Preface

This document considers the extent to which the development of cloud computing (from the perspective of cloud services *per se* and cloud-hosted services delivered over cloud platforms) raises issues of concern to telecommunications regulators. The cloud is defined (and its varieties classified) in various ways. These definitions are not authoritative, stable or future-proof. They share certain elements – for instance, distinctions among cloud architectures or business models that offer users X-as-a-service access to platforms, infrastructures, software, hardware, and converged communications. These ‘architectures’ can alter the effectiveness and reach of regulatory powers and duties; for example, users gain access to the cloud and to unregulated cloud-hosted services through the Internet in ways that are to some extent regulated; this creates some regulatory traction over these services (e.g. via prices and terms under which access is granted or the ease with which users and providers of cloud-hosted services can switch Internet service providers). A ‘reverse’ example is cloud-hosted alternatives to otherwise-regulated services (e.g. communications). These may challenge the effectiveness of regulation much as VOIP offers a way to ‘bypass’ regulated voice telephony, but over a greatly expanded range of services. Alternatively, competition within the cloud can provide market-based solutions to regulatory problems. For this reason, and to cope with the rapid development of new offerings and business models that ‘cross the lines’ as the cloud value network evolves, it is useful to attempt a stable scheme for assessing cloud development and identifying areas where new, modified or withdrawn intervention might be appropriate.

This document contains i) a mapping of the cloud landscape; ii) an overview of the current status and likely future evolution of the cloud services market; iii) a scheme for classifying cloud-related issues and iv) a prioritised indicative inventory of issues of potential regulatory concern. It also sketches some issues in need of theoretical development. It may be of interest to regulators and researchers interested in the regulatory implications of cloud computing, particularly as applied to consumer interests.

The work described here has its roots in a series of projects conducted under the auspices of RAND Europe and the University of Warwick. Support from the European Commission and various ministries of the US, UK and Netherlands’ government to those projects is gratefully acknowledged. The issues described have also been discussed at a range of conferences and seminars, and the authors acknowledge that many of the ideas discussed have their origins in open discussion. However, none of the views expressed should be attributed to any of those institutions or colleagues; they remain the authors’ own responsibility.
# Contents

Preface........................................................................................................................................ii
Table of figures ................................................................................................................................vii
Table of tables ................................................................................................................................viii
Summary........................................................................................................................................ix
Introduction...................................................................................................................................ix
Differentiating the cloud................................................................................................................x
Roles ............................................................................................................................................xi
Essential or defining characteristics..........................................................................................xi
Service Models ............................................................................................................................xii
Deployment Models....................................................................................................................xiv
General, economic and technical characteristics........................................................................ xv
  General (or ‘non-functional’) aspects...................................................................................... xv
  Economic Factors.................................................................................................................... xvi
  Technological Features........................................................................................................ xvi
Market situation........................................................................................................................... xviii
Potential Issues and interests for telecommunications regulators.......................................... xx
List of terms ................................................................................................................................ xxiv

CHAPTER 1   What is Cloud Computing? ..............................................................................1
  1.1 Interpretations ..................................................................................................................1
    1.1.1 Essential characteristics and features .................................................................2
    1.1.2 Roles ..................................................................................................................2
    Comment: clouds as two-sided markets....................................................................3
    1.1.3 Service Models ...............................................................................................5
    1.1.4 Deployment models .......................................................................................8
4.3 Issues with policy and regulatory interventions

4.3.1 Location and jurisdiction

4.3.2 Consumer information, transparency of CSP practices

4.3.3 Locus of control

4.3.4 Complexity of the cloud

4.3.5 Certification and other forms of self- or co-regulation

4.3.6 Cloud neutrality

4.3.7 Consumer/SME similarities, regulatory heritage and convergence

4.3.8 Trust

CHAPTER 5 Theoretical issues and applications

5.1 Computer-based financial trading

5.2 Supply chain repositories

5.3 The app ecosystem

5.4 Privacy issues

REFERENCES

Reference list

Annex: Three cloud scenarios

A. Introduction and key features

B. Short descriptions

Scenario 1: Cloud-max

Scenario 2: Nothing new

Scenario 3: Clouds as a new critical infrastructure

C. Relation to issues
Table of figures

Figure 1: Three cloud service models ................................................................. xiii
Figure 2: Two-sided market view ........................................................................ 4
Figure 3: The three cloud service models .......................................................... 7
Figure 4: Dimensions of the cloud ..................................................................... 10
Figure 5: Simplified value chain ......................................................................... 11
Figure 6: Enterprise cloud-hosted service revenue by sales channel, worldwide
           2010-2015 .................................................................................................. 22
Figure 7: Enterprise cloud-hosted service revenue by sales channel, worldwide
           2010-2016 .................................................................................................. 22
Figure 8: Drivers of cloud adoption ..................................................................... 30
Figure 9: Barriers to cloud adoption ................................................................... 31
Figure 10: Nebula Internet architecture ............................................................... 74
**Table of tables**

