrive/ Windows Live Mesh	http://explore.live.com/skydrive http://explore.live.com/windows-live-mesh	"Store, organize, and download your files, photos, and favourites on Windows Live servers, and access them from any computer with an Internet connection. Share photos and files that you create with your friends, collaborate on documents, or display photos and files that you create for anyone on the Windows Live network."	Storage and sharing purposes
SpiderOak	https://spideroak.com/	"SpiderOak provides an easy, secure and consolidated free online backup, sync, sharing, access & storage solution." "SpiderOak offers a different approach to online backup by combining a suite of services into one consolidated tool - free online backup, synchronization, sharing, remote access, and storage. This difference is further measured in our zero-knowledge privacy policy… Our flexible design allows you to handle data from any operating system (Mac, Windows and Linux) or location (external drives, network volumes, USB keys, etc...) using just one centralized account."	Storage and sharing purposes
Spotify	www.spotify.com	"Spotify is a new way to listen to music. Millions of tracks, any time you like. Just search for it in Spotify, then play it… Spotify comes in all shapes and sizes, available for your PC, Mac, home audio system and mobile phone… You can also share music with a flick of the wrist. Send it straight to your friends, or post tracks on social networks."	Streaming and sharing music
Waze	www.waze.com	"Waze is a free, community-based traffic & navigation app. When you download Waze, you not only get free navigation, but also become part of the local driving community, joining forces with other drivers nearby to outsmart traffic, save time and improve everyone's daily commute."	Crowdsourcing tool for traffic navigation

Source: Civic Consulting Internet research carried out in January 2012

Cloud services used by businesses

The broadest class of cloud products offered to business may be the productivity suites that mirror the PC software (such as OpenOffice and Microsoft Office) in use by 'information workers' in businesses around the world. These suites typically contain word processing, spreadsheet, email, diary and presentation tools. Microsoft has recently launched a cloud version of its suite (Office 365), while Google offers both consumer and enterprise versions of its Docs, Gmail and Calendar services.

Many more specialised cloud products are offered to businesses. One of the best-known is Salesforce.com, which offers customer relationship management tools that allow companies to manage their sales teams and all contacts with customers. Basecamp and Huddle allow project teams inside and across companies to plan activities collaboratively, and share and comment on project resources, along with external partners. Slideshare lets companies (and individuals) share, discover and comment on presentations. SAP provides cloud-based supply chain monitoring services based on radio-frequency identification (RFID) technology.

Larger companies can use cloud platforms and infrastructure services to write custom applications and outsource their own computing and storage requirements.

An overview of selected cloud based services targeted at businesses is provided in the table on the following page.

Table 2: Examples of popular business-focused cloud services

	Website address	Description of service on website	Examples of usage
Amazon EC2/S3	http://aws.amazon.com/ec2/ http://aws.amazon.com/s3/	"Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers… Amazon EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire." "Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for developers. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web."	Computing and storage purposes

	Website address	Description of service on website	Examples of usage
Basecamp (37signals)	http://basecamphq.com/	"Basecamp is the world's most popular web app for storing, coordinating, and managing your company's projects, tasks, discussions, and decisions. When you keep everything together in Basecamp, everyone stays up to date, everyone knows where everything is, and nothing ever gets lost." "Project Management is all about communication. Projects go well when people talk to each other, discuss issues openly, and communicate clearly. Basecamp is focused on making this easy."	Project collaboration
Box	www.box.com	"Box offers secure, scalable content-sharing that both users and IT love and adopt… Box lets you store all of your content online, so you can access, manage and share it from anywhere." "Box provides everything you need to collaborate on content online… Make sure everyone's on the same page with version history… Exchange feedback in one place, whether it's a quick comment or an in-depth discussion… Keep projects on track by assigning and managing tasks around any file… Get a detailed, real-time view of everything going on with your content."	Content/project management
Huddle (Ninian Solutions Limited)	www.huddle.com	"Collaboration in the cloud... File sharing: share files across the firewall with your colleagues and partners; Project management: collaborate and assign tasks to get work done efficiently and effectively; People: users profiles allow you to connect with the specific people you need to contribute to your project."	Project collaboration
Microsoft Office 365	www.office365.com	"It's familiar Microsoft Office collaboration and productivity tools delivered through the cloud. Everyone can work together easily with anywhere access to email, web conferencing, documents, and calendars." "All of your employees—whether they're power users or casual workers—can easily and securely access the same Office tools and information. They can be productive on PCs, phones, and browsers from virtually anywhere… Tightly integrating cloud-based and on-premises workloads enables you to maximize your current technology investments, deploy at your own pace, and get the benefits of the cloud in a way that works for your business."	Collaboration on Microsoft Office documents

	Website address	Description of service on website	Examples of usage
Salesforce.com	www.salesforce.com	"Salesforce.com is the enterprise cloud computing company that is leading the shift to the Social EnterpriseTM—helping companies connect to customers and employees like never before... Customer Relationship Management (CRM) software solutions allow you to manage the relationships you have with your customers, using a combination of people, processes and technology."	Project management, customer relationship management

Source: Civic Consulting Internet research carried out in January 2012.

Cloud services used by public authorities

Government cloud adoption strategies include the use of cloud-based productivity and project management tools that are also popular with businesses. As well as gaining significant cost savings, governments are planning to use cloud technology to increase the quality and innovation in the services they provide to citizens. This is an aim that is already stated in many on-going e-government initiatives although few of these are currently cloud-based in the EU. Use is gradually increasing, in areas such as transport services, health services, education and contracting,[25] however the majority of EU public sector organisations are still in the planning and investigation stages when it comes to cloud computing.[26]

Table 3 provides selected examples of public sector current use of cloud computing in the EU, illustrating how it can be used to provide services to consumers and businesses, or collaborations with other public organisations. Table 4 gives some examples from South Korea and the US; these countries are at present in relatively more advanced stages of systematic use of cloud computing in the public sector. The US government's Federal Information Technology programme includes a "Cloud First" strategy,[27] and a portal dedicated to cloud computing applications for the public sector has been established in order to fast-track adoption.[28] This portal helps public authorities with procurement of cloud services (SaaS and IaaS) from recommended services providers. In South Korea, cloud computing forms part of the strategic development of the so called 'ubiquitous environment' or ubiquitous computing (u-city, u-home, u-learning), which seems to be another term for the Internet of Things.[29]

Public administration use, and barriers to use, of cloud computing is explored further in the next chapters (Sections 3.3 and 4)

[25] Wyld, D. C., *The Cloudy Future of Government IT: Cloud Computing and the Public Sector around the world*, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, 2010.

[26] Redshift Research, *Adoption, Approaches & Attitudes: The Future of Cloud Computing in the Public and Private Sectors, 2011*, p. 12. The survey covers cloud adoption on a global level, and shows that globally overall a majority majority of public authorities are still in the investigation stages when it comes to cloud computing. See also http://www.informationweek.com/news/government/cloud-saas/229900072.

[27] See http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf.

[28] See www.apps.gov.

[29] See http://eng.kcc.go.kr/user/ehpMain.do; the strategy brochure, *Where We Stand*, can be downloaded from this site of the Korean Communication Commission.

Table 3: Examples of public administrations use of cloud computing

	Description	Website address
FINLAND Cloud Software Program	The four-year Cloud Software Program (2009-2013) is funded by the Finnish communications technology research company TIVIT and Tekes and the Finnish Funding Agency for Technology and Innovation. It seeks to support business developing cloud solutions. More recently, the government-sponsored 'Energy Efficient Data Centre' project sought measures to improve the energy efficiency of cloud centres in Finland. The national ICT service centre *Kuntien Tiera Oy*, serving municipalities, created a framework agreement for use of cloud services by 225 local authorities serving 46% of the Finnish population, in order to save on the cost of software installations and management.	http://www.cloudsoftwareprogram.org/
SLOVENIA KC Class	The Slovenian Ministry for Higher Education has partnered with the European Commission and industry to develop the KC Class program. KC Class brings together institutions that deal with cloud computing in the country and has broad industry support. It currently employs researchers and developers from six small businesses, four middle-sized enterprises, and seven research organisations, who work to develop local solutions, services and products in the field of cloud computing.	http://www.kc-class.eu/
SPAIN Barcelona	The city of Barcelona in Spain serves more than 1.6 million inhabitants and draws about 6.5 million visitors each year. Many citizens work remotely outside of the office and Barcelona draws thousands of business people who come to conferences each year. Consequently the city officials, in partnership with the Microsoft Innovation Centre for Productivity decided to create and launch a portal, called 'Third Place', aimed at helping people to find suitable places with wireless connectivity and other resources (e.g. printers) where they can work while on the move around the city.	http://www.findthirdplace.com
SPAIN Madrid	Tecnigral is a Madrid-based company specialised in environmental services solutions for inner cities. Its ArboMap product for urban management has achieved great success with local authorities across Spain, especially Madrid City Council. Tecnigral wanted to build a web-based solution to help Madrid citizens send requests to their city council to better maintain local tree growth. In July 2010, the cloud-based version of the web-based solution 'Un alcorque, un árbol' went to market. It was adopted by Madrid City Council to help manage more than 245,000 trees around the capital, which are cared for by 300 maintenance workers. The rapid scalability of the services helps to cope with spikes in demand.	http://www.microsoft.eu/cloud-computing/case-studies/cloud-helps-the-city-of-madrid-stay-green-one-tree-at-a-time-cm1l.aspx

	Description	Website address
SPAIN Catalonia	The Government of Catalonia (Generalitat of Catalonia), based in Barcelona, needed a cost-effective and easy way to upgrade their IT infrastructure, in order to expand to 144,000 users. It decided to fully migrate to cloud services transferring 10,500 users to email services via Microsoft Exchange 2010. The initiative is expected to generate savings varying from 20% in the migration from previous Microsoft Exchange versions up to 83% in those from previous operator email services. Moving and consolidating email services to the private cloud in the new data centre of the Catalonian government should increase flexibility for civil servants, with a combination of heavy and light users across one application.	http://www.microsoft.eu/cloud-computing/casestudies/private-cloud-services-for-the-government-of-catalonia-c19m19l.aspx
UK London	The London Borough of Newham is a local authority that serves a population of around 250,000 east of the City of London. By sharing services with the neighbouring local authority of Havering, Newham is pioneering a transformation in both councils with the use of cloud computing. Its online portal service, which is available to every resident, will encourage more people to conduct transactions online rather than at council offices. With reusable technology, the platform is to contribute to Newham and Havering's target of more than €13 million cashable savings between them, without cutting front-line services.	http://www.microsoft.eu/cloud-computing/casestudies/pioneers-for-it-services-for-the-public-sector-use-cloud-to-cut-costs-and-improve-service-cm1l.aspx
UK East of England	NHS East of England (EoE) is the Strategic Health Authority (SHA) for the region, providing leadership to 40 local NHS organisations. NHS EoE was tasked with recruiting 10 host organisations to participate in "Safety Express", which aims to significantly reduce patient harm from pressure ulcers, catheter acquired urinary tract infections, falls and venous thromboembolism. Each selected host organisation then formed an improvement team of up to 10 healthcare professionals to work across primary, community, acute and social care within the region. NHS EoE uses Huddle (see Table 2 above) to co-ordinate the project. This means teams working at different locations can share documents, conferencing facilities are available, and Huddle can also be accessed from any location at any time.	http://www.huddle.com/customers/case-studies/nhs-east-of-england/

Source: Microsoft, *Towards a 'Cloud-Active' Europe – Examples of Member State and Regional policies and investments helping Europe realize the potential of cloud computing*; http://www.huddle.com/customers/case-studies/nhs-east-of-england/.

Table 4: Examples of government cloud computing projects beyond Europe

	Description
'U-cities' (SOUTH KOREA)	In South Korea the government is adopting cloud technology for the provision of government services, such as in the fields of tax payment, business licensing, vehicle registration and education. For example, in the field of education it plans to develop a cloud computing network, where students can store digital textbooks that they can access from their laptops or smartphones. One major part of the South Korean government's plans for the development of cloud computing in the public sector is its promotion of ubiquitous cities, or 'u-cities'. These cities are referred to as 'ubiquitous', as the exchange of information is theoretically possible anywhere and at any time. Data can be shared between all major information systems – not only governmental, but also business and residential – and computers are built into all buildings and streets. The aim is to allow services to function more efficiently, by speeding up and extending the flow of information. Some of these u-cities are making use of cloud computing technology, such as the city of Busan. The city has recruited the help of Cisco and Korean Telecom to deliver cloud-based city services to mobile devices. These 'Smart+Connected Community' (S+CC) services, which will cover areas such as urban mobility, energy management, distance learning and security, should be available to city workers by 2012 and all citizens by 2014. As part of the project, Busan is rolling out comprehensive wireless Internet coverage across the city, which will be available to all residents and visitors who own a mobile device.
Apps.gov (UNITED STATES)	In the United States the federal government implemented an official cloud computing storefront for the public sector, Apps.gov, in order to streamline procurement processes for cloud services and reduce the costs for federal agencies to acquire cloud services. Cloud service vendors are invited to submit their cloud services to the GSA (US General Services Administration) for approval, following which the services are made available. The site features a complete listing of all approved cloud services available to federal agencies. The cloud services primarily aim at increasing operational efficiencies and optimising common services and solutions across organisational boundaries. Vendors and services provided are categorised according to the type of services they provide: Software as a Service (SaaS) (mainly in the form of productivity and business Apps); Infrastructure as a Service (IaaS) (IT services offerings); and social media. Examples of implementation include the Federal Labor Relation Authority (FLRA), which moved to a cloud-based Software-as-a-Service case management system that allows users the flexibility to monitor case activity anytime and anywhere. The projected results are big reductions in the total cost of ownership, up-front licensing costs, annual maintenance costs, and hardware acquisition costs.

Source: Information on South Korean smart cities retrieved from http://gigaom.com/cleantech/ibm-cisco-microsoft-plan-green-cloud-cities/; http://daviddeans.ulitzer.com/node/1731851/; http://blogs.planning.org/sustainability/2011/11/03/cloud-based-services-infrastructure-transforms-busan-metropolitan-city/; http://blogs.cisco.com/government/cloud-based-services-infrastructure-transforms-busan-metropolitan-city/#more-44979/; http://www.good.is/post/south-korea-s-making-the-switch-to-digital-textbooks/, March 2012 Information on US government cloud computing retrieved from https://www.apps.gov/ and http://www.info.apps.gov/content/federal-cloud-computing-case-studies/, March, 2012.

2 USE AND POTENTIAL BENEFITS OF CLOUD COMPUTING

KEY FINDINGS

- Surveys show that most online consumers use cloud computing in the form of webmail services, with a little less using online applications for sharing content. The main benefits of the cloud for consumers relate to convenience, flexibility, reduced costs, ease of use, the ability to share content, improved access to information and online content, automatic maintenance and updating, and potentially better security.
- Businesses stand to benefit most by avoiding capital expenditure for IT, and being able to scale IT resources; this implies lower barriers to entry, bringing new products to market more quickly, and can help the creation of innovative SMEs. Businesses can also work together more effectively thanks to project management and collaboration cloud services. Furthermore, businesses with innovative ideas can use cloud providers' infrastructure to design custom applications and provide original services and products to consumers, businesses and administrations.
- The same cost-saving benefits for businesses also apply to governments, but governments can also benefit from cloud technologies by increasing the quality and innovation within e-government services they provide to citizens and businesses - services that could reduce citizens' and businesses' administrative burdens. There are already examples of public administrations, both locally and nationally, which have either adopted or are planning to adopt cloud-based services, and increasingly governments are developing comprehensive cloud computing strategies.

2.1 Current use of cloud computing and potential benefits for consumers

Most of the research on consumer use of, and attitudes to, cloud computing applications and services comes from the US. According to a 2011 survey by Ipsos ITX MediaCT,[30] 90% of online Americans acknowledge use of cloud-based services when asked about brands that offer cloud-based solutions. A large majority of consumers (76%) use webmail services such as Hotmail or Gmail; 61% use social networking cloud-based services; a little less than a third (31%) stream video and music from cloud-based services such as Netflix; 17% store and share personal photos online; 10% use cloud-based office software such as Google Docs; and only 7% use online storage or backup services. However, most of them do not know what the term 'cloud computing' means, as evidenced by the fact that only about half of respondents indicated they were familiar with cloud-based email.

[30] Ipsos OTX MediaCT, *Head in the clouds? Cloud computing and consumers*, Free year-round insights Technology Edition #2, June issue, 2011, at http://www.ipsos.com/mediact/sites/ipsos.com.mediact/files/pdf/Head%20in%20the%20clouds.pdf. Comparable survey data related to cloud computing in the European context is not available in the public domain.

Another report by the market research NPD group showed similar findings, with 76% of respondents reported using some type of Internet-based cloud service in the last year, with email, tax preparation and online gaming as the most popular, though photo and video sharing (on social networking sites, Picasa, Flickr or YouTube) as well as office applications and back-up and storage also on the rise compared with a Pew Internet report of 2008.[31] The research shows that cloud applications have not supplanted computer-based software as yet.[32] Further, the report highlights the fact that tax services are the only type of cloud application consumers seem to be willing to pay for.

Many consumer-targeted cloud services are provided as free services based on customer profiling and targeted advertising business models. So essentially these models are monetizing consumer personal data (for example by automatic scanning of emails or logging of transactional data), though consumers are not necessarily aware of the trade-off (see also Section 4.2.3 on privacy, below). Others, usually more office-oriented applications provide advertisement-free services. They may have reduced security or functionality compared with their paid-for equivalents, with the aim of building up their paying client base, similar to a free introductory offer.

It is not unreasonable to assume that similar usage figures, particularly for use of web-based email, would be revealed in Europe and particularly in the countries with high penetration broadband - but clearly absence of such public research is a gap at the EU level, which could be easily remedied (see recommendations, Section 7).

The expansion of cloud computing for individual consumers has also been fuelled by rapidly increasing use of smart phones to access various applications over the Internet - for example Vodafone reported that smartphones were responsible for 21% of all data traffic on its European networks in September 2011, compared to 12% in March 2011.[33] A further impetus to consumer take-up of cloud computing applications has been the success of the tablet PC and the launch of the iCloud by Apple which hosts and delivers a multiplicity of content over the Internet and is accessed through any number of user devices. The Google Chromebook, released in the second part of 2011, is specifically geared to get users to do everything via the web (see also Section 2).

The main benefits supported by respondents were access from anywhere and any device (37%), the ability to back up data (29%), and saving on computing costs (21%) - though in all three cases less than half of respondents agreed and in the case of savings only a substantial minority of a fifth. The potential benefits of cloud computing are therefore yet to be realised or understood by many consumers. The earlier Pew Internet survey found similar benefits for consumers, in addition to ease of use and the ability to share information with others.

[31] See https://www.npd.com/wps/portal/npd/us/news/pressreleases/pr_110809.

[32] 24% of respondents reported purchasing traditional software in the previous 6 months. For the 2008 report, see Pew Internet and American Life Project, Horrigan, J. B., *Data Memo re Use of Cloud Computing Applications and Services*, 2008.

[33] Ofcom, *International Communications Market Report,* 2011, p. 234 et ff, for this and other similar statistics see http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/.