<table>
<thead>
<tr>
<th>Table 1: End-user control under various delivery models</th>
<th>xiv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2: Business and consumer benefits</td>
<td>xvii</td>
</tr>
<tr>
<td>Table 3: Overview of policy issues</td>
<td>xxi</td>
</tr>
<tr>
<td>Table 4: End-user control under various delivery models</td>
<td>7</td>
</tr>
<tr>
<td>Table 5: Cloud-hosted email usage</td>
<td>23</td>
</tr>
<tr>
<td>Table 6: Examples of consumer cloud services</td>
<td>25</td>
</tr>
<tr>
<td>Table 7: Proportion of those using online applications and services to store data who cite ‘major reason’ for using them</td>
<td>26</td>
</tr>
<tr>
<td>Table 8: Citizen and consumer harm issues</td>
<td>39</td>
</tr>
<tr>
<td>Table 9: Implementation and related issues</td>
<td>41</td>
</tr>
<tr>
<td>Table 10: Scenarios</td>
<td>72</td>
</tr>
<tr>
<td>Table 11: Citizen and consumer harm issues in three scenarios</td>
<td>78</td>
</tr>
</tbody>
</table>
Introduction
Cloud computing provides a technical and business model for making computing services (including storage and processing) available to a wide range of users over the Internet. It may have profound effects on many aspects of social and business life and is therefore a matter of potential regulatory concern. These concerns overlap with telecommunications regulators’ statutory duties because access to the cloud takes place over the telecommunications networks and because cloud activity may substitute for or complement other activities and services currently falling within their remit. Therefore, to the extent that their authority extends to the cloud, it is useful to understand whether intervention might be necessary and appropriate; where cloud activities cannot be regulated or where regulatory authority is fragmented or patchy, it is important to assess the degree to which the development of the cloud and the market for cloud services alter the effectiveness of regulatory governance. Beyond this, the cloud is rapidly rising up business, societal and political agendas; for example, Vice-President Kroes of the European Commission (Commissioner for the Digital Agenda), called for Europe to “go beyond cloud-friendly. A ‘cloud active’ Europe would help create opportunities in Europe…we can expect productivity gains across Europe’s economy as a whole.”

As noted in the Preface, this paper is intended to provide a resource for addressing these issues by providing: i) a mapping of the cloud landscape; ii) an overview of the current status and likely future evolution of the cloud services market; iii) a scheme for classifying cloud-related issues and iv) a prioritised indicative inventory of issues of potential regulatory concern. We begin with three background sections: a primer on the definition and classification of the key qualities and characteristics of cloud computing; a summary of the broader market environment; and the thresholds for at least one telecom regulator’s interest in cloud issues. This is followed (in Chapter 4) by a mapping of potential direct and indirect policy concerns and an assessment of the scope for regulatory intervention and by a sketch of some issues of regulatory concern posing interesting theoretical challenges. An annex develops three scenarios used in the development of the analysis. The balance of this summary provides brief overviews of these sections.

Differentiating the cloud

The cloud is different from other information services and products in a number of potentially significant ways. They reflect the perspectives of various stakeholders involved with the cloud, which may lead to coordination challenges in identifying problems and implementing solutions. To draw out essential characteristics of the cloud, it is useful to start with a definition that already garners considerable currency within policy circles, as proposed by the US National Institute of Standards and Technology (NIST):

“a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

In essence, the cloud gives cloud users access to a wide range of ICT-related functions configured and delivered as services over the Internet. From outside an organisation, this may be viewed as a shift of functions once performed by computers at the network’s edge (e.g. hosting software and data) into data centres in the network’s core. From inside the enterprise, the cloud allows the coordination and integration of applications and data operating on multiple machines into a seamless whole.