Table 5: Examples of consumers' benefits from cloud computing

Agreement	Total	Male	Female	18–34	35–54	55+
Being able to access my files or data from anywhere and any device, not just at home, would be really useful	37%	38%	35%	46%	35%	29%
I would only use 'the cloud' to back up copies of files or data that I already have on my computer or hard drive	29%	30%	28%	32%	29%	26%
I'd expect 'the cloud' to make my computing cheaper overall	21%	26%	17%	27%	19%	16%

Source: Ipsos OTX MediaCT, *Head in the clouds? Cloud computing and consumers*, Free year-round insights Technology Edition #2, June issue, 2011, at http://www.ipsos.com/mediact/sites/ipsos.com.mediact/files/pdf/Head%20in%20the%20clouds.pdf. Base: 1007 internet users aged 18+ (male = 489, female = 518, 18–34 = 307, 35–54 = 386, 55+ = 314)

There are other important benefits for individual users: the maintenance of their technology equipment and software is more hassle-free, by removing the complexity of managing all the updates or latest versions of software or replacing equipment to buy more and more storage capacity for all their music or videos. Consumer organisations interviewed also pointed to the security of the information stored in the cloud as a potential benefit, as it gives consumers various features, such as encryption, that would be too complex for the majority to use themselves. Consumers can benefit from the potentially improved security of cloud providers, in the form of economies of scale of many protective technical measures, such as filtering and preventing attempts to stop the service ('denial-of-service attacks'), security software update management and configuration of operating systems, employing security experts, preventing physical access to data centres and so on. Large providers can also replicate data in more than one location, and reallocate resources fast when under attack.[34] Some of the applications available in the 'cloud' can also enhance personal financial security in Internet transactions, for example payment intermediaries. However, security is flagged as a double edged sword, as shown in Section 4.2 below.

The box on the next page provides a summary of the potential benefits of cloud computing for end users:

[34] ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009, pp.17-20.

Box 1: Summary of potential benefits of cloud computing for end users[35]

Lower computer costs. A high-powered computer is not needed to run cloud-based applications. Since applications run in the cloud, a desktop computer does not need the processing power or hard disk space demanded by traditional desktop software, or even a DVD drive.

Improved performance. With fewer programs using the computer's memory at the same time, it will perform better. Desktop computers that use cloud-based services may boot and run faster because they have fewer programs and processes loaded into memory.

Reduced software costs. Instead of purchasing software applications, cloud computing applications can often be obtained for free. An example is the Google Docs suite for consumers.

Instant software updates. Updates to a cloud-based application generally occur automatically and are available on logging into the cloud. When accessing a web-based application, the latest version is usually instantly available, without need for an upgrade.

Improved document format compatibility. All documents created by web-based applications can be read by any other user accessing that application. There are fewer format incompatibilities when all users are sharing documents and apps in the same cloud.

Unlimited storage capacity. Cloud computing can offer virtually limitless storage. A computer's current hard drive space is small compared to the storage space available in the cloud. Note however that large scale storage is generally not available for free, even in a cloud environment.

Increased data reliability. Unlike desktop computing, in which a hard disk crash can destroy personal data, a computer crashing in the cloud should not affect the storage of data, as typically cloud services provide multiple layers of security (see however Section 4.2 below for a discussion of data security in a cloud environment).

Universal document access. Documents stay in the cloud, and can be accessed from wherever with an Internet-capable device and an Internet connection. Documents are instantly available independent of location, removing the need to carry them when travelling.

Latest version availability. When editing a document from one location (e.g. at home), that edited version is identical to the document accessed from another location (e.g. at work).

Easier group collaboration. Multiple users can collaborate easily on documents and projects. Because the documents are hosted in the cloud, not on individual computers, an Internet connection is all that is needed to collaborate.

Device independence. When changing computers or moving to a portable device, existing applications are still available. There is no need for a special version of a program for a particular device, or to save a document in a device-specific format.

[35] Source: Adapted from Miller, M., *Cloud Computing Pros and Cons for End Users*, February 2009. http://www.informit.com/articles/article.aspx?p=1324280.

2.2 Current use of cloud computing and potential benefits for businesses

Cloud computing can be seen as a turbo-charged and flexible form of outsourcing by a business or organisation. It reduces their IT management overheads, while also enabling the large-scale consolidation and optimisation of computing hardware and software resources. Instead of investing capital on buying expensive equipment, companies only need to allocate operational budgets to 'rent' access to those services that are required at any given time. This can level the competitive playing field, making large-scale computing resources available for the first time to small businesses and other organisations that do not have a suitable infrastructure in place (including, at a macro scale, emerging economies, at least for those regions that have a sufficiently reliable and fast broadband infrastructure in place).[36] At the cloud provider level, aggregation levels the peaks and dips in demand variability, so allowing higher server utilisation rates.[37]

As indicated in the previous section, cloud services can support all kinds of business applications and services, covering the full range of business requirements - from business continuity planning, to coping with spikes in demand, to a fully outsourced service.[38] They can enable businesses to bring new products to market more quickly, through more effective collaboration as well as the availability of powerful, cheap computer resources.

Clouds allow business processes to be linked together between many different providers, and enhance the collaboration between different departments of the same organisation. An example for an EU-based business that started from scratch to provide cloud-based networking and project collaboration services to business and governments is presented in the following box.

[36] World Economic Forum, *Exploring the Future of Cloud Computing*, 2010, p.3. See also OECD, *Cloud Computing*, forthcoming.

[37] Microsoft, Harms, R. & Yamartino, M., *The Economics of the Cloud*, Microsoft whitepaper, 2010, p.2.

[38] European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010, p.1.

Box 2: Huddle: 'Collaboration in the cloud'[39]

Huddle is a UK-based start-up cloud provider founded in 2006, which focuses on what they see as a new market, called 'content collaboration' where collaboration and content management converge. According to Huddle, "90% of this collaboration is happening between businesses rather than internally, which is why it's so important that you can collaborate across the firewall". Similarly, according to Huddle more than 75% of UK central government departments make use of their platform for collaboration purposes. For the UK government they have built a private version of Huddle, which is "sitting directly on government servers, so no-body else has access to it." The fact that Huddle is based in the UK has proven an advantage to European clients - in particular governments who are "very keen to keep their data not only in Europe but also working with a European provider rather than going to companies [based in the US]." along with a tool allowing users to export their data from Huddle at will. They cite the main obstacle to providing their service across borders as different data protection policies, but also that vertical markets in different countries have different regulations. Huddle's future vision for cloud computing is a drastic reduction in the waste caused by the duplication of efforts inside and between companies and administrations – "our vision is to make sure that all this knowledge that is still locked up in your email inboxes, on your desktop, on your servers, or some other legacy system, is available for everybody to use" - with a particular focus on opening the market to SMEs.

For all sorts of businesses or public and private organisations cloud computing can provide both flexibility and cost efficiency. It minimises infrastructure costs, allowing companies to experiment with novel services and smoothly scale those that are successful from thousands to millions of customers, without needing a large up-front investment in computing systems. This would mean potentially much lower barriers to entry for starting-up businesses and entrepreneurs, which in the medium and long term also means growth and jobs.[40]

According to recent industry surveys, current take up of cloud computing services by business is still in its early days, though gradually gaining momentum. A 2011 survey with 500 European IT decision makers (CIOs) in five EU countries,[41] shows that a minority of the businesses surveyed have adopted cloud services throughout the company; the most popular company-wide cloud applications being phased in are basic computing infrastructure needs such as website hosting, email hosting, database hosting, servers and storage (between 20-24% of companies). Other applications used (partially or throughout the company) are desktop applications, human resources, payroll/finance, customer relationship management, business intelligence and supply chains. The survey further shows that, as the transition from an existing infrastructure to something completely new is a daunting prospect for many companies, the ease of transition is the top key enabler to make them do so (58%), followed by quality

[39] Source: Civic Consulting interview.

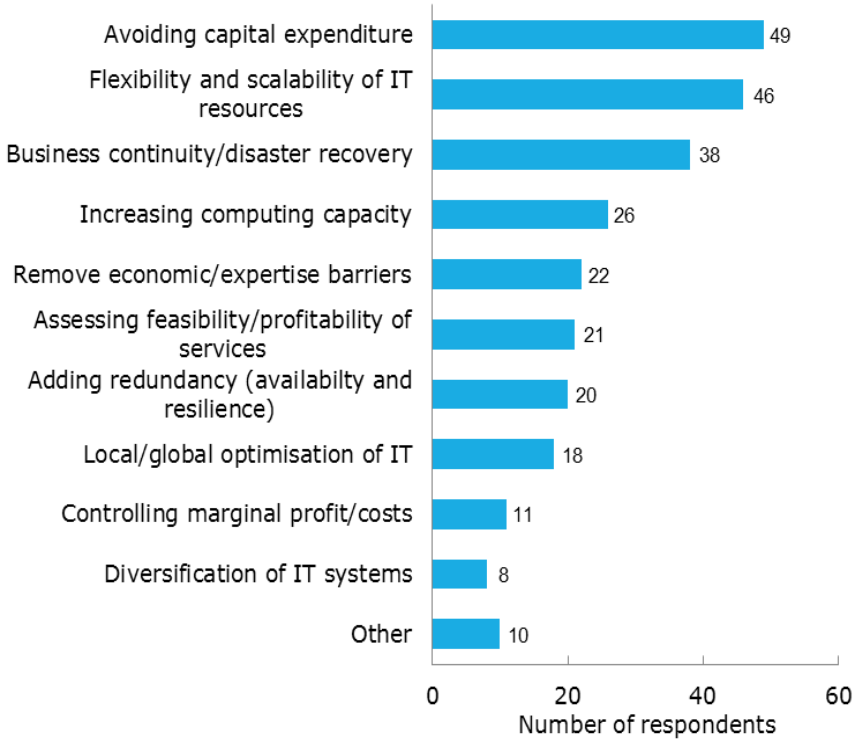
[40] For example, one study found that under certain assumptions cloud services could enable new and existing companies to create between 300,000 and 1.5 million jobs in Europe in 2009-2014; see Etro, F., *The Economic Impact of Cloud Computing on Business Creation*, *Employment and Output in Europe*, Review of Business and Economics, Vol. 54, 2, 2009, pp. 179-208. Note that this refers to gross, not net, job creation.

[41] Colt, *European CIO Cloud Survey*, April 2011, p.3, at http://www.colt.net/cdnucm/groups/public/@cdn/@public/documents/generalcontent/cdnp_005990.pdf.

assurance and cost-saving pressures (55% each) as well as regulatory issues linked to data protection and security (54%) (see Section 4.2 below). Overall, according to this survey, the adoption of platform as a cloud services (PaaS), i.e. using the cloud for development of new or custom applications is still in its infancy in Europe.

ENISA, the European Network and Information Security Agency, carried out a detailed survey of the small and medium business (SME) perspective on cloud computing, to inform its wider work on security risks assessments. Over a quarter of the responding companies had fewer than 10 employees. It found that by far the biggest reasons for SMEs considering cloud services for adoption are avoiding capital expenditure for IT and the flexibility and scalability of IT resources it brings:

Figure 3: Motivations for business to use cloud computing



Source: ENISA, Catteddu, D. & Hogben, G. (eds.), *An SME perspective on cloud computing- Survey*, 2009, Drivers - Question 3. Reproduced here with permission.

As well as the money-saving potential, flexibility and enabling start-ups to enter the market, organisations we spoke to emphasised another major benefit of cloud computing, which may be one of the most important ones in the long run as an innovation enabler: people can do things with cloud computing they have not done before, or can do the same things as before but in a new and more efficient way. A typical comment made by one interviewee regarding the potential gains for small and medium-sized companies is as follows:

> *"SMEs … can have access to their resources and their capacity easily from the cloud. With the cloud they can set up operations and they can network. …The potential is enormous for companies to go international, and to sell products worldwide. It's not just the single market - there's a worldwide dimension."*

However, as the box illustrates with an example from the area of e-health, many challenges remain for companies willing to expand cloud-based services across borders (such as differing privacy requirements in EU countries, see also Section 5.1 below).

Box 3: KMS Sales and Solutions: 'Hybrid clouds for new healthcare services'[42]

KMS Sales and Solutions is a German SME founded in 1996 that provides data solutions for the healthcare industry, to better manage facilities, staffing, and patient needs. In particular they now provide a cloud-based service called Eye on Health, which they claim 400 hospitals are currently using in Germany, roughly 20% of the market. The service, which uses a cloud-based database to extract data, works by combining hospitals' own data (such as private data concerning patients, doctors and illnesses in general) with data from public sources (such as geospatial, socioeconomic, epidemiological and demographic data) and then making this information publicly available for healthcare providers, consumers, and investors. The sensitive data therefore does not leave the hospital, whereas the public data emerges from the cloud, creating a hybrid cloud. Healthcare providers and administrations can use the service to pinpoint specific medical needs, while investors can plan future health services based on the market data. In particular, KMS suggests that Eye on Health could be used to make information available to the general public, for example with "an overview of which hospitals are better at dealing with certain procedures than others, or even where certain procedures are available or not. And you could combine that and say 'this is your location, what's the nearest hospital which deals with certain types of diseases'." A crowdsourcing tool for consumers is also envisaged via an app for smartphones, "with which we can take the location of the person using the application and by which they can then submit the disease instances they have seen". They find that such services could also be extended to other EU countries, but this would again require harmonisation in privacy and data protection rules: "privacy is dealt with [differently] within the different countries, different systems are being used, and it's extremely difficult and expensive for any vendor to deal with that in the European field [of healthcare]."

[42] Source: Civic Consulting interview.

2.3 Current use of cloud computing and potential benefits for public authorities

As already indicated in Section 2 above, government cloud users are often initially focused on the cost reductions that cloud systems can bring, for example by using cloud-based productivity and project management tools that are also popular with businesses. The US government's Federal Information Technology programme includes a 'cloud first' policy, with an immediate goal of moving 20 billion US Dollar of the total federal 80 billion US Dollar budget earmarked for IT spending to cloud services.[43] The UK government's cloud strategy is following this approach, and promises that "the government will be able to more easily exploit and share commodity ICT products and services. This enables the move from high-cost customised ICT applications and solutions to low cost, standard, interchangeable services where quality and cost is driven by the market. It means changing the culture of government to adopt and adapt to the solutions the market provides and not creating unnecessary bespoke approaches."[44] The six initial commodity services established under the UK government's 'G-Cloud' programme by government departments, agencies and a local council are:

- Collaboration (Software as a Service, SaaS)
- Infrastructure as a Service and Platform as a Service (IaaS and PaaS)
- Email (SaaS)
- Customer Relationship Management (SaaS)
- Web Hosting and online Content Management Systems (IaaS and PaaS)
- Enterprise Resource Planning

Other departments will be mandated to build on these services wherever possible, rather than procure their own custom-made systems. There will also be cross-programme core services, such as Identity Assurance and Management, and monitoring of security threats.[45]

As well as gaining significant cost savings, governments are planning to use cloud technologies to increase the quality and innovation within the services they provide to citizens. This will result from increased competition between suppliers, the ability to rapidly prototype and trial new systems, and lower barriers to entry for smaller businesses. To this end, the UK government has just launched a 'Government Application Store', called the Cloudstore that will allow government users to compare accredited cloud software against their own requirements.[46] The store features some 1,700 applications provided by 250 businesses, which can be accessed on a pay-as-you-go basis by any government department without the need for lengthy procurement procedures. About half of businesses featured are small and medium size enterprises. Most of these services will have to undergo an accreditation and assurance process, so this is still work in progress.

[43] Kundra, V., *Federal Cloud Computing Strategy*, 2011, p.1.
[44] HM Government, *Government Cloud Strategy*, 2011, p.6.
[45] Ibid, pp.5, 12, 13.
[46] http://www.govstore.net/.

The box on the next page provides an overview of expected benefits as outlined in the UK government's G-Cloud strategy, published in March 2011 as a 'sub-strategy' of its wider ICT strategy:

Box 4: Expected benefits as outlined in UK government's G-Cloud strategy[47]

Many more common commodity solutions – a range of the best industry ICT services and solutions available off the shelf so the government, its agencies and related bodies can use what they need when they need it and not create duplicate services that cannot be shared;

Flexibility and freedom – the ability, if required, for departments and organisations to change service provider easily without lengthy procurement and implementation cycles, no 'lock-ins' to long contracts and the freedom to quickly adopt better value and more up to date solutions;

Ready and easy to use – complete solutions that are already assured for security, performance and service management. Ready access to 'hybrid cloud' solutions that allow the cost efficiencies of the 'public' cloud to be used alongside more secure / dedicated private cloud solutions based on a consolidated data centre and service estate;

Low cost – Services that are paid for on a usage basis, driven by strong competition on price and quality. Transparent costs along with quality and scope-of-service metrics for simpler comparison and control;

Competitive marketplace – a range of service providers constantly improving the quality and value of the solutions they offer, from small SME organisations providing niche products to large scale hosting and computer server capacity;

The strategy also mentions related benefits to business, which include transparency and an open marketplace, avoiding lock-in to long-term service contracts, simple and fair procurement, and freedom to innovate.

[47] Source: HM Government, *Government Cloud Strategy*, March 2011, p.6.

The costs savings for the central government for shifting to a cloud computing model is projected to be as in the following table:

Table 6: Projected UK central government savings when shifting to cloud technologies

Cloud strategy elements	Savings by year in millions of GBP			
	2011-12	2012-13	2013-14	2014-15
G-Cloud & Application Store	-	20	40	120
Data Centre Consolidation	-	20	60	80

Source: HM Government, *Government Cloud Strategy*, 2011, p. 16.

The UK Government Cloud Strategy is currently one of the most advanced formal pan-government and specifically cloud-computing related strategy within the EU that was reported to us during the research for this study. Nonetheless, a number of cloud computing initiatives are incipient, and some of the EU Member States are advanced in their implementation of overall digital strategies and provision of e-government services. As mentioned in Sections 5.3 and 6.2, a key issue will be ensuring interoperability of these government clouds. Estonia and Austria are notable examples of advanced e-government strategies, but at present their systems may not be strictly defined as using 'cloud computing' as understood by the NIST definition (see Section 2) and were developed well before the 'cloud' became a widely discussed topic.

Austria for example has a comprehensive digital and e-government strategy[48] and is in the process of formulating and implementing a new cloud computing strategy as an element of it.[49] Estonia has digitalised all its administrative systems as far back as the 1990s and currently has some 200 databases (state and private ones) that are connected to the e-government system using a unified standard (called the X-Road), that helps provide over 1,000 services both in electronic and mobile form.[50] As explained by Estonia's President in a recent speech at the London Conference on Cyberspace, the X-Road, and digital signatures for authentication, are the two key elements in their whole e-government system, which is accessed via a single portal, *eesti.ee* - the one-stop shop for these hundreds of various e-services (see the following box).[51]

[48] See http://www.bka.gv.at/site/6506/default.aspx/.

[49] An interviewee from Austria summarised the current situations as follows: "… we've prepared a position on Austria's approach toward cloud computing and in the next year we will set up the detailed implementation of this position paper, how and in what areas we are able to move into the cloud, or what type of cloud, public/private clouds, so I would say we have added an approach according to our e-government strategy."

[50] See http://www.ria.ee/x-road/.

[51] President Ilves, speech at the London Conference on Cyberspace, 1 Nov 2011, http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/on-demand-video/on-demand-day-1/.

Box 5: The Estonian system of e-government[52]

The two key elements underpinning Estonia's e-government infrastructure are digital signatures for authentication and a secure, decentralised data management system, 'the X-Road'. Digital signatures are a universally binding method allowing citizens to sign any legal document with notary power (i.e. as if the document were signed on paper in the presence of a witness and certified by a notary). The digital signature was passed into law in 2000; it was first used with chip-based smart cards and card readers, later with mobile phone-based applications and implementation. The advantage of such an open design from the start is that any new public or private application simply builds on top of the existing trust between citizens and the state and does not inhibit surrounding technologies from evolving over time. The X-Road was launched in 2001. It links together Estonia's various e-services and databases, both in the public and private sector. Initially, it was developed as an environment that would facilitate making queries to different databases. Now, a number of standard tools have been developed for the creation of e-services capable of simultaneously reading from and writing to multiple databases, transmitting large datasets, and performing searches across several databases. According to an Estonian government representative it is the linkage of databases – e.g. health records and digital prescription - that has allowed the X-Road to be successful in fostering the provision of e-services (via the national web portal eesti.ee) where standalone service systems have failed. Any government agency or business can choose or create their desired product, meaning new services can be added one at a time as they become available. Now more than 100 organisations have joined the X-Road, resulting in the creation of over 1,000 new services.

In terms of benefit and visibility to its citizens, the Estonian system is already a very, and probably the most, comprehensive e-government system in the EU. According to the Estonian Systems Authority, all that would remain to 'cloudify' its systems is the 'virtualisation' of the data centre, or consolidation of the different (private) data centres. Learning from the Estonia experience, the EU close neighbour and partner country Moldova has recently (September 2011) launched its own e-government strategy based on a 'private cloud' model, i.e. with a cloud specifically reserved for government purposes, designed to transform the country's governance system by 2020.[53] This is a good example of how benefits of the cloud computing model can be put to societal use in a country with limited resources, relatively small broadband penetration, and some corruption in government which the strategy is also designed to solve, as 'computers cannot be corrupted'.[54] The strategy envisages consolidation of dozens of existing data centres into just a few.

Other countries are also setting out government strategies such as the Digital Agenda in France, Germany's Trusted Cloud program, the Irish Program for Government Computing, and the Netherlands Central Government Digital Work Environment. In general, these programs aim to join up infrastructure, reduce costs and invest in better, more secure cloud computing which will be used more widely.

[52] Interview with Estonian Information Systems Authority; President Ilves, speech at the London Conference on Cyberspace, 1 Nov 2011; see also http://www.ria.ee/x-road/.

[53] Interview with the e-Government Centre of the Republic of Moldova; see also http://egov.md/upload/Proiect%20Strategie%20Tehnologica.pdf.

[54] President Ilves, speech at the London Conference on Cyberspace, 1 Nov 2011, as above.

Throughout the EU, there are individual examples of local or national public administrations that have adopted cloud services (see also Table 3 above). The extent to which this is happening in the EU has not been adequately surveyed,[55] although a number of case histories is quoted, including on the dedicated websites of the large cloud service providers Google and Microsoft.[56] Several of these schemes are innovative and ambitious, for example the planning and construction of a sustainable smart city in the Portuguese municipality of Paredes, called PlanIT Valley; or a Citizen Service Platform used by 200 small municipalities in Spain, for services such as e-forms, secure transactions or case management (see the following box on PlanIT Valley).[57]

Box 6: PlanIT Valley - a 'smart' city prototype making use of the cloud[58]

PlanIT Valley is being developed in northern Portugal with the endorsement of the Municipality of Paredes and the national government. It will be built in a series of phases and will house a population of 225,000 when completed in 2015. It is to be a prototype smart, sustainable city, where all waste is processed and recycled on site. At the core of PlanIT Valley lies the Urban Operating System, a technology platform that allows for the sustainable management of resources while enabling software developers to provide innovative solutions and applications through a cloud-based platform, PlaceApps. These will be similar to apps for smartphones, only they will make use of the entire city's databases and cloud technology. Cloud-based computing is central to bringing all the technology together, whether it be in computer and mobile telephone network infrastructure, city traffic management, waste services routes, supply chain management, optimum control of peak electricity demand, assisted parking, or emergency services. 'Urban indicators', automatically-gathered metrics, will measure the economic, social, environmental and institutional aspects of PlanIT Valley to ensure that the city's development continuously adapts to changes with real-time modelling and simulation. Waste should be minimal, since careful analysis of the indicators will be used to manage resources and improve processes, and applications will be built on reusable technology, and smart metering will enable the Urban OS to monitor resources so that each building has the energy and water it requires. Along with PlaceApps, PlanIT valley will have many online services that residents will be able to access via an online platform.

[55] See also Section 2.2 above, re a global survey by Redshift Research, *Adoption, Approaches & Attitudes: The Future of Cloud Computing in the Public and Private Sectors*, 2011, p.12. The survey shows that globally overall a majority of public authorities are still in the investigation stages when it comes to cloud computing.

[56] See http://www.google.com/apps/intl/en/customers/index.html#tab0/ and http://www.microsoft.eu/case-studies/.

[57] Microsoft, *TOUCH - Microsoft Technology in Government, Education and Healthcare*, 2011, pp 19, 28. Available at http://www.onwindows.com/digital-editions/touch/2011/spring/default.aspx. For an advanced example of such smart city planning, see Table 4 regarding the development of 'ubiquitous computing' cities, or 'u-cities', in South Korea.

[58] Source: Ibid, pp 19; see also http://living-planit.com/planit_valley.htm.

The examples provided in this section indicate that public administrations, as for business, need good motivation to adopt cloud computing on a strategic country-wide level; cost reductions play an important role, but not always the most important one as public administrations tend to use 'private clouds' for their needs, which, depending on the applications and services, may not achieve such large cost reductions as 'public clouds' (see Section 2.1.3 above). The drivers to adopt cloud computing models may be different for different countries, depending, for example, on the administrative structure and culture, as well on the political will to establish an e-government strategy. However, as has been illustrated above, potential benefits are expected to be significant. One of the interviewed EU officials, an expert on public administration services, sees cloud technologies as a transformative factor, both in the context of reducing administrative burdens, and as giving citizens better value and control:

> *"[Cloud computing] is one of those key enablers to transform public administrations… it will have an impact in terms of efficiency, or effectiveness, because public authorities will be able to reuse services from some of their colleagues in order to offer better service. […] …some Member States have done [this] already, to reduce the administrative burden by asking just once for information. [….] It will also enable the private sector or the citizens to have services delivered to themselves where they wish, which is why it will empower them."*

3 RISKS RELATED TO CLOUD COMPUTING

KEY FINDINGS

- The biggest perceived barriers for both consumer and SME take-up of cloud computing are lack of privacy, data security, provider lock-in, lack of standardisation, and jurisdictional issues relating to applicable law and law enforcement access to data.
- Potential general data security risks arising from cloud computing relate to: an increase in threats to data confidentiality due to the concentration of data on common cloud infrastructure; the loss of IT control and governance by organisations using cloud services; and an increased risk of data interception in authentication and transmission procedures.
- Transparency is often lacking in providers' provisions concerning data security, in particular a lack of data integrity guarantees combined with disclaimers of liability clauses in contracts; a lack of standards regarding data control and security; and often unclear and incomplete information concerning security and privacy on cloud providers' websites.
- Multiple approaches exist to tackle these vulnerabilities, such as differentiation of the level of security needed by sensitivity of data or use of a 'private cloud' managed by the organisation itself or a provider. Additional data security assurance could also be provided through a form of audit and certification systems of cloud services providers.
- The main challenges surrounding the legal issues regarding privacy relate to: ambiguities as to the role of the cloud service provider; uncertainty regarding applicability of EU laws; the need for more effective data protection; uncertainty regarding laws governing international data transfers, and the lack of universality in data protection legislation.
- Law-abiding consumers or business users storing their data in the cloud may well be affected by compulsory orders for disclosure, without notification, as in a public or shared cloud authorities may seize the servers or computers containing personal information of the guilty and innocent alike; this is compounded by a lack of standards in providers' 'thresholds' of disclosure.

As discussed in Section 2 above, cloud computing is not a new technology but is a new model of networked computing. Providers of the various services can be located anywhere in the world and the data centres holding users' data can be located anywhere in the world, including in several places simultaneously. Furthermore all users of cloud computing – consumers and organisations – give up partial or total control of their data by entrusting it to a provider. These two essential characteristics of cloud computing – diverse geography and control of information or resources – are at the core of the majority of risks and policy challenges related to cloud computing.

Some of these challenges are inherent to the nature of cloud computing, particularly risks around legal and contractual matters, data security and interoperability and standards. Other important issues are not new, but have been intensified further by the nature of cloud computing, chief amongst them information privacy and data protection.

In her recent speech to the World Economic Forum, Vice-President of the European Commission Neelie Kroes summed up well the challenges and barriers that stand in the way to her ambitious plans for a 'Cloud-active' Europe, following extensive consultations and research: "The results are clear: many still hesitate before the Cloud. They worry: how do I know what service I am buying? Will my data be protected? Which Providers can I trust? If I don't like what I am getting, can I switch providers easily? Or, if I really don't like what I'm getting, can I easily enforce the contract through legal action?"[59]

3.1 Consumer and SME concerns

Consumers' concerns, as expressed in surveys[60] and by consumer representatives, principally revolve around the use of their data and personal information which is entrusted to cloud providers. But there are other important consumer protection issues related to cloud computing provision, which were highlighted at a meeting organised by the Consumer Federation of America of EU and US consumer representatives, academic experts and industry providers.[61] As well as concerns regarding data use, main issues identified as concerning consumers are law enforcement access, provider lock-in, data security, and secondary uses of user data, consumer protection jurisdiction, and provisions for massive provider failures, such as bankruptcy or natural disasters (more on this below).

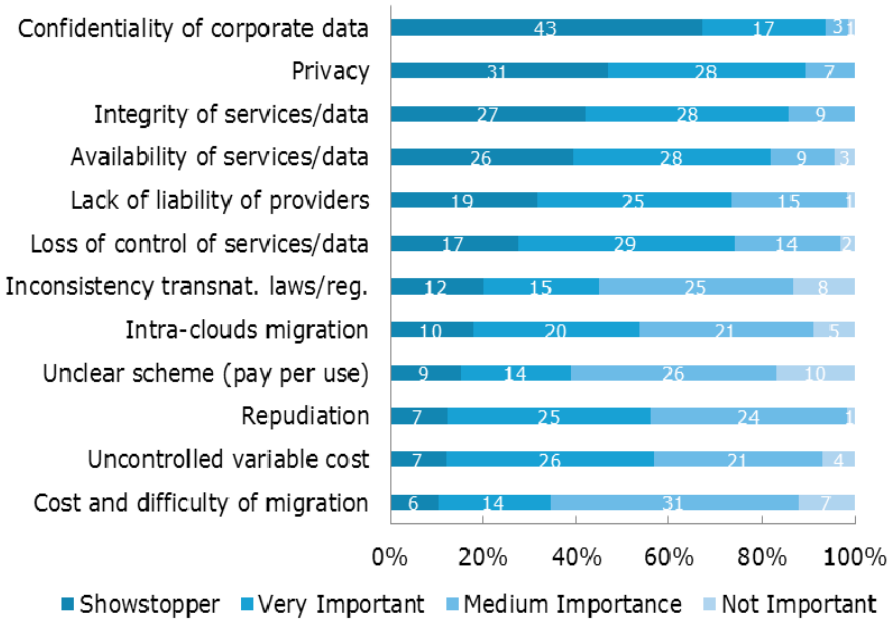
Business is also significantly concerned with privacy and security issues as shown in the graph below, with confidentiality of corporate data acting as the biggest potential showstopper for the surveyed SMEs, followed by privacy and integrity of services/data.

[59] Kroes, N., *Setting up the European Cloud Partnership*, Speech at the World Economic Forum, Davos, Switzerland, 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=0&language=EN&guiLanguage=en.

[60] Ipsos OTX MediaCT, *Head in the clouds? Cloud computing and consumers,* Free year-round insights Technology Edition #2, June 2011. P.9. 53% of respondents agreed with the statement "I'd be concerned about who 'owned' my data or files if they were stored in 'the cloud'".

[61] Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010.

Figure 4: SME main concerns regarding Cloud Computing



Source: ENISA, Catteddu, D. & Hogben, G. (eds.), *An SME perspective on cloud computing- Survey*, 2009. Reproduced here with permission.

According to the CIO survey mentioned previously, concerns about security remains the biggest hurdle impacting cloud take up (63% of respondents), but other issues are starting to emerge, such as supplier lock-in (46%) and geographic location (31%).[62] Other barriers to SMEs taking up cloud computing both as service providers and users include lack of standardisation to ensure them a single market across Europe, the diversity of relevant legislation across Europe (e.g. consumer digital rights, privacy, and security) and (for users) resistance to change business models.[63]

Governments and regulators also cite information security issues and fear of vendor lock-in as their two biggest worries, according to research carried out for the World Economic Forum,[64] and strongly confirmed by our interviews with government officials.

The main risks and concerns related to cloud computing are outlined in more detail below. The issues around diversity of jurisdictions, particularly relevant to the single market operation, are discussed in Section 5.1.

[62] Colt, *European CIO Cloud Survey*, 2011, available at http://www.colt.net/cdnucm/groups/public/@cdn/@public/documents/generalcontent/cdnp_005990.pdf.

[63] European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010, p.57. Available at http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[64] World Economic Forum, *Exploring the Future of Cloud Computing*, 2010: http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

3.2 Data security, protection and risk management

Security for cloud services is essential to protect personal, corporate, and government data. Security means protection from unauthorised access, integrity (i.e. information is not corrupted or changed or deleted by mistake), and backing up to safeguard against availability, integrity and confidentiality.

Security and protection of data has long been an issue in an online environment. But the cloud computing model introduces some new specific risks or vulnerabilities, as well as reducing others. On the one hand, as mentioned in Section 3.1, cloud computing can benefit from the economies of scale of many protective technical measures, such as filtering and preventing attempts to stop the service ("denial of service attacks"), security software update management and configuration of operating systems, employing security experts, preventing physical access to data centres and so on. Large providers can also replicate data in more than one location, and reallocate resources fast when under attack.[65] On the other hand, there are a number of potential increased risks as outlined in specialist studies such as the one produced by the European Network and Information Security Agency (ENISA). For example, the fact that services from different organisations are running on the same cloud service using data on the same physical media implies that failure to fully isolate services and to fully wipe deleted data can threaten security. A second example, also characteristic of cloud computing, is related to loss of IT control and governance by the organisations using the service – so conflicts could arise between customer and provider systems, or the rules and responsibilities could be unclear.[66] A third example concerns the fact that users manage and access their cloud accounts through the Internet, so that can increase security risks in transmission or through log-in (authentication) procedures, if the data is not encrypted in transmission or if the authentication is weak (such as only through a password).[67]

Such a concentration and centralisation of processes and data storage on the same data centres increases the risk of massive failure, since errors that would ordinarily affect only a single consumer or organisation in isolation now affect thousands, if not millions of people. An example of a site massively failing is the bookmark sharing site Ma.gnolia, which underwent a meltdown in 2009, with the service losing both the store of the user data and the back-up. The data was never recovered.[68] Other examples of failures, for economic or business scalability reasons include G.hos.t, a file sharing site that closed its business down giving users two weeks to retrieve and back up all their data.[69] A third example is the online personal finance advice site Wesabe, an innovative start-up site that closed down in 2010.[70] Less extreme but occurring more commonly are cloud provider outages: as shown in the table on the next page, most major cloud providers have had to deal with outages entailing a disruption in their service continuity, potentially causing considerable losses for consumers and businesses.

---

65 ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009., pp.17-20.

66 This is related to a lack of transparency regarding the operation of cloud services, which are often considered a "black box".

67 ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009. For isolation failure, see p.35; for loss of governance, see p.28; for management interface compromise, see p.37.

68 See http://www.wired.com/epicenter/2009/01/magnolia-suffer/.

69 See http://techcrunch.com/2010/03/02/ghost-cloud-files-shuts-down/.

70 See http://techcrunch.com/2010/06/30/wesabe-shuts-down/.

Table 7: Major reported cloud service provider outages

Cloud provider outage	Description
Microsoft (Sep 2011)	"Millions of Microsoft users were left unable to access some online services overnight because of a major service failure… Hotmail, Office 365 and Skydrive were among the services affected… The latest disruption is believed to have lasted for around two-and-a-half hours, between 0300 GMT and 0530 GMT."[a]
Google Docs (Sep 2011)	"The outage was caused by a change designed to improve real time collaboration within the document list… This change exposed a memory management bug which was only evident under heavy usage… The entire outage lasted around 30 minutes."[b]
Amazon EC2 (Apr & Aug 2011)	"Due to some serious failure in Amazon data centre in Northern Virginia in United States, Amazon Web Services (AWS) suffered a major outage… affecting thousands of websites that rely on AWS… Many start-ups and web companies… who hosted their services in the US East region were affected due to this outage."[c]
Intuit (Mar 2011)	"Two months ago, several of [Intuit's] popular services… went down in a cloud computing outage that the company blamed on faulty maintenance, effectively human error…"[d]. "Every aspect of Intuit's online presence, including its main website, was out for almost two full days."[e]
Gmail (Feb 2011)	"150,000 Gmail users [found a] blank page when logging into their Gmail account. Google promised a quick fix, but to some users, services go back on after four days of outage… Software bugs have affected several copies of the data."[f]
Hotmail (Dec 2010)	"Information from around 17,000 user accounts was suddenly deleted, and it took Microsoft two days to restore normalcy. Improper load balancing between servers was blamed."[d]
PayPal (Nov 2010)	"Internet payments system PayPal suffered a widespread outage that lasted for several hours late last week, leaving merchants using the platform unable to complete electronic transactions… A series of service interruptions meant that the PayPal website was unavailable to all users for a period of about four hours."[g]
Salesforce.com (Jan 2010)	"Almost all of Salesforce.com's 68,000 customers suffered at least an hour of downtime. The company reported 'systemic failure' in its data centre, with everything, including backup, going down for a brief period."[e]
Rackspace (Jun 2009)	"The hoster-turned-cloud provider suffered a major cloud outage in June of 2009, when a breaker flipped, a line of generator backups failed and several racks of servers went down."[e]

Source: a) http://www.bbc.co.uk/news/technology-14851455; b) http://techcrunch.com/2011/09/09/google-explains-its-google-docs-outage/; c) http://articles.economictimes.indiatimes.com/2011-06-14/news/29657125_1_cloud-availability-zones-aws; d) http://www.cloudtweaks.com/2011/06/should-you-be-concerned-a-list-of-recent-cloud-computing-failures-%E2%80%93-ii/; e) http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-outages-What-can-we-learn; f) http://www.cloudbusinessreview.com/2011/06/30/the-10-worst-cloud-outages-lessons-learned.html; g) http://www.information-age.com/channels/security-and-continuity/news/1294788/data-centre-failure-causes-paypal-outage.thtml;

Risk assessment is an important aspect of cloud computing security. In 2002 the OECD adopted Security Guidelines[71] which include a set of nine key principles to help all stakeholders address computer security in a networked environment, including the principles that 'participants' should (Principles 6 to 9):

- "Conduct risk assessments";
- "Incorporate security as an essential element of information systems and networks";
- "Adopt a comprehensive approach to security management"; and
- "Review and reassess the security of information systems and networks" to fit new threats and vulnerabilities.

These guidelines take a risk-based approach to security and as a key approach recommend a continuous round of assessment and reassessment with all the 'participants' taking on various responsibilities. This approach is also taken by ENISA in its 2009 cloud computing report.[72]

3.2.1 Transparency of provider's provisions concerning data security

Users of cloud computing services, be they businesses or individual consumers, do have a right to expect secure storage of their data, as well as data integrity. However, it seems that many providers of services not only avoid giving any guarantees for data integrity, but actually disclaim liability for it, as a 2010 study comparing and analysing provider contracts demonstrates; a number of these providers specifically state that liability for the preservation and integrity of data lies with the customer.[73] Others guarantee integrity only for additional payment. Consumer representatives agree that there is a case for differentiated levels of security protections, also in terms of costs, according to needs; but they maintain that this should not imply that basic security considerations, such as data integrity, be compromised.

Further, customer control of data in the cloud can be diminished depending on the service model (e.g. a social network, a collaboration tool or a back-up/storage service) and different providers have different standards of security, which can be for the same levels of service offered, including when that service is free.[74] Often clear information about security and data protection measures are difficult to find or not available on the sites of the service providers.