Below, we propose definitions of cloud services, cloud-hosted services and cloud enhanced services. These are neither original, fixed nor entirely distinct but are useful for the purposes of discussion. They can be used to refer to the services themselves or to the kinds of entities who provide them. These distinctions are familiar in the world of converged services, e.g. in relation to the distinctions among communications, information and data service providers; they have a range of intuitive meanings, but can be given precise legal expression when required.

- **Cloud services** are those used to provide access to computing resources and the computing resources themselves (e.g. storage, processing, etc. as technical capabilities). They tend to be provided by communications service companies and those who maintain and operate data centres and other physical assets used to provision cloud users’ service needs.

- **Cloud-hosted services** (sometimes called cloud-based) are the applications made available to users of cloud services. They overlap to a degree with cloud services – for example, data storage services can be provided in ways that more closely resemble a hard drive or a database application. They are often provided by entities that contract with cloud platform providers to meet users’ needs.

- **Cloud enhanced services** are those provided by users of cloud-hosted services, for example retailers who use cloud-hosted data services to manage their operations.

---

2 Mell and Grance (2010)

3 The vast cloud of classification schemes, starting with the NIST approach (Mell and Grance 2010) continues to evolve, so we have used the most common features.
Roles

The key players in the cloud landscape perform one or more distinct roles.

Cloud Service Providers host and manage the underlying infrastructure and offer different service models (e.g., SaaS, PaaS, IaaS - see below) to cloud-hosted service providers, cloud consumers, the cloud service brokers or cloud resellers. Cloud brokers and resellers can also act as “Cloud service providers.”

Cloud Service Brokers concentrate on the negotiation of relationships between consumers and providers without owning or managing the whole Cloud infrastructure. They may add extra services on top of a Cloud provider’s infrastructure to make up the user’s Cloud environment. In this sense, they can also act as cloud-hosted service providers.

Cloud Resellers: Resellers can become an important factor of the Cloud market as Cloud service providers expand across countries. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as “resellers” for their Cloud-hosted products in a particular region.

Cloud-hosted Service Providers develop software applications that they make available to other users of cloud platforms. In doing so, they may make use of cloud services such as storage, processing and virtualisation, in which sense they are also cloud consumers.

Cloud Consumers: End users belong to the category of Cloud consumers. However, Cloud Service Brokers, Cloud Resellers, Cloud-hosted Service Providers – and even Cloud Service Providers - can belong to this category as customers of another Cloud Service Provider, Broker or Reseller.

In addition to the definition shown above, NIST also refers to a model of five essential characteristics of cloud computing, three service models and four deployment models or usage scenarios, known as the “5-3-4 model”.

Essential or defining characteristics

The five essential characteristics of cloud services are:

- On demand self-service – the ability for the user to provision computing capabilities automatically
- Broad network access – capabilities that are available over the network through standard mechanisms (e.g. via IP).
- Resource pooling – the cloud provider dynamically pools and allocates computing resources (such as processing memory, network bandwidth) to offer to multiple users
- Rapid elasticity – capabilities can be rapidly and elastically provisioned to quickly scale up and down. These capabilities can appear to be unlimited

---

4 This classification draws heavily on European Commission 2010.
• Measured service – cloud systems possess a metered capability allowing resources to be automatically controlled and optimised.

Service Models

Cloud (and cloud-hosted) services are delivered to users in different architectures; these offer varying technological capabilities and business models. These differences are significant both for the eventual commercial and economic impacts of cloud computing and for the different ways in which power and responsibility are divided within them. The three service models identified by NIST are summarised as:

**Software as a service (SaaS)** – cloud consumers use applications supplied by cloud service and cloud-hosted service providers (and cloud service brokers) located on a cloud infrastructure available through various client devices, the most popular being a web-browser. The consumer has little or no control over the underlying cloud infrastructure.

**Platform as a Service (PaaS)** – cloud consumers, cloud-hosted service providers or service brokers can deploy their own or acquired applications using programming languages and tools supported by the cloud provider. They are able to control deployed applications and application hosting environment configurations.

**Infrastructure as a Service (IaaS)** – cloud consumers, cloud-hosted service providers or cloud brokers can provision processing, storage, networks and other basic computing resources and deploy and run arbitrary software including operating systems and applications. Although IaaS consumers do not manage or control the underlying infrastructure, they can control operating systems, storage and deployed applications and (to some extent) networking (e.g. host firewalls).