---

[71] OECD, *OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*, 2002, p.11, available at http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[72] ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009, p.5 et ff.

[73] Bradshaw, S., Millard, C. & Walden, I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper no. 63, 2010, p.21 et ff.

[74] See for example reviews and ratings on security and privacy of different providers on http://www.kimpl.com/1297/secure-online-backup-file-sync-service/.

To check the clarity, completeness and accessibility of the information given by cloud service providers on different aspects of data security and privacy, we conducted a website check of 15 public cloud services for consumers and businesses in the framework of this study. We found significant differences in how detailed and clear the information provided on these websites was. On several occasions, our researchers could not find essential information regarding aspects such as the physical security of data centres, the location of data and notification in cases of disclosure of information. Nonetheless, information on security and privacy was generally better supplied for business-oriented cloud services than for consumer-oriented ones. The detailed results of our website check are presented in the following box and table (for information on the scope and methodology of the assessment, refer to Annex 3):

Box 7: Results of website check of consumer and business cloud services

Consumer-oriented cloud services: First, our website check shows that it is not always easy to obtain information on security for consumer-oriented cloud services; and in two cases information may be almost entirely absent. However, for those which had security information, information on the security of data at rest on cloud providers' servers was almost always provided, but exact details on the nature of such security (e.g. whether data is encrypted) was sometimes lacking. Security in the area of identification, authentication and permissions was more often than not alluded to in some form, with the exception of one cloud storage service. Information concerning the security of data transfers between the user and the cloud provider was found to be less clear, especially concerning the level of SSL (Secure Sockets Layer) encryption, and the fact that such security may differ according to the type of data transmitted for one provider. Concerning the physical security of data centres and the redundancy level of data, information was totally absent for three providers, but sufficiently clear and complete for the other providers under study. Information regarding network security was rarely present and sometimes incomplete, while some form of certification arising from external auditing was only clearly mentioned when such auditing had indeed taken place.
Second, information on privacy policies for consumer-oriented cloud services was similarly difficult to access for almost half of the providers, in particular because multi-product providers often referred users to their general privacy policy rather than a distinct privacy policy for their consumer cloud offering. Information regarding the type and use of collected personal information, its encryption, and its conditions for disclosure, was almost always clearly outlined. Information was less clear, however, regarding the location of personal data, its deletion or retention, and whether the user would be informed of personal data disclosure to third parties or of changes to the provider's privacy policy. One provider was nonetheless clear on all of these points.
Finally, for the additional criteria analysed, little information was provided. Some providers highlighted disaster recovery programs; only one provider clearly indicated that consumers would be able to port their data to other services were they to terminate their account; and there were only three providers for which information could be found regarding their membership to a consumer privacy dispute resolution entity.

Business-oriented cloud services: Business-oriented cloud services provided much better information regarding security. Information was easy enough to obtain, even if a whitepaper often needed to be downloaded to acquire all relevant information; it was in any case far more complete than information on security for consumer-oriented cloud services. With the exception of one provider, almost all providers had sufficiently clear and complete information on security of storage and transmitted data, authentication security, physical and network security, data centre redundancy, and certification.
Next, information on privacy policies was also in general easy to obtain. Information was broadly clear and complete regarding the type and use of collected personal information, whether it was encrypted, the conditions for its disclosure to third parties, data retention and deletion, and notification in the event changes were made to the privacy policy. Information was however less clear regarding the location of data, as well as whether the user is notified of the disclosure of data. One provider was nonetheless clear on both of these points.
As for the additional criteria assessed, most providers had a disaster recovery program in the event of data breaches or data centre failures; two providers clearly highlighted the portability of the data they are entrusted with and hence interoperability with other providers; and three others pledged to refer users to ADR mechanisms if complaints relating to privacy remained unresolved.

For more detailed results of the website check, refer to the tables on the following pages.

Table 8: Provision of information on security conditions and privacy policies regarding cloud services for consumers

	Storage and content sharing cloud services				Other consumer cloud services				
	Provider 1	Provider 2	Provider 3	Provider 4	Provider 5	Provider 6	Provider 7	Provider 8	Provider 9
Security									
Ease of obtaining information regarding security	Easy	Not easy	Easy	Not easy	Not easy	Easy	Not easy	n.a.	n.a.
Security of storage data/data at rest (e.g. 128-bit AES encryption)	Clear	Not clear	Clear	Not clear	Clear	Clear	Clear	n.a.	n.a.
Identification and application security (e.g. "multi-factor authentication", permissions restrictions)	Not found	Not found	Clear	Not found	Clear	Clear	Clear	n.a.	n.a.
Security of data transfers (e.g. SSL encryption)	Clear	Not found	Clear	Not found	Clear	Clear	Not clear	n.a.	n.a
Physical security of data centres and redundancy level (i.e. how much is data backed-up?)	Clear	Not found	Clear	Not found	Not found	Clear	Not clear	n.a.	n.a
Network security (e.g. firewalls, DDoS mitigation)	Clear	Not found	Not found	Not found	Not found	Not clear	Not found	n.a.	n.a
Certification or auditing (e.g. SAS70, ISO 27001)	Clear	Not found	Not found	Not found	Not found	Clear	Not found	n.a.	n.a
Privacy									
Ease of obtaining information regarding privacy	Easy	Not easy	Easy	Not easy	Not easy	Easy	Easy	Easy	Easy
Type and use of collected information	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear
Encryption of personal information (e.g. credit card number, passwords)	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Not clear
Location of data	Clear	Not found	Not found	Clear	Not found	Clear	Clear	Not clear	Not found
Conditions for disclosure of personal information (e.g. for law enforcement)	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear
Notification if data disclosed	Not found	Clear	Not found	Not found	Not found	Clear	Not found	Not found	Not found
Data retention and deletion	Clear	Clear	Clear	Not found	Clear	Clear	Not found	Not found	Clear
Changes to privacy policy	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear	Clear
Additional information									
Procedure for dealing with problems (e.g. service failure, data breach)	Not found	Not found	Not found	Not found	Not found	Yes	Yes	Not found	Not found
Interoperability/portability of data	Not found	Not found	Not found	Not found	Not found	Yes	Not found	Not found	Not found
Member of consumer privacy dispute resolution entity	Not found	Not found	Yes	Yes	Yes	Not found	Not found	Not found	Not found

Source: Research conducted by Civic Consulting in December 2011 on the websites of 9 consumer-oriented cloud providers. For providers 8 and 9, the 'n.a.' grading was attributed for all assessments of security information, since their services are online applications that do not allow consumers to upload data.

Table 9: Provision of information on security conditions and privacy policies regarding cloud services for businesses

	Collaboration cloud services				Other business cloud services	
	Provider 1	Provider 2	Provider 3	Provider 4	Provider 5	Provider 6
Security						
Ease of obtaining information regarding security	Easy	Easy	Easy	Easy	Easy	Easy
Security of storage data/data at rest (e.g. 128-bit AES encryption)	Not found	Clear	Clear	Clear	Not found	Clear
Identification and application security (e.g. "multi-factor authentication", permissions restrictions)	Not found	Clear	Clear	Clear	Clear	Clear
Security of data transfers (e.g. SSL encryption)	Clear	Clear	Clear	Clear	Clear	Clear
Physical security of data centres and redundancy level (i.e. how much is data backed-up?)	Clear	Clear	Clear	Clear	Clear	Clear
Network security (e.g. firewalls, DDoS mitigation)	Clear	Clear	Clear	Clear	Clear	Clear
Certification or auditing (e.g. SAS70, ISO 27001)	Not found	Clear	Clear	Clear	Clear	Clear
Privacy						
Ease of obtaining information regarding privacy	Easy	Easy	Easy	Easy	Easy	Not easy
Type and use of collected information	Clear	Clear	Clear	Clear	Clear	Clear
Encryption of personal information (e.g. credit card number, passwords)	Clear	Clear	Not found	Clear	Clear	Clear
Location of data	Not clear	Clear	Clear	Not clear	Not found	Not found
Conditions for disclosure of information (e.g. for law enforcement)	Not clear	Clear	Clear	Clear	Clear	Clear
Notification if data disclosed	Not found	Not found	Clear	Not clear	Not found	Clear
Data retention and deletion	Clear	Clear	Clear	Clear	Not found	Clear
Changes to privacy policy	Clear	Clear	Clear	Clear	Clear	Clear
Additional information						
Procedure for dealing with problems (e.g. service failure, data breach)	Yes	Yes	Yes	Yes	Yes	Not found
Interoperability/portability of data	Not found	Yes	Yes	Not found	Not found	Not found
Member of consumer privacy dispute resolution entity	Yes	Not found	Not found	Yes	Yes	Not found

Source: Research conducted by Civic Consulting in December 2011 on the websites of 6 business-oriented cloud providers.

Our website check indicates that a lot could be done by cloud service providers to improve the information concerning security and privacy given on their websites. However, even if essential information in this respect is available and easy to find on the websites of cloud service providers, it may be difficult for many consumers – and many small business users too – to understand the technical intricacies of the data security offers to make meaningful comparisons, and whether services comply with established standards or legislation. Consumers and business users of cloud computing services also have to make balanced choices between security and other considerations such as privacy generally, efficiency and quality of the service. This is compounded by the fact that trustworthy and independent online reviews or service tests and reports in this area (e.g. by consumer organisations) are still in their infancy.

3.2.2 Approaches to address data security vulnerabilities

Data security vulnerabilities of cloud computing are being addressed in various ways, an obvious way being the differentiation of needed data security level by type of data. The stringency requirements will vary according to the type of data stored and the needs of the users, and so will the related security risks. This was emphasised by a several of our interviewees. One European industry representative explained:

> *"Everyone's interested in the protection of their data. … with enterprises [it] is more emphasis on confidential business secrets, that are important for running the business; with governments it's being entrusted with citizen data; and with citizens maybe there's less of the volume or percentage of data that they feel they need to keep under their immediate control, but with all three categories there's an awful lot of data you don't seek out expensive security protection for."*

The same point is also emphasised by a government official:

> *"People fixate on public administration being about personal data, but there's a huge amount … - probably around 50% - which doesn't contain any data like that. A huge amount of what we do is not affected by security and data protection issues. […] You can't say that the cloud per se is not secure, it just depends on how you use it. [We need] the right sort of security where it's needed and not paying for security where it's not needed."*

A leading cloud provider pointed out that it reflects these differing demands by differentiating the number of 'layers of security' provided:

> *"…For specific services we offer more layers of security. So the answer should not be a single standard, a single level of security for all the services that you provide, but a tailored, layered approach, offering different degrees of security according to the different risk and sensitivities related to the services."*

As an example of how an administration could introduce cloud computing in the public sector while ensuring the right level of security for different types of data, the box below presents the conclusions of a study by the Fraunhofer Institute. The study identified several scenarios for possible uses of cloud computing in the German public sector, two of which are presented below.

Box 8: Two scenarios for use of cloud computing in the public sector in a way that ensures data privacy[75]

Making government agencies more efficient

Data privacy issues could be resolved and administrative processes made more efficient by differentiating between personal and non-personal data, with the example of complaint management. Citizens could first make complaints to a complaint management service provider, running in a private or community cloud, to ensure personal data is protected. Complaint data would then be delivered anonymously to the responsible public authority. This agency does not need to know the identity of the issuer of those complaints to perform its core tasks, meaning it could run its processes in a public cloud infrastructure (e.g. with a private cloud provider).

Simplifying cross-administrative processes

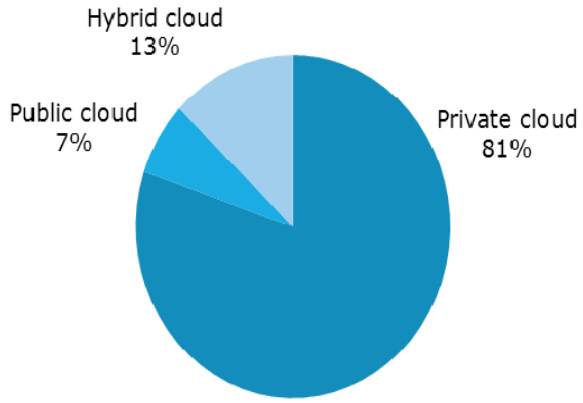
A cloud providing a secure document storage service could simplify the interaction between administrations, businesses, and citizens, optimize governmental processes by delivering documents, and improve cross-administration processes by the electronic exchange of documents. Citizens could own electronic document safes (EDS) to store and manage their documents, in an interoperable format, to which they can choose to grant access to government agencies for administrative procedures or businesses. Citizens would access the document safe using an application providing secure encrypted communication and authentication. The EDS provider could then be organised as a collaboration of several data centres with dedicated resources, using cloud computing to manage these resources (i.e. maintaining a community cloud). As any particular data stored in the EDS is encrypted, the EDS provider would not know what data are stored in a particular EDS.

Another approach to address at least some of the above mentioned potential vulnerabilities of cloud services is, as mentioned before, the use of a 'private cloud', i.e. a cloud that is operated solely for an organisation, be it managed by the organisation itself or a provider. A 2010 survey of 200 French IT managers found that most companies are following a 'private cloud first' strategy: over 75% were prioritising investment in private clouds (see figure below), although SMEs had a preference for 'public cloud' systems - particularly for collaboration tools such as Basecamp and Huddle. Legal and security concerns were the major inhibitor, particularly for adopting public clouds. There was a clear preference for services hosted in France.[76]

[75] Source: Adapted from Fraunhofer Institute For Open Communication Systems, *Cloud Concepts for the Public Sector in Germany – Use Cases*, August 2011.

[76] Pierre Audoin Consultants, *Le Cloud Computing en France: Résultats de l'enquête auprès de 200 décideurs informatiques*, 2010, p.10.

Figure 5: French IT managers' priority for cloud computing investment



Source: Pierre Audoin Consultants, *Le Cloud Computing en France: Résultats de l'enquête auprès de 200 décideurs informatiques*, 2010. Reproduced here with permission. N=200. Sum total does not equal 100% due to rounding.

There are also technical approaches that cloud infrastructure and service providers as well as users can take to improve data security. For example, by encrypting data before it is stored in a cloud data service, a customer can greatly reduce the probability it will be compromised. The US healthcare company TC3 took this approach to store sensitive patient records and healthcare claims in a cloud storage service.[77]

One complementary way of providing data security assurance for consumers, but also for companies is to have some form of audit and certification systems of cloud services providers. This view is promoted by a variety of stakeholders including some of the big cloud providers, who were part of the mentioned meeting hosted by the Consumer Federation of America. The recommendations resulting from this meeting pointed out that: "… it is our consensus view that cloud providers should make their systems available for analysis by outside security experts. This could take the form of expert audit, which would result in the conferral of an industry-recognised certification".[78]

Cloud customers could obtain security assurances from audits, showing provider compliance with relevant ISO and other standards. Gaps between required governance controls and cloud providers' contract offerings can put compliance certification at risk if a cloud provider has not demonstrated compliance or does not permit audit by a customer. As explained by one of the interviewed national government officials:

> *"There are for sure some certifications necessary which are brought by the cloud vendor even if you are running it in the private cloud environment. Some things need to be proven, but also to be checked and evaluated against criteria, a catalogue, to give you back this objective feeling of security and privacy."*

[77] Armbrust, M., et al., *Above the Clouds: A Berkeley View of Cloud Computing*, 2009, p.15.
[78] Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010, p.18.

A general observation was made by one of the European officials whom we spoke to, who pointed out that governments can use their vast purchasing power across Europe to drive higher security standards:

> *"The public sector has a big punch when it comes to public IT procurement and it could also drive the market in certain ways, or shape the offer, make sure that providers comply with certain security requirements, or transparency requirements etc., and if the public sector gets its act together it will have a big impact ..."*

3.2.3 Privacy - the legal issues

Privacy and data protection issues are not cloud computing specific, but pose challenges generally in the online environment, particularly in cross-border situations and internationally. However, there are some specific issues related to privacy in the cloud computing model that pose particular challenges, and privacy is a very determining factor in the development of cloud computing technologies. A speaker at the 2011 Digital Agenda Assembly pointed to the fact that data risk is seen as an obstacle to uptake by 90% of cloud suppliers, and that the EU should build on the Data Protection Directive (Directive 95/46/EC) as a competitive advantage in cloud markets.[79] There was less certainty on this point amongst those who responded to last year's EU public consultation on cloud computing, with opinions reported as divided on whether updates to the Data Protection Directive, would "facilitate cloud computing while preserving privacy", although there were more positive than negative answers both for individuals and companies.[80]

Ambiguities and uncertainties regarding the application in practice of the current Data Protection Directive to cloud computing services were outlined by the European Data Protection Supervisor in a statement at the European Parliament. In his view, five relevant challenges need resolving, namely:

- Ambiguities regarding the role of the cloud service provider;
- When the EU law applies and when it doesn't;
- Ensuring more effective data protection;
- International data transfers; and
- Processing individual/consumer data for purely personal purposes.[81]

Regarding the *role of the cloud service provider* under current EU legislation, the Supervisor's conclusion is that the role will need to be determined on a case by case basis, as providers can be both data processors and data controllers and therefore specific guidance is needed for this purpose. This is important, because the Data Protection Directive puts most of its obligations on data controllers, whereas fewer obligations are imposed on data processors, i.e. entities that are 'entrusted' by the controllers to process data.[82]

---

[79] Pilar del Castillo Vera MEP in Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011, p.3.

[80] European Commission, DG Information Society and Media, *Cloud Computing: Public Consultation Report*, 2011, p. 3.

[81] Hustinx, P., *Data Protection and Cloud Computing under EU law*, Third European Cyber Security Awareness Day, BSA, European Parliament 2010.

[82] Ibid., p.2.

In terms of the *applicability of the law*, there is a clear gap when both the provider and its equipment (data centres, servers, etc.) are located outside the EU but the service is used by EU citizens, as is the case for example with EU citizens using the collaboration services of Box.com or Basecamp. In this case, a cloud provider would "not be caught by EU law", as the Supervisor pointed out.[83] The remedy would have to be to extend the applicability of the law to such a situation, though enforcement and redress may be an issue.

The challenge of *ensuring more effective data protection* in practice applies to all data processors and controllers (and the whole of the Internet). For this reason it has been proposed to include the principles of 'accountability' and 'privacy by design'[84] in the EU legal framework for data protection. According to the Supervisor, in "the context of cloud computing services, this means that controllers and processors would have to *demonstrate* that they have taken all the necessary measures to ensure that data protection rules and principles are complied with. This approach would also be very interesting where personal data are entrusted to providers in third countries."[85]

A related challenge is *international data transfer.* The Supervisor pointed out that the Data Protection Directive "prohibits transfers of personal data to countries which do not ensure an adequate level of protection. Unless an exception applies, the data controller must adduce adequate safeguards for the protection of personal data: for example, enter into a contract with the recipient of the data ensuring that the data will remain adequately protected. The problem is that these rules rely on a definition of data transfer from 'point to point'. They require having a contract, and sometimes a notification to the authority for each transfer to a country where the legal framework is not adequate." The Supervisor concluded that in practice, "this is very difficult to implement, particularly in cloud computing that entails the continuous transfer of personal data".[86]

There is support from the industry for a principle-based approach to address these challenges, as stated to us by a large technology company:

> *"The development of cloud computing infrastructure and services should follow the principles of 'privacy by design' and 'accountability', where privacy requirements are taken into account early on and throughout the development lifecycle and where entities take responsibility for the information they collect no matter where it resides."*

[83] To put it precisely, and in the words of the European Data Protection Supervisor: "A cloud provider established in the EU - or acting as processor for a controller established in the EU - will in principle be 'caught' by EU law. A cloud provider which uses equipment (such as servers) in an EU Member State - or acting as processor for a controller using such equipment - will also be caught. A cloud provider in other cases - even if it mainly and mostly targets European citizens - would not be caught by EU law.", ibid. p.3.

[84] 'Privacy by design' means that "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal", see European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A Digital Agenda For Europe, COM(2010) 245 final/2*, 2010.

[85] Ibid, p.5.

[86] Ibid, p.4.

Finally, and importantly, consumers who are increasingly using cloud services to manage their *personal information for private purposes* – such as storing calendars, pictures, family documents – may not be covered by the current EU data protection framework. This is because Article 3 excludes from the scope of application of the Directive data processing carried out "by natural persons in the course of a purely personal or household activity" (the so called 'household exception'). The Supervisor argues that if "the information uploaded to the cloud is not covered by the Directive because it is information of a personal nature, then the processing activities that are carried out on behalf of the individuals involved might not be covered either. Obviously, many cloud providing services, even when they cater to end users, will be covered by the existing EU data protection legal framework. However, in other situations, the legal framework may not apply." This is a gap in the current legislation that would need to be filled, for example through explicitly requiring that "services provided to individuals acting in a purely personal capacity are bound by the same requirements as 'regular data processors'".[87]

On 25 January 2012, the European Commission published a proposal for a comprehensive reform of the data protection rules. It was not the mandate of this study to assess the extent to which the proposed reform would address the gaps mentioned above that are relevant in the context of cloud computing. However, the Commission emphasised that by having "future-proof, technologically neutral regulations", the proposals "will give long-lasting certainty to data protection issues online".[88] The reform provides for "increased responsibility and accountability for those processing personal data" and safeguards that "EU rules … apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens", according to the Commission.[89]

3.2.4 Access to data by law enforcement authorities

Particular concerns have been voiced regarding the possibility of disclosure of personal and confidential information by cloud providers when compelled by law enforcement authorities to do so, without a warrant (as law enforcers would be obliged to do when seizing personal property on owner's premises, e.g. a computer), and without informing the data owners. The US Patriot Act is often cited in this context, as it enables surveillance of data stores across international borders, e.g. data stored in the EU by companies with headquarters in the US based on US legislation.[90]

An analysis by a Brussels-based legal firm puts the situation into a more balanced context, however, by explaining that although the US Patriot Act's provisions are a reality, the EU Data Protection Directive exempts Member States from privacy protections when e.g. public security or economic well-being of the State are at stake, and so in many EU countries cloud services providers may be obliged by law to disclose personal data they hold without the data owner or the data subject being made aware.[91]

---

87 Ibid, p.6.

88 http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf.

89 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/868&format=HTML&aged=0&language=EN&guiLanguage=en.

90 See e.g. http://arstechnica.com/tech-policy/news/2011/12/patriot-act-and-privacy-laws-take-a-bite-out-of-us-cloud-business.ars .

91 Linklaters, Van Overstraeten, T. & Bruyndonckx, B., *Law Enforcement and Cloud Computing*, 2011.

A similar argument was made by the representative of a large cloud provider, who remarked to us:

> *"The problem in our opinion should not be focused only on the Patriot Act, but on the due process of law and jurisdictional issues in the cloud environment, which you know are the same issues that you may have for an Italian or UK service provider in relation to the application of local laws to a service or its cloud and the possibility that the server data on the cloud is only US citizen data. So I think the focus here should be on due process of law when it's about access to user data."*

There is also the question of how easy it actually is for the surveillance authorities to access databases cross-border, with one of our interviewees, a European official, emphasising that it is "much more complicated" before data can be obtained under the US Patriot Act. Nevertheless, for public authorities in the EU, applicable legislation from countries outside the EU remains of potential concern when contemplating outsourcing to public clouds, because the majority of the big companies providing the services are operating under US jurisdiction, as another European official pointed out:

> *"[Third-country legislation such as the US Patriot Act] is why most public services do not want to have to use a public cloud infrastructure. They might develop their own private cloud, so having control of the infrastructure, having the control of the data centres, but using for example Amazon services or Gmail for instance, most public authorities are totally opposed to that, because the risks are far too high. […] So this is a risk and I would say at the same time it can also be exploited as an opportunity to see the creation of European clouds, which are under European jurisdictions."*

Law-abiding consumers or business users storing their data in the cloud may well be affected by compulsory orders for disclosure - for example in a public or shared cloud authorities may seize the servers or computers containing personal information of the guilty and innocent alike.[92] And consumers may not even realise that they have data stored in clouds, for example if they use smart phones. As shown by the already mentioned study of cloud provider contracts, providers have different 'thresholds' of disclosure and may accept wider requests for information from law enforcement agencies "at their sole discretion", such as connected to intellectual property infringement or illegal content; or state that the customer has all responsibility for keeping information confidential, for example through encryption.[93]

One way to ensure better consumer protection regarding data disclosure is for providers, whenever possible, to notify consumers when a law enforcement or civil request has been made for their information as well as provide consumers with privacy-enhancing technologies, such as encryption.[94]

---

[92] Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010, p.10. A good example of this is the cloud storage file-sharing service Megaupload, which was forced to shut down by the US Justice Department on 19 January 2012 under the PRO-IP Act of 2008, for allegedly operating as an organization dedicated to copyright infringement. In addition to storing illegal material, Megaupload was also used legitimately by many thousands of people worldwide. See http://www.smh.com.au/it-pro/cloud/megaupload-closure-hits-legitimate-cloud-users-20120123-1qcum.html for further information.

[93] Bradshaw, S., Millard, C. & Walden, I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper no. 63, 2010, pp.22, 27.

[94] Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010, p.15.

4 CHALLENGES RELATED TO ACHIEVING A DIGITAL SINGLE MARKET

KEY FINDINGS

- Fragmentation of the digital single market along geographical borders due to differing legal frameworks may restrict or slow down the development of EU-wide cloud-computing based services, for example those dependent on intellectual property rights (music, films).
- Rights and responsibilities in the cloud are not yet clear due to lack of transparency or difficulties in finding information, problems with contracts, the complexities of many jurisdictions or the fact that for each legal issue - data protection, contracts, consumer protection or criminal law - the jurisdiction may differ. There also gaps in the relevant legislation when applied to cloud computing.
- Cloud providers' contracts often disclaim liability, contain inappropriate or illegal clauses and lack certain key pieces of information such as the location of data centres. In particular, service contracts offered to SMEs are rigid, with little room for negotiation. A majority of interviewed stakeholders agree there is a need for standardised contracts, with specific requirements regarding safety, security and reliability.
- Standardisation efforts for cloud services are proliferating. However, even if consumers would greatly benefit from interoperable cloud services, support for interoperable standards from industry is mixed, with some industry players fearing that early standardisation could stifle innovation.

The Digital Agenda, part of the Europe 2020 strategy, has a vibrant digital single market as one of its key goals, and identifies the barriers that have to be brought down to achieve this. These barriers include the fact that many large Internet businesses originate from outside Europe, and that there is still considerable uncertainty regarding legal rights and responsibilities across the market.[95] Such observations could also apply to the cloud computing model. The Digital Agenda mentions cloud computing specifically only in the context of public authorities' collaboration and scientific innovation.[96]

However, given its cross-cutting character, which throws into perspective many more general online issues, and the potential to assist in the development of Europe's SME sector, cloud computing has gradually come up the political agenda and a related strategy is due in summer 2012 following research and a public consultation on the part of the Commission. The risks outlined above are not inherent to the 'cloud', they are mostly issues for the online environment generally, but the nature of the networked technology puts them into sharper relief, and makes the need for resolutions more imperative. In our interviews, this point of view was communicated in different ways, by officials, consumer rights groups and industry alike.

[95] European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A Digital Agenda For Europe, COM(2010) 245 final/2*, 2010, p.7.

[96] Ibid, pp. 23, 24.

4.1 Market fragmentation, jurisdictional uncertainties and legislative gaps

4.1.1 Internal market fragmentation

Cloud computing has a market scope that goes beyond geographical national borders. However, the EU digital single market still remains fragmented due to legal regimes that differ across Member States.

For example, in the domain of digital content, only a limited level of harmonisation has occurred following the Copyright Directive,[97] and there is therefore a particular concern for cloud services that depend on a uniform intellectual property rights (IPR) regime to cross borders. In addition, Member States lack a harmonised method of copyright management. But, as most of our interviewees pointed out, this is not an issue specific to cloud services, as all online services that allow e.g. the streaming of music and video content – such as YouTube or the cloud-based service Spotify – are affected by this fragmentation: due to differing IPR regimes, content can often be blocked in different Member States. As explained in a Commission Communication of 2010, "to set-up a pan-European service an online music store would have to negotiate with numerous rights management societies based in 27 countries. Consumers can buy CDs in every shop but are often unable to buy music from online platforms across the EU because rights are licenced on a national basis."[98] One European official noted that a cloud computing environment may nonetheless make enforcement of IPR more difficult, since it is harder to know where data is stored. To tackle barriers to cross-border online licensing rights and improve the governance and transparency of the functioning of collecting societies, the proposal for a Directive on Collective Rights Management is planned for adoption in the first quarter of 2012, among other measures.[99]

Another source of fragmentation of the internal market relevant for cloud computing is Europe's telecommunications markets and their fragmented network regulation. As noted in the above Communication, "Europe's telecom markets are partitioned on a Member State basis, with purely national, rather than Europe-wide, numbering, licensing and spectrum assignment schemes." Member States each comprise several internet service providers (ISPs) operating essentially at the national level, and clouds are still dependent on ISPs to reach their customers. As a study by Tilburg University points out,[100] these ISPs are bound to different jurisdictions across Europe, with different access regimes and different transparency regulations to disclose network management. As such, a cloud provider would have to oversee potentially 100 ISPs to ensure that its service is ubiquitous throughout the

[97] Directive 2001/29/EC. See http://kluwercopyrightblog.com/2011/12/21/the-infosoc-directive-ten-years-after/ for more information on the effects of the Copyright Directive. The main problem would appear to be a lack of a harmonised set of mandatory exceptions and limitations to the exclusive rights of authors. As shown in DLA PIPER, *EU study on the Legal analysis of a Single Market for the Information Society: New rules for a new age?*, 2009, "As a result, Member States can decide if and how to implement the exceptions and limitations. The list of exceptions also exhibits many ambiguities and leaves ample discretionary room to Member States. Consequently, the exceptions and limitations have become a cluttered chaos on the Member States level."

[98] European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A Digital Agenda For Europe*, *COM(2010) 245 final/2,* 2010

[99] See European Commission, *Digital Agenda for Europe*, Annual Progress Report, 2011.

[100] Sluijs, J. P., Larouche, P. & Sauter, W., *Cloud Computing in the EU Policy Sphere*, TILEC Discussion Paper No. 2011-036, 2011. Available at SSRN: http://ssrn.com/abstract=1909877.

EU. And if these ISPs decide to embark on differentiation strategies, then a cloud provider "could be left with a patchwork of different ISP platforms to contend with",[101] involving large transaction costs to adapt to varying network management practices and regulations. These platforms could also offer different levels of quality of service, making it impossible for cloud providers to be ubiquitous in the same way across Europe (in terms of processing power and computational speed), leaving consumers and businesses located in different Member States with uneven access to cloud services.[102] To attempt to solve this issue, the 2009 electronic communications framework has tried to improve coordination of national regulators, including through BEREC, the Body of European Regulators for Electronic Communications.

4.1.2 Jurisdictional uncertainties and related market fragmentation

The striking result of the recent public consultation on cloud computing is that there is general confusion – including among companies, as well as administrations, and individuals – regarding rights and responsibilities in cross-border cloud computing situations; and similarly there is a general lack of certainty in the legal framework, with a vast majority of respondents agreeing that liability in cross-border situations was unclear.[103] Related to the latter result, one of the interviewed European officials remarked:

> *"Pertaining to the liability question, the legal regime was unclear according to our public questionnaire in 90% of cases. Basically all people say it is an issue. If I were a policymaker, this figure would shock me. It´s not only the suppliers who say this: the users say it, the consumers say it, all groups say they don't know what to apply."*

Reasons quoted by respondents include lack of transparency or difficulties in finding the information, problems with contracts (see Section 5.2. below) and the complexities of many jurisdictions or of the fact that for each legal issue - data protection, contracts, consumer protection or criminal law - the jurisdiction may differ.[104]

Of perhaps even greater concern is that a little less than half of the companies responding to the consultation did not know which jurisdiction applied to their own operation;[105] one of the reasons highlighted was the burden of understanding and complying with multiple laws and regulations. And it is not just about the multiplicity of EU laws (and differences in their national implementation), since as explained in the sections above, data can travel and be stored anywhere round the world, including in several places at once.

[101] Ibid.
[102] But it must be emphasised that this would only be particularly important cloud services that require very high bandwidth/quality connections (e.g. HD video streaming).
[103] European Commission, DG Information Society and Media, *Cloud Computing: Public Consultation Report*, 2011, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf.
[104] Ibid, p.2.
[105] Ibid.

These uncertainties can lead to both 'jurisdiction shopping' by users to find providers that offer better protections in areas that they are interested in, or providers using stronger protections in certain areas as a marketing advantage.[106] More importantly, these uncertainties are continuing to fragment the public cloud computing market along national borders in what is essentially a borderless networked medium; geography is still a strong factor. This seems to be particularly the case with public administrations, but also small and medium businesses share similar concerns regarding the physical location of their information under a foreign jurisdiction, particularly in sectors such as high-tech, health and bio-technology; these concerns apply even within the EU, due to differing interpretations of the EU law.[107]

As a result of this jurisdictional confusion and fragmentation of the internal market, there are increasing calls for further harmonisation of laws across the Member States. From the interviews conducted for this study it appears that this is one area where there is a convergence of views from consumer groups, industry and administrations, and not just for data protection laws.

Finally, and equally important, the discussion of effective solutions needs to cover not just the EU, but the wider global environment, and particularly for 'public cloud' services which all the individual consumers and the majority of SMEs use. Currently this includes primarily transfers of data between the EU and the US, which is governed by the so-called Safe Harbor Framework.[108]

[106] See e.g. Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011 p.6: Robert Jenkins of CloudSigma stated that his company has found that the EU infrastructure, reliability, and data protection regime are assets in selling cloud services to customers in Latin America.

[107] European Commission, *Hearing with SMEs, meeting note*, 2011; see http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7734&utm_campaign=isp&utm_medium=rss&utm_source=newsroom&utm_content=tpa-261/.

[108] To provide a means for US organisations to comply with the EU Data Protection Directive, the US Department of Commerce in consultation with the European Commission developed a "safe harbour" framework, which was approved by the EU through Commission Decision 2000/520/EC. It is a way for US organisations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU Member State authorities under privacy laws. Self-certifying to the US-EU Safe Harbor Framework ensures that EU organisations know that US organisations provide "adequate" privacy protection, as defined by the Directive, see Commission Decision 2000/520/EC and http://export.gov/safeharbor/eu/eg_main_018476.asp.

4.1.3 Gaps in applicable laws

As well as the obstacles to cross-border provision of cloud services and uncertainties regarding legal rights and obligations due to the fragmentation both globally and within the EU single market, the several pieces of EU legislation that do apply, also have been identified to have gaps and other weaknesses in their application to cloud computing, due to its specific features. The most relevant pieces of legislation, and related gaps, are outlined below:[109]

- Data Protection Directive,[110] and the related individual Member States' laws regarding access to data stored in the cloud (relevant for all stakeholders). Gaps are covered comprehensively in section 4.2.3 above;
- E-Privacy Directive (relevant for all stakeholders).[111] Gaps include: data breach notification requirements do not apply to cloud services providers (only 'Communication services providers', i.e. ISPs and mobile networks); the obligations for communications secrecy may not be possible to meet in a cloud environment;
- Unfair Commercial Practices Directive (business to consumer practices only).[112] Gaps and weaknesses in terms of consumer protection include: additional differing rules at national levels (e.g. re information provision or language); diverging requirements for different sectors to which the cloud service applies (e.g. health care, financial services, etc.). In addition, as the Rand study points out[113], "it remains to be seen whether the use of behavioural advertising as a key element of 'free' cloud services should fall in the framework of the Unfair Commercial Practices Directive in countering misleading or aggressive advertising";
- Unfair Contract Terms Directive (consumer contracts only).[114] See Section 5.2 below;
- E-Commerce Directive (relevant for all stakeholders).[115] This law may not work where the information society service provider (e.g. the trader) uses a cloud service whose location is difficult to determine; transparency rules in the Directive may be difficult to enforce in a cloud service situation; applicable law linked to physical location. See also section 6.2 below;
- Data Retention Directive.[116] Its rules specifying periods of retention for personal data for law enforcement purposes, may not apply to cloud-based service providers.

[109] Source: Robinson, N. et al., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Rand Europe, time.lex, University of Warwick, 2011., pp. 87-90.
[110] Directive 95/46/EC. On 25 January 2012 the Commission published a proposal for a comprehensive reform of the data protection rules, including full harmonisation across the Member States.
[111] Electronic Communications Privacy Directive, as amended by the Citizen's Rights Directive 2009/136/EC.
[112] Directive 2005/29/EC.
[113] Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., Hopkins, P., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Rand Europe, time.lex, University of Warwick, 2011, p. 89.
[114] Directive 93/13/EEC.
[115] Directive 2000/31/EC.
[116] Directive 2006/24/EC.

4.2 Provider contracts

Given all the uncertainties around jurisdiction and legal frameworks described above, contracts are the main tools whereby providers set the terms of their relationship with customers, called Service Level Agreements (SLAs) or End User Agreements (EULAs). Privacy terms and conditions appear separately or incorporated into the others. For consumers and SMEs using public clouds these contracts are 'off-the-shelf' take-it-or-leave-it, often tick-box type agreements, not surprisingly given these clouds' characteristics and economies of scale. Detailed analysis of such contracts broadly supports concerns expressed by stakeholders.[117] The mentioned study of cloud provider contracts examined 31 sets of standard Terms and Conditions of cloud service providers targeting individual consumers and/or business; of these 15 apply US jurisdictions, the rest apply various EU jurisdictions. Contracts asserting US jurisdictions have generally more wide-ranging disclaimers of liability than those which choose to be governed by EU laws. The study found that many contracts are silent on key terms. Some contain clauses that appear to be inappropriate or unenforceable, and in some cases illegal (under EU unfair contract terms legislation); services that may be modified or discontinued without cause and without notice; and often lack of information on the location of the data centres. In terms of redress in case of complaints or disputes, providers may offer arbitration procedures, though in some cases they may even require it, which would be deemed as an unfair term in EU jurisdictions.

For consumers these are one-sided agreements, and in general, as both the study and our interviewees remarked, they are better protected by existing EU consumer protection legislation than small businesses. However, there are issues of understanding and redress. If the contracts are unclear, long and unreadable, and omit key terms, then it is unlikely that consumers would exercise their rights in case of dispute, even if they were able to seek redress in a jurisdiction other than their own. Therefore, consumer representatives point out that there is a need for agreement on what are the key terms and conditions that are important to consumers, as well as pointing to contracts as an area that may benefit from standardisation and increased transparency (see also the results of our website check of cloud providers in Section 4.2.1 above).[118]

[117] Bradshaw, S., Millard, C. & Walden, I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper no. 63, 2010, available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 .

[118] Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010.

Contracts are essential to SMEs, as reported at a recent European Commission hearing with their representatives.[119] They generally lack experience and do not have enough information. They need good sound agreements with undertakings regarding safety, security, reliability etc. But as customers, SMEs are at a disadvantage when dealing with service providers and lack market power. Service contracts offered to them are rigid, with little room for negotiation. They point out that many SME owners have a limited IT knowledge, are wary of the loss of control and potential data security issues and do not have the time or skills to investigate or implement thoroughly. They need also mechanisms for redress. As one of the interviewed European officials explained:

> *"If you think of a small furniture shop in the middle of France, or in Bulgaria, they have no understanding at all. They might just think, 'oh, I get very cheap instant web access and visibility if I sign up with them', then they might realise they went into something quite dangerous …, not reading the information, and so. […] I'm thinking primarily [of] SMEs, but … that [is even true] for big companies. Because at the moment [some very large cloud providers] are so strong that they just impose their own rules, and we have to re-balance that."*

The situation may be different for public authorities (as well as large companies), who usually opt for private clouds with tailor-made, but higher-priced contracts, and have more negotiating power concerning terms and conditions. There is some evidence that when, for example, public authorities do want to use public clouds, major cloud vendors with standard contracts are prepared to adapt the rules according to the wishes of their customers. A much quoted example is that of the city of Los Angeles in the US, which only adopted Google email services after the company changed its standard contract. Another example from Europe, though as yet unresolved, is of the Odense Municipality in Denmark which intends to use the Google Apps online office suite within its schools; this would include processing of sensitive data about pupils, such as health and social issues. As a consequence the Municipality sought the opinion of the Danish Data Protection Authority (DPPA), which concluded that this cloud application was not appropriate to process confidential and sensitive data about pupils; detailed reasons quoted included inadequate terms and conditions and inappropriate levels of security.[120] The DDPA is currently awaiting a renewed offer. The authority told us:

> *"We would like to see better data processor contracts. […] we need [the] development of some standard data processor contractual clauses to be used for cloud services. We have useful standard clauses for third-country transfers;[121] we don't have standard contractual clauses for data processors to be used inside EU. We need to see some similar data processing agreement which provides more detail using the good elements already found in the standard clauses for third-country transfer to data processors. For example concerning subcontracting by the processor, which*

[119] European Commission, *Hearing with SMEs, meeting note*, 2011; http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7734&utm_campaign=isp&utm_medium=rss&utm_source=newsroom&utm_content=tpa-261/

[120] Datatilsynet (Danish Data Protection Agency), *Processing of sensitive personal data in a cloud solution*, 2011: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/. A similar case is a recent decision reported from Norway, where public sector organisations will be banned from using Google Apps after the Norwegian data protection authorities ruled that the service did not comply with Norwegian privacy laws because there was insufficient information about where data was being kept. Reportedly, the decision came from a test case in Narvik, where the local council had chosen to use Google Apps for their email. See: http://blogs.ft.com/fttechhub/2012/01/google-faces-norwegian-public-sector-ban/#axzz1kQQVgCYX/.

[121] See 'international data transfer', Section 4.2.3 above.

should only take place with the prior consent of the controller and only in such a way, that the subcontractor is bound by the same rules. Another example is the processor's right to audit the processor and subcontractor on location. We also need to see more transparency from the cloud provider, as to location of data. We need to see possibilities for supervision."

The provision of more standardised, transparent contracts, containing simple and clear clauses, was also the view of the majority of respondents, both individuals and companies, to the Commission cloud computing consultation; 83% feel that guidelines and checklists on model terms for contracts would be useful.[122] Some of the major providers' views are more nuanced, however:

"We are simplifying our contracts. We are trying to make them very clear so as to avoid a situation where no-one is responsible. At the same time we believe there is still room for negotiation and businesses to look into the market and choose the solution that is more in line with their needs and expectations. So again, model contracts in a global environment need to take into consideration a lot of different aspects..."

4.3 Interoperability, standards, and data portability

Many of our interviewees highlighted the risk of the development of concentrated, incompatible cloud services. There are significant returns to scale with cloud infrastructure, and dominant providers have incentives to erect barriers to entry to new competitors. As described before, cloud infrastructure emerged from the existing internal systems of companies such as Amazon, Microsoft and Google, which has led to heterogeneous services and interfaces, reducing interoperability and competition and creating a risk of lock-in for customers.[123] As noted in a presentation by Francisco Garcia Moran, director general of DG Informatics (DIGIT) of the European Commission, "The supply side is not interested [in standards] – too early: players prefer to gain market share", while on "the demand side is hesitant – current solutions could result in lock in situations".[124] One interviewed European official explained the differences between the current situation in the cloud market and the previous introduction of new technologies, such as mobile communication:

"If you were in mobile communications in the 1990s, there was no way you were going to pour billions of investment into the mobile infrastructure, or into the manufacture of portable mobile handsets unless you knew there was going to be a single standard. You certainly weren't going to invest everything only to find that someone else had taken half the market with a de facto standard. All of the incentives for standardisation were on [the investor's] side. In cloud [computing, providers are] trying to monetise infrastructure they've already got. They've got no incentive to standardise at all, quite the contrary. Their incentive is to gain as much of the market as possible, a lock-in. The only way around it is to mobilise users."

[122] European Commission, DG Information Society and Media, *Cloud Computing: Public Consultation Report*, 2011, p.3.

[123] European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010, p.23.

[124] Moran, F. G., *The European Cloud Computing Strategy*, Tutorial at the 5th International Conference on Theory and Practice of Electronic Governance, 2011, p.5.

The European Commission's 2008 Future Internet Communication stated that "the win-win of open interfaces and open standards is that the market can grow for all ... dominant players may try to use proprietary standards to lock consumers into their products or to extract very high royalties from market players";[125] while Pilar del Castillo Vera MEP told a recent conference that interoperability and open specifications are essential to an open and competitive cloud, demanding that "users should be able to access or change cloud services as easily as changing a mobile phone provider".[126]

The recent reform package for data protection rules proposed by the European Commission foresees that citizens will "have a right to obtain a copy of their data from one Internet company and to transmit it to another one without hindrance from the first company", which is also relevant for cloud services.[127] It remains to be seen how the final wording of the related rules will be, but already at this stage it is clear that a right to data portability will need to be complemented by standards-based competition, if cloud services are to fulfil their promise for supporting cost reductions and innovation across the whole EU economy.

One of the interviewed consumer organisation pointed out why standardised interfaces between clouds are important when considering data portability:

> *"… when I upload several hundred gigabytes of data into the cloud and I want to change the cloud, it's pretty hard work to download it all and upload it somewhere else. So the best would be if there was a possibility to transfer the data from one cloud to another very easily. There should be … standardised interfaces between these clouds. So that it's easy to transfer directly."*[128]

While it is clear that interoperability of cloud services would be required to enhance competition, there are, however, differing views on what constitutes interoperability, as one European official explained:

> *"If [a large cloud provider A] creates a cloud platform, it's greatly in its interest that anyone in the world can interface with it, no matter which device you have. They call that interoperability. The question is, [if] you were using a … service [of a company B] which was dependent on a sub-service which was in the … cloud [of provider A] and another [subservice] in another cloud [of a different provider] - how would they interoperate and how could they? In whose interest is it to establish that interoperability? It's in your interest, but not in theirs."*

[125] European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. Communication on future networks and the internet, COM(2008) 594 final*, 2008, p.8.

[126] Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011, p.3.

[127] See http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf.

[128] In addition to ensuring consumers' ability to upload and download data from different clouds, it is also important to ensure that formats remain interoperable.

But there is some support for interoperable solutions in industry. A large cloud provider declared to us it embraced this possibility, because it is "forcing [us] to try and make a great product in order to convince the users to stay with us, not because the user is locked, but because the user is choosing." And a representative of a large technology company emphasised in an interview that "the delivery of open, interoperable solutions that embrace industry standards is essential – both within the cloud solution stack and between providers of cloud services".

Standardisation efforts for clouds are proliferating, with a European official quoting a number of more than 100 different standardisation groups that are trying to produce cloud standards.[129] His conclusion was: "We must wait until either the market sorts it out, or we can come to some more formal standards for public procurement." Several industry representatives we interviewed for this study warned of the imposition of standards too early in cloud development, because "standards should sometimes compete with each other and proprietary solutions to make the most use of innovation" (the view of a large technology company). A representative of a large cloud provider promoted "encouraging standardisation efforts in defining needs, but not pinning specific standards down. Governments need to monitor the market, promote interoperability but also take note of efforts made by companies." The reluctance concerning standardisation efforts was also expressed at the Digital Agenda Assembly, where a European cloud provider pointed out that standards can be a double-edged sword, stifling innovation and leading to a lowest-common denominator approach if introduced too early.[130]

[129] A selection of standardisation efforts are listed, for example, CERN & ESA, *Strategic Plan for a Scientific Cloud Computing,* 2011, p.20.

[130] Robert Jenkins of CloudSigma in Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011, p.6.

5 CLOUD COMPUTING IN THE FUTURE

KEY FINDINGS

- In the short term, it is uncertain whether there will be significant changes in the types of cloud services offered. However, their availability and capacity are likely to continue to increase, as economies of scale drive ever-larger data centres, which will continue to migrate towards sites with cheaper energy.
- While some services are likely to move to the public cloud given the potential cost savings, other services will still remain in a private environment, because there remain many instances where the intelligent use of small scale solutions is as efficient, or even more efficient than large scale ones.
- Issues such as security and privacy could slow down development because if business users or public authorities do not have the confidence or the evidence that public clouds can be trusted, they will not take up the technology. But lack of competition, mainly due to insufficient interoperability, could be one of the biggest hurdles to overcome in cloud computing development.
- An important future challenge will be in identifying the areas where cloud computing development could be coordinated on the European level to avoid duplication and waste. This would mean tackling essential standards issues to achieve interoperability, ensuring effective competition between providers, by addressing for example vertical integration of service providers or enabling better public procurement for cloud services to encourage new market entrants, and coordinate both European and national cloud computing initiatives.
- Connectivity will gain in importance, since the increased usage of cloud services will result in customer dependency on the availability of high-speed broadband, (including wireless 4G mobile networks or other available technologies); upload speeds in particular may become an important factor. Cloud services accessed through mobile devices would be facilitated by EU-wide access to Internet without complicated or costly roaming arrangements.
- Due to jurisdictional problems, in practice European consumers are unlikely to be able to seek redress from cloud services providers in other jurisdictions. Providing adequate means for redress is necessary for the future in the consumer services area, since there is a strong asymmetry of powers between consumers and providers of cloud services.

5.1 Future cloud computing trends

Predicting the future is by definition not a precise science, though at least some of the forecasts made about the likely development of cloud computing are beginning to come true. A majority of technology experts and stakeholders (71%) surveyed by Pew Internet in 2010[131] believe that they will "live mostly in the cloud" in 2020, rather than on a desktop, "working mostly through cyberspace-based applications accessed through networked devices", rather than depending on personal computer applications.

[131] Pew Internet and American Life Project, *The future of cloud computing*, 2010.

Some cloud services are already relatively mature, so there are unlikely to be significant changes in the types of cloud services offered in the short term. However, their availability and capacity are likely to continue to increase dramatically. Economies of scale will drive ever-larger data centres, which will continue to migrate towards sites with cheaper (potentially renewable) energy.[132] Other types of resources (such as music and film) will become more widely available in a pay-per-use or subscription model through the cloud and in many more countries, provided the issues surrounding legal fragmentation mentioned above are dealt with.

An industry participant at the Digital Agenda Assembly summarised the most important development trends as "elasticity (more flexibility), federation (implying more interoperability and portability) and personal clouds (smart devices, services)."[133] Microsoft has forecast ever-greater benefits from cloud scale, and that security and other types of regulatory compliance will further improve with increased attention and development of provider tools and expertise. They also predicted that "cloud services will enable IT groups to focus more on innovation while leaving non-differentiating activities to reliable and cost-effective providers."[134] Over the long term the IT sector could also see a growth in jobs as well as a shift in the skills required and nature of jobs from technical tasks to more administrative tasks, in terms of negotiating contracts and dealing with customer inquiries.[135]

A representative of a large technology company told us they expect that better cloud federation will allow data to move easily and securely within and across clouds. They predict the greater automation arising from technological innovation will allow cloud services to be specified, located and provisioned with minimal human interaction, allowing greater data centre optimisation for maximum utilisation and power efficiency. They share most providers' views that services will seamlessly adapt to end-users' devices - whether smartphones, tablets, laptops, or larger desktop computers. These devices can be made cheaper and less complex by moving some of their storage and computing resources into the cloud, as can already be seen in Google's new Chromebook laptop which is essentially the eponymous browser from which you access the various applications, such as word-processing or photo storage or editing, etc. It does depend on Internet connectivity (see also below), with limited capabilities offline.

However, while some expect most services to move to the public cloud given the potential cost savings, others emphasise that specific services will still remain in private environments, as mentioned in Section 4.2.4, because – taking electricity as an example – although big power plants are often a more efficient way to produce energy, this is not always the case and there are many instances where the intelligent use of small scale solutions is as efficient, or even more efficient than large scale ones.

---

[132] Google has filed for a 'water-based data centre' patent, see http://bits.blogs.nytimes.com/2008/09/07/googles-search-goes-out-to-sea/.

[133] Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011, presentation of Moisés Navarro Marín, Director of Cloud Strategy and Services at Telefónica, p.5.

[134] Microsoft, Harms, R. & Yamartino, M., *The Economics of the Cloud*, Microsoft whitepaper, 2010.

[135] The impact of cloud computing on employment in the IT sector is uncertain and beyond the scope of this study, but for more details see Wyld, D. C., T*he Cloudy Future of Government IT: Cloud Computing and the Public Sector around the world*, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, 2010, p. 12; and Euractiv.com, *Cloud Computing: Good or bad for IT jobs?, 2011* http://www.euractiv.com/specialreport-cloud-computing/cloud-good-bad-jobs-news-509132; and LSE, Castro, D, Grous, A & Karrberg, P, *Modelling the Cloud - Employment effects in two exemplary sectors in The United States, the United Kingdom, Germany and Italy,* January 2012.

Tim O'Reilly, who coined the term "Web 2.0", suggested that: "the future belongs to services that respond in real time to information provided either by their users or by nonhuman sensors." He thinks that the cloud is the natural home of these services, due to their requirements for high availability and the combination of data from multiple sources.[136] In any case, the availability of cheap computing power and storage through the cloud is expected to enable all kinds of new services, at the consumer level and beyond (see Section 6.3.2 below).

5.2 Future hurdles to overcome

Current challenges and barriers to the take up of cloud computing model described in Section 5 will continue to persist until tackled by both industry practices and appropriate policies. As mentioned previously, issues such as security and privacy may not be showstoppers, but they could slow down development because if business users or public authorities do not have the confidence or the evidence that public clouds can be trusted, they will not take up the technology.

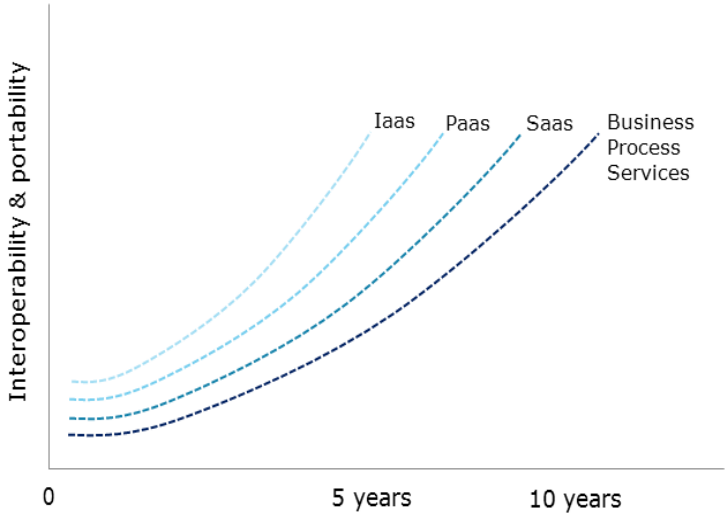
The most important and cloud-specific of all the predicted future barriers to development is the lack of interoperability with the resulting impacts on competition, already described in some detail in Section 5. There it was concluded that the development of standards is essential in this respect. A lack of standards is mainly a significant problem in the provision of platforms as a service (PaaS, see page 16), as here the application programming interfaces (APIs) are usually proprietary, or particular to each service.[137] This means that organisations can get locked into a particular service provider, and also become vulnerable to price increases. In this context, agreement by providers to rely on open standards is one of the important future solutions.

The figure below illustrates how quickly the different infrastructure, platform, software and business process cloud sectors are expected to develop when interoperability and portability are increasing.

[136] The Economist, *Let it rise: A special report on corporate IT*, 2008, p.8.

[137] European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010.

Figure 6: ICT Capability Evolution



Source: Macleod, A., *Update on G-Cloud, Application Store for Government and Data Centre Consolidation,* Cabinet Office presentation; 2011 [138]

5.2.1 Member State cooperation on cloud computing initiatives

As shown in Section 2.2, there has been little take-up so far of cloud computing by public administrations in the EU as its potential is still under investigation; if adoption increases however, an important future challenge will be in identifying the areas where cloud computing development could be coordinated on the European level to avoid duplication and waste.

In this respect, interoperability will be significantly important if EU countries are to work together on cloud projects, as one European official emphasised:

> *"If Member States want to start sharing resources, so even hardware, they must have clear, common specifications, common infrastructure, because otherwise they will never be able to start sharing resources. […] There are discussions to create data centres in the Nordic countries, because you save a lot of energy by not having to cool it so much. And so yes, it's important at EU [level] that we work and avoid some of the mistakes we made in the [past] which led to a terrible frustration about the lack of interoperability..."*

One model of cloud computing that may be particularly relevant for the EU is 'federated clouds' - the practice of managing consistency and access controls when two or more independent geographically distributed clouds share either authentication, files, computing resources, command and control, or access to storage resources. It may have particular importance in assuring interoperability between different national cloud services between different Member States.

[138] Available at http://api.ning.com/files/ubaK*nRPy2S2IUEMYr6Fd9y42NuIKybSVRtwZNhSSavbhqjtrksXTz8NzabjjybVkHmxgoj69369a9IDPyYMeAGykgyXljNs/UIMPpresprescopy.pdf

As well as such standards related interoperability/competition issues, it will be important to consider how existing EU policies can be applied to the specific characteristics of cloud computing. The study by Tilburg University mentioned previously[139] gives a detailed and technical analysis of the capability of EU legislation to address issues specifically related to competition, such as interoperability, portability, lock-in and vertical integration (i.e. the potential for ISPs who are the 'gateways' to the clouds to also provide cloud services and therefore have a potential impact on competition and net neutrality). The study argues that the three relevant legal regimes – EU competition legislation, the telecommunications framework and the E-Commerce Directive – have profound effects on clouds, but fail in covering cloud computing "where it really matters". It concludes: "New services such as cloud computing demonstrate the level of convergence between network operators and ISPs, content providers and electronic commerce services. This situation calls for a streamlined approach in which the scope and reach that services like cloud computing afford is facilitated by regulatory frameworks. Now it seems the opposite situation is in place…"[140] Concerns such as vertical integration, fragmentation of the internal market or data portability will need to be addressed at EU level, in line with the existing strategies and possibly beyond them.

Finally, public procurement is another area for EU cooperation, as it is an important driver of competition, and in this respect European public authorities have a crucial role to play in encouraging innovation and giving chances to new market entrants. In her recent (January 2012) speech to the World Economic Forum, Neelie Kroes, Vice-President of the European Commission and responsible for the Digital Agenda, points out that public IT procurement makes up about 20 percent of the whole market but it is currently fragmented and with limited impact. This buying power can be harnessed through more harmonisation and integration, and ultimately through joint procurement across borders.

As an example of future possibilities, the UK government, under its G-Cloud strategy, held recently an open public procurement tender, with a simplified procedure to also encourage SMEs. The approach is to create procurement frameworks of suppliers who can provide cloud services, so that public organisations can get immediate access as needed.[141] The preliminary results show that nearly 300 suppliers submitted offers for around 2,000 separate services. This is compared to the current situation, with 80% of the public administration services provided by only half a dozen suppliers in long term contracts.[142]

5.2.2 Connectivity

A further possible risk raised by our interviewees of increased usage of cloud services was the resulting customer dependency on the availability of high-speed broadband (including wireless 4G mobile networks or other available technologies). Cloud computing increases the amount of data that is transmitted via broadband, and so the demand for bandwidth will increase; there may be data transfer bottlenecks, as explained by a European official:

[139] Sluijs, J. P., Larouche, P. & Sauter, W., *Cloud Computing in the EU Policy Sphere*, TILEC Discussion Paper No. 2011-036, 2011. Available at SSRN: http://ssrn.com/abstract=1909877.
[140] Ibid, p.38.
[141] See http://gcloud.civilservice.gov.uk/supplier-zone/.
[142] See Chant, C., *CIOs You must be the change you wish to see in the world,* 2011, at http://gcloud.civilservice.gov.uk/2012/01/12/cios-%E2%80%A6-you-must-be-the-change-you-wish-to-see-in-the-world/.

"If we build these fast networks, we build them for a reason because things will flow through them, and not just YouTube videos, even though they make up the bulk of the projections. But other things will be there too and you need this very fast, low latency infrastructure to make cloud computing work for everyday stuff. Starting my work process, if it is served by the cloud, I cannot wait just because there's congestion; otherwise people will not adopt it. It's slowing down the adoption process. On the other hand, once you have the cloud services available people want to use them and will demand and will also pay for the faster networks."

Further, that nature of work in the cloud means that people will want upload speeds that are similar to download speeds, so upload speeds may become a very important factor. Currently download speeds are often significantly higher than those for upload.[143]

In order to take up the challenge of high-speed pan-European broadband connectivity, the European Commission has proposed the Connecting Europe Facility, which has at least 7 billion Euro earmarked for investment in high-speed broadband infrastructure. The Digital Agenda sets 2020 targets of broadband access for all Europeans at speeds of at least 30 megabits per second (Mbps), with at least 50% of households subscribing to speeds above 100Mbps.[144]

5.2.3 Consumer protection and the single market

Cloud services for consumers are already quite mature and established, with millions of users. They will develop further, for example with the fast expansion of sites such as Netflix for renting movies or Spotify for streaming music, providing the current fragmented EU licencing and copyright regimes are properly addressed (as the Commission plans as part of the Digital Agenda 2020).[145] Examination of the issues related to intellectual property in the online environment, even if they are not confined to, or specific, to cloud computing, as shown in Section 5.1.1, is crucial to the development of a digital content single market. EU consumers, as our interviewees have pointed out, are protected from 'cloud harm' by existing laws, particularly the unfair contract terms and unfair commercial practices legislation. However, as highlighted in earlier sections, many mass service providers are based outside of EU jurisdictions, and key contract terms are not transparent or provided. So in practice European consumers are highly unlikely to be able to seek or obtain redress. Providing adequate means for complaints and redress is necessary for the future in the consumer services area; both alternative means – such as online disputes procedures – and collective means of redress, since there is a strong imbalance of powers between consumers and providers of cloud services. In the Digital Agenda 2020 the European Commission committed to explore proposals in the field of collective redress, based on stakeholder consultation.

[143] OECD, *Network Developments in Support of Innovation and User Needs*, 2009.

[144] See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/709&format=HTML&aged=0&language=EN&guiLanguage=en

[145] The Digital Agenda for Europe 2020 has a number of forthcoming actions to address this issue under its Pillar 1 covering the digital single market (http://ec.europa.eu/information_society/digital-agenda/index_en.htm). See also Section 7.2.1 below.

5.3 Future EU-wide benefits

Europe has an ambitious Digital Agenda which constitutes a key part of the smart growth concept within the broader Europe 2020 strategy. The Agenda contains plans for over 100 specific initiatives to spur on further development of the EU information and communication technologies sector. Cloud computing is mentioned specifically in the context of research and innovation and public authority collaboration,[146] though it has relevance to other actions proposed, particularly those related to the single market. The plan is to publish in 2012 a strategy on stimulating cloud computing, as well as engage Member States in the on-going large scale pilot projects for interoperability in areas of public interest (called the Competitiveness and Innovation Programme). These pilots include projects on the deployment of integrated care services, preparation of a services infrastructure on the EU level and an e-justice project.[147]

Many of the other Digital Agenda initiatives proposed by the Commission in fact address the barriers and risks mentioned above in Sections 4 and 5. For example, under initiatives designed to achieve a "vibrant digital single market" and enhance consumer trust, actions for the next 12-24 months include updating of the 1995 Data Protection Directive with new legislation (as mentioned above, Commission proposals published 25 January 2012); and legislative proposals for Alternative Dispute Resolution and Online Dispute Resolution, to address the current redress gap (proposals were published on 29 November 2011). In addition, extensive reviews of the copyright and licensing regimes are planned. Although these issues are not inherent to cloud computing, they nevertheless have a great potential to influence the further and rapid development across the EU of in-the-cloud services such as music and film rentals and streaming.[148]

5.3.1 Environmental impacts of cloud computing

Aside from the general benefits to the competitiveness and innovation in IT services for European consumers, businesses and governments already discussed, the main additional benefit cloud computing can bring is its potential to make IT more environmentally friendly. It may allow organisations to reduce power consumption by idle servers; make more efficient use of energy and hardware resources; and even move energy-intensive computation to data centres where renewable energy is available. On the other hand, cloud computing can also have a negative impact on the environment - the initial building of the big data centres adds to the IT infrastructure overall owned by businesses, governments and consumers. Also, higher energy efficiency reduces costs, which frees capital for acquiring new servers or data centres, leading to the so-called rebound effect (with a possible result that there is no overall reductions in CO_2 emissions). Research to provide methodologies and calculate all these impacts is still in the early stages; one study estimates a potential total carbon emissions reduction for the EU as a whole of around 7.42 million tonnes.[149]

---

[146] European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A Digital Agenda For Europe, COM(2010) 245 final/2*, 2010.

[147] See Action 56 at http://ec.europa.eu/information_society/newsroom/cf/fiche-dae.cfm?action_id=214&pillar_id=47&action=Action%2056%3A.

[148] For actions planned in the next 12-24 months, see European Commission, *Digital Agenda for Europe, Annual Progress Report*, 2011.

[149] OECD, *Cloud Computing,* forthcoming 2012, pp.13-15; citing Thomond, P., Gann, D., MacKenzie, I and A. Velkov, *The Enabling Technologies of a Low Carbon Economy; From Information Tehcnology to Enabling*

ICT for sustainability is another one of the key actions envisaged within the EU Digital Agenda 2020, which recognises that ICT can both contribute to increased energy consumption and be more resource efficient and have a positive impact on the environment. The industry has been asked to adopt a common measurement methodology for its energy performance and greenhouse gas emissions and the proposed methodologies are currently being tested in pilots.[150]

5.3.2 Future cloud services for the single market

As indicated before, pilot project initiatives are on-going to create a common pool of public administration services for the single market. There is an obvious role to play for the EU institutions to assist Member States in coordinating their cloud activity, so as to enable greater benefits of scale as well as ensure more effective collaboration in the areas prescribed by the Treaties, from customs to RAPEX (the common rapid alert system for product safety). Essential inter-EU collaboration activities could be improved by adopting cloud technologies, as one interviewed European official explained:

> *"There are some classical transaction processing systems, very similar to SWIFT in banking, in e-government. They are all set up until now as a software application development, very specific. Many policies need that kind of transaction-based control system. The hope is that you can build them in a much simpler and cost-effective way so that it becomes reachable for those policies to have that. If you do it for customs and taxes, it is justified. This brings so much money in. If you do it for immigration, Schengen – it's also justified. […] I think almost every DG of the Commission would love to have such a system."*

Another European official elaborated further on the potential benefits of mutual learning and increased effectiveness for public administrations that such technology-facilitated collaboration can bring:

> *"If you look at the complexities of public administration, where administration has the tendency just to work in silos, recreating services, recreating the knowledge which is needed to offer the services, it's a way of getting that knowledge or the services from their colleagues in another administration, then they would be in a position to offer far better services. … web technology, web services, enables them to do that in an extremely effective way ... [For example,] in the public procurement domain administrations [are] recreating all kinds of databases with VAT numbers …. If, on the contrary, the VAT authorities were giving access to their VAT databases to all public administrations, they would no longer have to keep it themselves … but they would have direct access to the source of information and would therefore have … up-to-date information, and they would even not have to ask back to the companies about their VAT numbers, when they participate in a bid."*

One cross-cutting service important for both e-government and business services is authentication, or proof of identity, and this has been identified as a good prospective cloud service. The Digital Action Plan envisages the review of the eSignature Directive and cross-border recognition of e-IDs as a key enabler for the single market.[151] A European official explained why establishing a common digital identification system is important in his view:

Technology: Can Cloud Computing Enable Carbon Abatement? Summary Report, 2011 at http://www.enablingtechnology.eu/environment/academic_study.

[150] See section regarding pillar 7 in European Commission, *Digital Agenda for Europe, Annual Progress Report*, 2011, p.14.

[151] See Actions 8 and 83.

"eID is the key to everything else, particularly in the public area. Once you know the person, then you know what to do. You need to have a mechanism of eID in which you can trust... if you do open the services to third parties … it multiplies the security risks ... So we need to develop some technology that will enable us to avoid that."

Discussions on e-ID always invoke "Big Brother" fears, particularly in countries such as the UK that do not have identity cards. According to one of the government officials however, authentication need not be connected to an ID card:

"We are implementing now the mobile electronic identity which will allow in any circumstances to use your digital certificate in relation to electronic services from state... It's your electronic identity but it's not stored on the ID card. It's stored on this subscribed identity board in your phone, in the SIM card of your phone. And whenever your signature or certificate is required, you just enter your PIN to access the information on your SIM card and the certificate becomes available to the application."

At a strategic level, the European Network and Information Security Agency (ENISA) has recommended that "national governments and European Union institutions [...] further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied, both in terms of legislation and security policy and where interoperability and standardization could be fostered. Moreover such a European Union wide infrastructure could be used in the context of a pan European mutual aid and assistance plan for emergencies."[152]

Also, the European Space Agency (ESA) and the European Organization for Nuclear Research (CERN) recently presented in a joint document the vision of forming a European Industrial Strategy for a Scientific Cloud Computing Infrastructure to be implemented by 2020. The cloud computing infrastructure is expected to "provide interoperable services for computing, data dissemination, data archiving, application development platforms, large-scale open and free data-set management and libraries". It is intended to provide physical and organisational structures and assets needed for the IT-related operation of research institutions, enterprises, governments and society. "To join the European Cloud Computing Infrastructure, a service provider will need to demonstrate compliance with quality standards, compatibility with other providers and adherence to security/integrity rules."[153]

The potentially large benefits to research reside particularly in the flexibility, speed and pooling of common resources that the cloud technology model can provide, as explained by one of the European officials we spoke to:

"[CERN's Large Hadron Collider produces] a humongous amount of data every second and today they are working on a European grid infrastructure pushing this out so that researchers in real time can see the data pulsing round the globe. And this grid is basically public sector … But they see the development is so quick now that it might not be possible to keep up the speed that they want by keeping it on the public sector…. They made an analysis and saw that the providers in Europe are not there yet, even American ones. [..] So they started a process where they came together to pool common requirements and the idea is to pool either concretely or virtually their buying power, vis-à-vis the sector. [..] And that is a good example and we wish we could replicate something approaching this in the wider public sector space. The research is only one side. They tend to be the forerunners because they have more data than everybody else."

[152] ENISA, Catteddu, D. & Hogben, G. (eds.), *Security and resilience in governmental clouds*, 2011, p. 9.
[153] CERN and ESA, *Strategic Plan for a Scientific Cloud Computing infrastructure for Europe*, 2011.

6 CONCLUSIONS AND RECOMMENDATIONS

- In terms of policy instruments, the main concerns and risks related to cloud computing can be divided into three main categories: *legislative framework-related* (legal fragmentation; jurisdiction; compliance and liability; enforcement and redress), *contracts/terms and conditions-related* (Service Level Agreements; End User Agreements; privacy terms and conditions; clarity and transparency), and *standards-related* (interoperability; portability; vendor lock-in).
- Relevant actions to promote and encourage further development of cloud computing are already included in the programme for the Digital Agenda for Europe. Based on the evidence collected in the framework of this study, actions in five areas could be considered by EU policy makers:

1. *Address legislation-related gaps*, by fully harmonising data protection rules across the EU; by addressing gaps related to cloud computing in other EU legislation; by better protecting users regarding data disclosure by providers to law enforcement authorities; by fostering global agreements on data protection standards; and by providing collective redress against security and privacy breaches in cloud services. Cross-border cloud services depending on a uniform intellectual property rights regime would benefit from an increased level of harmonisation in this respect.
2. *Improve terms and conditions for all users,* by developing international best practice models for contracts, or 'model contracts'; and by ensuring complete transparency by providing all terms and conditions in a very clear format.
3. *Address stakeholder security concerns,* by examining the feasibility of an independent auditing and certification system for provider security systems; and by extending to cloud services providers the applicability of some of the provisions that apply to ISPs and mobile networks under the EU electronic communications regulatory framework.
4. *Encourage the public sector cloud,* by developing systems of cloud-based collaboration between public administrations across the EU and coordinating Member States' efforts; by promoting the adoption of cloud computing by EU institutions, as well as its integration with the EU's e-government plan; and by encouraging the development of best practices in public procurement across the EU, including wide use of open standards.
5. *Promote further research and development in cloud computing,* in particular regarding: costs and benefits of conventional IT services versus cloud provision; how EU legislative frameworks and international agreements fit current and future cloud computing services scenarios; the economic impact and the environmental impact of cloud computing; empirical research comparable across the EU 27 on cloud computing user experiences, behaviour and risk perception; and cloud-based awareness and resource exchange systems particularly to educate and exchange best practices for SMEs and public authorities.

6.1 Conclusions

The purpose of this study is to provide a broad overview on cloud computing, and specifically how it relates to consumers and EU digital single market goals, in terms of benefits, related risks and policy challenges. Its aim is to provide background information and advice for the Members of the European Parliament IMCO (Internal Market and Consumers) Committee on priority measures and actions to be undertaken in this field. One of the first challenges encountered during the research for this study was to find an established, widely accepted definition of cloud computing. It does not denote a new technology, but rather a new way of delivering computing services. Without a workable definition, it can be a rather vague term with a multitude of meanings which can be as broad as to encompass the whole of the Internet. We therefore adopted for this study the NIST (the US National Institute of Standards and Technology) definition of cloud computing, which - to paraphrase - refers to computing services and resources (such as software programmes, remote file storage, etc.) that can be accessed from any device at any time and from everywhere, regardless of geographic location, and that can be rapidly scaled to a user's need with minimum management effort.

Under this definition, there are certain benefits and risks that are inherent to the cloud computing model, rather than apply to the online world as a whole. Other concerns expressed strongly by stakeholders - mainly about privacy and security of data entrusted to the 'cloud' - are related to the online world generally, but the cloud computing model intensifies them, and generates a lack of user confidence and trust that can limit adoption.

Cloud computing has in recent years gained in importance and has climbed up on the EU policy agenda because of its close links with the single market goal of achieving a stronger and more competitive digital internal market, as outlined in the ambitious Digital Agenda. A look into the potential benefits of this computing model justifies its perceived importance as a tool for the single market as it can bring considerable cost savings and increased competitiveness of IT services to public and private organisations. It also makes it possible for small start-up businesses to enter the market without worrying about large investments into IT infrastructures; therefore it is also one of the enablers for innovation and jobs creation. Potentially too, it can be an effective tool for collaboration at the EU intergovernmental level and for enhancing e-government services for EU citizens. Consumers could also benefit from the greater convenience, flexibility and cost-saving afforded by cloud services. These important benefits indicate the need to spur on its further development in Europe.
We have identified a number of main specific concerns and risks, expressed by virtually all those we interviewed, as well as widely acknowledged in the literature reviewed. They relate broadly to issues concerning privacy, security, trust and quality of service. In terms of policy instruments, these can be divided into three main categories:

- **Legislative framework related**: *legal fragmentation; jurisdiction; compliance and liability; enforcement and redress*. Due to fragmentation of legal regimes within the EU 27 Member States, and the fact that data centres and providers can be located anywhere round the world, it is not generally clear which legal system is applicable to a cloud computing service; there is difficulty in providing cloud services across borders; and there is general confusion regarding rights and responsibilities related to cloud computing services. Different Directives and Regulations may have different liability provisions. Relevant legislation may also have important gaps in its applicability to cloud computing services, given also that there is as yet no established universal definition. Consequently there may be limited enforcement and

compliance, and difficulties in obtaining redress. The choice of laws may have serious repercussions for European based SMEs since they may not be able to afford the inconvenience and expense of enforcing their rights in another country or continent. Particularly relevant legislation includes: the Data Protection Directive,[154] and the related individual Member States' laws regarding access to data stored in the cloud (relevant for all stakeholders); the E-Privacy Directive[155] (relevant for all stakeholders), the Unfair Commercial Practices Directive[156] (business to consumer practices only), the Unfair Contract Terms Directive[157] (consumer contracts only), and the e-Commerce Directive (relevant for all stakeholders).[158] Also very relevant are various international agreements and guidelines, e.g. the Safe Harbour agreement regarding data protection with the US, the OECD Guidelines for the Protection of Privacy in Transborder Data Flows, and the OECD Security Guidelines.

- **Contracts/terms and conditions related**: *Service Level Agreements (SLA); End User Agreements (EULA); privacy terms and conditions and issues related to clarity and transparency in disclosure*. Due to uncertainties regarding applicable law and jurisdictions, contracts are the main tools for establishing relationships between cloud providers and customers. For consumers and the majority of business users of public multi-tenancy 'clouds', they are 'fixed menu', rather than *à la carte,* with the terms set by the providers. For SMEs not covered by consumer protection legislation they are the only provision available. Large companies and public authorities may have more clout to negotiate. Contracts may be lacking key terms or use unfair or even illegal terms, are unclear and difficult to read and/or print, often apply out-of-EU legislation resulting in difficulties to access redress, may have no readily accessible complaints mechanisms, and many deny liability for loss of data and other damage, and give no information regarding the location of data centres where the customer data is stored.

[154] Directive 95/46/EC. On 25 January 2012 the Commission published a proposal for a comprehensive reform of the data protection rules, see Section 4.2.3 of this study.
[155] Electronic Communications Privacy Directive, as amended by the Citizen's Rights Directive 2009/136/EC.
[156] Directive 2005/29/EC.
[157] Directive 93/13/EEC.
[158] Directive 2000/31/EC.

- **Standards related:** *interoperability; portability; vendor lock-in*. There is a risk of further development of concentrated, incompatible cloud services. Profitability of IT cloud services provision increases with the number of users, so there are no incentives for dominant providers to make their systems compatible with others and thus open the doors to competition. This may have an impact on cost reductions and innovation across the whole of the EU economy. Lack of interoperability also creates the risk of lock-in for customers particularly when there is no mechanism to export large amounts of stored data. It may also preclude effective inter-governmental co-operation on the EU level, including in the delivery of e-government services. Standardisation, including use of open standards, is the most important tool for achieving interoperability; there are currently many standardisation efforts, though they are not as yet necessarily converging.

If not addressed, these issues can be a barrier to future adoption of this IT model, particularly by SMEs and public authorities where take up so far has been limited. The 'cloud' for individual consumers is much more developed and used by many millions of people, nevertheless there are risks there too, related to information asymmetries and potential individual detriment. Further, lack of adoption by SMEs can also have an impact on new Europe-generated innovative services for consumers.

6.2 Recommendations for possible actions

Based on the evidence collected during this study, in this final section we outline some of the most important 'high-level' solutions that could be considered by EU policy makers to promote and encourage further development of cloud computing. Many relevant actions are already included in the programme for the Digital Agenda for Europe, with some of the most relevant for promoting cloud computing including the publication of a strategy on stimulating cloud computing in the digital single market due in early 2012; the proposal for the reform of the data protection rules (published 25 January 2012); the proposal for a Regulation on European Standardisation and the Commission Decision to set up a European multi-stakeholder platform on ICT standardisation to provide advice and expertise (of 28 November 2011).[159] Most recently Vice-President Kroes announced the launch of a Partnership with an initial 10 million Euro investment, made up of all the main players in the cloud computing field which will, essentially, look into finding solutions to all the barriers and challenges identified in the sections above, but start with public authority procurement.[160]

[159] European Commission, *Digital Agenda for Europe, Annual Progress Report*, 2011; Pillars 1, 2 and 5.

[160] Kroes, N., *Setting up the European Cloud Partnership*, Speech at the World Economic Forum, Davos, Switzerland, 2012, see http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38.

6.2.1 Address legislation-related gaps

Actions would be designed to address fragmentation in legal regimes as well as any gaps in the applicability of existing frameworks. Main measures could include:

- Full harmonisation of data protection rules across the 27 EU Member States in the review of the Data Protection Directive.
- Review of the Directive to cover key identified gaps in the applicability to cloud computing privacy protections, including introduction of new principles of accountability and privacy by design as well as extension of the data breach notification rules.[161]
- Forthcoming reviews of other EU legislation (e.g. the e-Commerce Directive) to address their applicability and gaps related to cloud computing.[162] In particular, reviews of EU legislation that has been transposed into Member State laws in a non-uniform manner, potentially fragmenting the digital single market. Cross-border cloud services that depend on uniform intellectual property right regimes would benefit from an increased level of harmonisation in this respect.
- Better user protection with regard to compulsory data disclosure by providers to law enforcement authorities, by advance notification and provision of encrypted 'data lockers'.
- Global agreements on data protection standards, including via supporting the revision of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and a review of the current Safe Harbour agreements.
- As well as speedy adoption (in 2012) of the legislative proposals for Alternative Dispute Resolution (ADR) and Online Dispute Resolution (ODR), serious consideration should be given to providing consumers with means of collective redress against security and privacy breaches in cloud services. This is not an area in which individual consumers are likely to be able to take action.

[161] On 25 January 2012, the European Commission published a proposal for a comprehensive reform of the data protection rules (see European Commission, *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) 11 final*, 2012, at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf). The proposed new legal framework consists of two legislative proposals: a 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); and a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

[162] Regarding e-commerce, see the recent European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 94*, forthcoming 2012, at http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm . For other legislation, see European Commission, *Digital Agenda for Europe, Annual Progress Report*, 2011: in particular, a proposal for a Directive on Collective Rights Management is planned for adoption in the first quarter of 2012; a revision of the Directive on enforcement of intellectual property rights (IPR) which will address online piracy is expected in the first half of 2012; a review of the eSignature Directive and mutual cross-border recognition of e-Ids is due in the second quarter of 2012; a potential review of the Directive on re-use of Public Sector Information may occur in 2012; a 2011 Commission proposal for a Regulation on European Standardisation is under review by the Council and European Parliament in 2012; the Commission will adopt the technical implementing measures for the E-privacy Directive in mid-2012; and a 2010 Commission proposal for a Directive on Attacks against Information Systems is under review by the Council and European Parliament in 2012.

6.2.2 Improve terms and conditions for all users

As seen from previous sections, there is a broad consensus that off-the-shelf contracts targeted at both consumers and SMEs need an overhaul, both in connection with some of the terms they contain, and in the way they communicate the key provisions to users, i.e. in their level of transparency. Positive steps can include:

- Development of international best practice models for contracts, or 'model contracts', outlining key points they should communicate and questions they should answer. Models and checklists are suggested in this report, and include issues such as information regarding what legislation the provider complies with, location of servers and the provider, specific liabilities and disclaimers, notice of deletion of user data, disclosure to third parties, etc.
- Ensuring complete transparency by providing all terms and conditions in a very simple, readable and readily accessible format including prominent access to the key provisions. Again, examples on how this can be achieved are mentioned in this report.

6.2.3 Address stakeholder security concerns

Security is a key concern for all cloud users, and related concerns can act as major barriers to adoption both by SMEs and public authorities. Large users can request audits of providers' security systems, while providers may be reluctant to allow private auditors detailed inspections of their systems. One positive recent action has been the temporary extension of the European Network and Information Security Agency's (ENISA) mandate, including the proposal to strengthen it. Other possible actions can include:

- Examination of the feasibility of introducing an independent auditing and certification system for provider security systems, targeted at providing necessary reassurance regarding security levels of providers for all stakeholders, but in particular for business and public authority users. Further investigation of the potential value of such systems in improving take-up.
- Extending to cloud services providers the applicability of the provisions that apply to ISPs and mobile networks under the EU electronic communications regulatory framework[163] regarding technical and organisational measures to manage risks to security and integrity of their networks, as well as to notify authorities of significant security breaches. This can be achieved through the current revision of the Data Protection Directive.

[163] Articles 13a and 13b of Directive 2009/140/EC amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

6.2.4 Encourage the public sector cloud

As the public authorities' take-up is currently limited, further measures can be taken to encourage pan-EU take-up both on national levels and for EU-level inter-governmental co-operation. To the latter end a start has been made with pilot research projects and initiatives such as the Connecting Europe Facility.[164] Clouds can assist greatly in the e-government agenda by providing information in one place to the citizen, together with software to manipulate the data. Measures could include:

- Development of systems of cloud-based collaboration in e-government actions between public administrations across the EU and coordination of Member States' efforts, while ensuring privacy and security impacts assessments and cost-benefit analysis before ambitious schemes are considered.
- Adoption of cloud computing by EU institutions, as well as its integration with the EU's e-government plans; this could form part of the forthcoming cloud computing strategy.
- Development and encouragement of best practices in public procurement across the EU, including wide use of open standards; development of a common portal for resources to share such practices.

6.2.5 Further research and development

This is an overarching need, to substantiate in further detail both the perceived benefits of cloud computing, the user experiences and risk perception, as well as further measurements of the benefits and impacts of cloud computing. Specifically:

- Research and measurement, using consistent and comparable methodologies, into costs and benefits of conventional IT services versus cloud provision for public authorities in Member States.
- Further analysis of how current EU legislative frameworks and international agreements fit particular cloud computing services scenarios, and how they would need to be adapted in the future.
- Further studies to measure both the economic impact and the environmental impact of cloud computing; there are still very few studies on these aspects, partly due to the fact that policy makers and academics do not have access to companies' data.
- Empirical research comparable across the EU 27 on user experiences, behaviour and risk perception.
- Development of cloud-based awareness and resource exchange systems particularly to educate and exchange best practices for SMEs and public authorities; these can take the form of resource portals, forums, webinars and other cloud-based collaboration tools.

[164] The Connecting Europe Facility will finance projects which fill the missing links in Europe's energy, transport and digital backbone, see http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1200&format=HTML&aged=0&language=EN&guiLanguage=en.

ANNEX 1 - BIBLIOGRAPHY

- *Industry recommendations to Vice President Neelie Kroes on the orientation of a European cloud computing strategy*, 2011.
- Armbrust, M., et al., *Above the Clouds: A Berkeley View of Cloud Computing*, 2009.
- Bradshaw, S., Millard, C. & Walden, I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper no. 63, 2010.
- BSA, *Cloud Computing Policy Agenda for Europe*, 2011.
- CEBR, *The Cloud Dividend: Part One - The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and the UK*, 2010
- CERN & ESA, *Strategic Plan for a Scientific Cloud Computing,* 2011.
- Chant, C., *CIOs You must be the change you wish to see in the world,* 2011.
- CIO/IDG Research Services, *CIO Global Cloud Computing Adoption Survey ResultsSummary*, 2011.
- Colt, *European CIO Cloud Survey*, 2011.
- Consumer Federation of America, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, 2010.
- Datatilsynet (Danish Data Protection Agency), *Processing of sensitive personal data in a cloud solution*, 2011.
- Digital Agenda Assembly, *Report from Workshop 18: "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand"*, 2011.
- DigitalEurope, *Position Paper on the European Commission's Communication on"A comprehensive approach on personal data protection in the European Union"*, 2011.
- DigitalEurope, *Cloud Computing. DigitalEurope's perspective*, 2011.
- DLA PIPER, *EU study on the Legal analysis of a Single Market for the Information Society: New rules for a new age?*, 2009.
- EGIZ, Zwattendorfer, B., *Anforderungen für E-Government Anwendungen in der Cloud*, 2011.
- Ellison, L., speech at Oracle OpenWorld 2008, September 25, 2008.
- ENISA, Catteddu, D. & Hogben, G. (eds.), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009.
- ENISA, Catteddu, D. & Hogben, G. (eds.), *An SME perspective on cloud computing-Survey*, 2009.
- ENISA, Catteddu, D. & Hogben, G. (eds.), *Security and resilience in governmental clouds*, 2011.
- ETNO, *ETNO Reflection Document replying to the public consultation on Cloud Computing*, 2011.
- Etro, F., *The Economic Impact of Cloud Computing on Business Creation*, Review of Business and Economics, Vol. 54, 2, 2009.

- Euractiv.com, *Cloud Computing: Good or bad for IT jobs?, 2011*
- European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. Communication on future networks and the internet, COM(2008) 594 final*, 2008.
- European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010*, 2010.
- European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A Digital Agenda For Europe, COM(2010) 245 final/2*, 2010.
- European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. Towards interoperability for European public services. COM(2010) 744 final*, 2010.
- European Commission, *Hearing with SMEs, meeting note*, 2011.
- European Commission, *Digital Agenda for Europe, Annual Progress Report*, 2011.
- European Commission, DG Information Society and Media, *Cloud Computing: Public Consultation Report*, 2011.
- European Commission, *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) 11 final*, 2012.
- European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 94*, forthcoming 2012.
- European Ministerial eGovernment Conference, *Borderless eGovernment Services for Europeans: Exhibition Catalogue*, 2011.
- Focus.com, *Is Facebook a cloud?*, 2011.
- Fraunhofer Institute for Open Communication Systems, *Cloud Concepts for the Public Sector in Germany – Use Cases*, 2011.
- Gallagher, S., *PATRIOT Act and privacy laws take a bite out of US cloud business*, 2011.
- Google, *Google contribution to the Public Consultation on Cloud Computing*, 2011.
- Google, *Security Whitepaper: Google Apps Messaging and Collaboration Products*, 2011.
- Guvernul Republicii Moldova, *Strategia Tehnologică Privind E-Transformarea Guvernării*, 2011.
- HM Government, *Government Cloud Strategy*, 2011.
- Hon, W. K., Millard, C. & Walden, I., *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1*, 2011.

- Hon, W. K., Millard, C. & Walden, I., *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2*, 2011.
- HP, *Transform data center economics and meet dynamic business needs: The business case for the HP CloudSystem Matrix*, 2011.
- Huddle, *Enterprise level security, the Huddle way.* Security whitepaper, 2011.
- Hustinx, P., *Data Protection and Cloud Computing under EU law*, Third European Cyber Security Awareness Day, BSA, European Parliament 2010.
- IDC, Bradshaw, D., *Western European Software-as-a-Service Forecast, 2009-2013*, 2009.
- IDC, Gens, F., Mahowald, R. P. & Villars, R. L., *IDC Cloud Computing 2010 - An IDC Update*, 2009.
- IDG New Service, Perez, J.C., *PayPal to open app store for developers*, 2010.
- Ilves, T., *Speech at the London Conference on Cyberspace*, 2011.
- India Knowledge@Wharton, *SlideShare's Rashmi Sinha: 'We Wanted to Reach Millions'*, 2010.
- Ipsos OTX MediaCT, *Head in the clouds? Cloud computing and consumers*, Free year-round insights Technology Edition #2, June issue, 2011.
- Irion, K., *Government cloud computing and the policies of data sovereignty*, 2011.
- kimpl.com, *Most secure online backup and file sync service*, 2011.
- Kincaid, J., *G.ho.st's Web-Based Operating System To Shut Down March 15*, 2010.
- Kincaid, J., *Online Finance Startup Wesabe Heads To The Deadpool*, 2010.
- Kroes, N., *Setting up the European Cloud Partnership*, Speech at the World Economic Forum, Davos, Switzerland, 2012.
- Kundra, V., *Federal Cloud Computing Strategy*, 2011.
- Kustor, P., *Cloud Computing - The Austrian Approach*, 2011.
- Linklaters, Van Overstraeten, T. & Bruyndonckx, B., *Law Enforcement and Cloud Computing*, 2011.
- LSE, Castro, D, Grous, A & Karrberg, P, *Modelling the Cloud - Employment effects in two exemplary sectors in The United States, the United Kingdom, Germany and Italy,* January 2012
- Macleod, A., *Update on G-Cloud, Application Store for Government and Data Centre Consolidation,* Cabinet Office presentation; 2011.
- Microsoft, Harms, R. & Yamartino, M., *The Economics of the Cloud*, Microsoft whitepaper, 2010.
- Microsoft, *TOUCH - Microsoft Technology in Government, Education and Healthcare*, 2011.
- Microsoft, *Office 365 Security and Service Continuity for Enterprises*, 2011.
- Microsoft, *Privacy in the Public Cloud: The Office 365 Approach*, 2011.
- Microsoft, *Towards a 'Cloud-Active' Europe – Examples of Member State and Regional policies and investments helping Europe realize the potential of cloud computing,* unpublished.

- Miller, M., *Cloud Computing Pros and Cons for End Users*, February 2009.
- Moran, F. G., *The European Cloud Computing Strategy*, Tutorial at the 5th International Conference on Theory and Practice of Electronic Governance, 2011.
- Navarro, M., *Cloud computing: What does it mean for Europe? Digital Agenda Assembly presentation*, 2011.
- NIST, Mell, P. & Grance, T., *The NIST Definition of Cloud Computing*, 2011.
- NPD Group, *Consumers Don't Know What Cloud Computing Is, Even Though They Use it All the Time*, 2011.
- OECD, *OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*, 2002.
- OECD, *Network Developments in Support of Innovation and User Needs*, 2009.
- OECD, *Cloud Computing,* forthcoming 2012.
- Ofcom, *International Communications Market Report*, 2011.
- Oxford Economics, *Digital Megatrends 2015 - The Role of Technology in the New Normal Market,* 2011
- Palmer, M., *Google faces Norwegian public sector ban*, 2012.
- Perez, J. C., *PayPal to open app store for developers*, IDG News Service, 2010.
- Pew Internet and American Life Project, Horrigan, J. B., *Data Memo re Use of Cloud Computing Applications and Services*, 2008.
- Pew Internet and American Life Project, *The future of cloud computing*, 2010.
- Pierre Audoin Consultants, *Le Cloud Computing en France: Résultats de l'enquête auprès de 200 décideurs informatiques*, 2010.
- Pierre Audoin Consultants, *PAC's Cloud Computing Worldwide by countries datamart 2012*, 2011.
- Ponemon Institute, *The Security of Cloud Infrastructure - Survey of U.S. IT and Compliance Practitioners*, 2011.
- Ponemon Institute, *Security of Cloud Computing Providers Study*, 2011.
- Poujol, M., *Trends and Evolution in Cloud Computing market in Europe*, 2010.
- Price, M., *Pinning Down the Cloud,* Wall Street Journal, 14 Feb 2011.
- Redshift Research, *Adoption, Approaches & Attitudes: The Future of Cloud Computing in the Public and Private Sectors*, 2011.
- Renda, S., *US "Cloud First" Policy Insights, EC-ETSI Standards in the Cloud Workshop*, 2011.
- Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., Hopkins, P., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Rand Europe, time.lex, University of Warwick, 2011.
- SIIA, *Guide to Cloud Computing for Policymakers. SIIA whitepaper*, 2011.
- Sluijs, J. P., Larouche, P. & Sauter, W., *Cloud Computing in the EU Policy Sphere*, TILEC Discussion Paper No. 2011-036, 2011.
- TACD, *Resolution on Consumer Protection in Cloud Computing*, 2011.

- Telecompaper, *France to form Andromede cloud computing Joint Venture in November*, 2011.
- Telecompaper, *Dassault Systemes pulls out of cloud project*, 2011.
- The Economist, *Let it rise: A special report on corporate IT*, 2008.
- The Lisbon Council, Mettler, A. & Williams, A. D., *The Rise of the Micro-Multinational:How Freelancers and Technology-Savvy Start-Ups. Are Driving Growth, Jobs and Innovation*, 2011.
- Thomond, P., Gann, D., MacKenzie, I and A. Velkov, *The Enabling Technologies of a Low Carbon Economy; From Information Technology to Enabling Technology: Can Cloud Computing Enable Carbon Abatement? Summary Report*, 2011
- Turcanu, I., *M-Cloud: E-Governance Techology Platform*, 2011.
- Vance, A., *Google's Search Goes Out to Sea*, 2008.
- Wired.com, Calore, M., *Ma.gnolia Suffers Major Data Loss, Site Taken Offline*, 2009.
- World Economic Forum, *Exploring the Future of Cloud Computing*, 2010.
- Wyld, D. C., *Cloud Computing: Is it the Fifth Utility?*, 2009.
- Wyld, D. C., T*he Cloudy Future of Government IT: Cloud Computing and the Public Sector around the world*, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, 2010.
- Yeh, C., *Box Innovation Network: Innovation in Enterprise Software is Possible*, 2011.

ANNEX 2 - LIST OF ORGANISATIONS INTERVIEWED

- Bureau Europeen des Unions des Consommateurs (BEUC)
- Datatilsynet (Danish Data Protection Agency)
- European Commission
- DigitalEurope
- European Digital Rights (EDRi)
- e-Government Center of Moldova
- Estonian Information Systems Authority
- Federal Chancellery of Austria - Digital Austria Platform
- Selected cloud service providers of different sizes (3)
- Large technology company
- United Kingdom Government Cabinet Office
- Verbraucherzentrale Bundesverband (VZBV)

ANNEX 3 - CLOUD PROVIDER WEBSITE CHECK METHODOLOGY

Over the December 2011 period we undertook a website check of 15 consumer- and business-oriented cloud services to assess the clarity, completeness and accessibility of information provided regarding their security conditions and privacy policies (see results tables in the main text).

We first assessed the general ease with which users can find information for both security and privacy. If a link is clearly labelled on the first page of the website, which then leads to a page clearly laying out relevant information or pointing to a document to be downloaded, then the grading received is 'Easy'. If any of the above provisions are lacking, then the grading received is 'Not easy'.

Next, all subsequent criteria are assessed according to the grading Clear/Not clear/Not found. Specifically, a 'Clear' grading refers to information that is present, easily accessible, easy to understand, and complete. 'Not clear' refers to information that is present, but which is either difficult to find or understand, or is manifestly incomplete. 'Not found' denotes the absence any information that could be obtained in a thorough search by our researchers (simulating the intensity of search that could be expected from a typical user, i.e. between 5 to 10 minutes for each of the 18 criteria assessed for each provider). Three of the 18 criteria assessed concern the provision of information that does not relate to security or privacy in particular, assessed in the last 3 rows of each table with the grading Yes (information present/Not found).

EUROPEAN PARLIAMENT

CATALOGUE BA-32-12-189-EN-C

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-3743-1
doi: 10.2861/81619

Publications Office

CLOUD COMPUTING