These models are illustrated in Figure 1: going up the vertical axis, abstraction increases and customer control decreases. In this figure, vertical integration refers to integration ‘up the stack’ from infrastructure through platforms run on that infrastructure to services delivered over the platforms. Horizontal integration refers to integration and interoperability within a given layer, e.g. among different SaaS offerings allowing for the ability to recombine or choose among different ‘modular’ services. From a market perspective, therefore, vertical integration involves takeovers, expansion or coordination along the computing value chain and horizontal integration refers to takeovers, expansion or coordination within layers of the value chain.
Figure 1: Three cloud service models

The extent of customer control is described in Table 1.
Table 1: End-user control under various delivery models

<table>
<thead>
<tr>
<th>Control over</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>(minor(^5))</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hosting environment</td>
<td>No</td>
<td>Possibly</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Operating systems</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Servers</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
</tr>
<tr>
<td>Network</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
</tr>
<tr>
<td>Cloud infrastructure</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Additional models now under development include the following:

**Hardware as a Service (HaaS)** – dedicated firmware accessible via the Internet e.g. XEN and VMWare; in effect this lets consumers obtain IT hardware, even up to the level of complete data centres, on a rapidly scalable and metered (pay-as-you-go) basis. In this case the user could acquire a data centre without actually having to invest in building one.

**Communications as a Service (CaaS)** – integrated or converged video, voice and data communications and associated services (e.g. VOIP, IP telephony offered to an SMB but provided by and owned by a third party data centre (Gartner, 2007), instant messaging, video conferencing, call recording, ) available from multiple devices.

**Deployment Models**

Cloud services provide users with a common platform for gaining access to shared cloud-hosted functionalities, services and applications. Some have their origins in the provision to a wider range of users of shared services formerly provided within large corporations; others arose specifically to address the needs of more-or-less homogeneous groups of users. It is therefore not surprising that they differ in terms of their openness or ‘deployment strategy.’ NIST identifies four deployment models for cloud computing:

**Private cloud:** the cloud infrastructure is operated solely for an organisation and may be managed by the organisation or by a third party and may be physically located within an organisation’s premises or offsite. Resources are provided to trusted users or customers via single-tenanted environment (technically, this means that each user has their own instance of the application or service involved); they are typically owned and/or leased by enterprise involved. Customers do not have direct access to functionalities; to them, this resembles Software as a Service. A consumer-facing example is provided by the eBay/PayPal transaction environment.

**Public cloud:** the cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services. These services are offered to multiple clients who want the advantages of shared-costs, elastic provision and

---

\(^5\) Basic user configuration settings only.
accountability\textsuperscript{6}. In public clouds, the distinction between user and provider may be blurred; both personal and enterprise users may employ cloud functionality supplied by others and/or offer their own services to other, external users. As platform services, public clouds are provided to all comers on open access terms but compared to other network utilities, they are (at the moment): more competitive, free of universal service obligations; and willing to offer a wide range of quality of service and pricing. Examples include: Amazon Elastic Compute Cloud (EC2), IBM’s Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

**Hybrid cloud:** the infrastructure is a combination of two or more clouds which remain unique but work together using technology that allows data and applications to move from one to the other. They are used in common by a restricted group of users. While firms can outsource significant parts of their IT infrastructure to others over public clouds, this often entails losing control over the resources used and the distribution, management and even the location of code and data. To achieve appropriate levels and patterns of control, hybrid clouds can be deployed using a mix of private and public cloud infrastructures.

**Community cloud:** the infrastructure is shared by several organisations and supports a specific community with similar or shared requirements, and participants offer a portion of their computing resources to a virtual cloud. Most public cloud providers offer their own infrastructure to customers; while they could resell other providers’ services or access to others’ infrastructure, they generally do not form large, cross-boundary aggregate infrastructures. In principle, local communities and SMEs could usefully combine their infrastructures to form community clouds. These can have a private or public character; Universities, SMEs or local community clouds could join together to build a private community cloud or resellers (e.g. Zimory) could pool different providers’ cloud resources for resale. Community Clouds are not very common although some initiatives have been started for research communities (e.g. CERN’s Research Grid, the UK’s National Grid Service (NGS), and the New Zealand Government Infrastructure as a Service initiative).

**General, economic and technical characteristics**

Cloud adoption and impacts can be linked to a range of general, economic and technical characteristics of this way of providing computing services.

**General (or ‘non–functional’) aspects\textsuperscript{7}**

*Elasticity*— clouds adapt to changing number and size of requests, and resource addition or removal;

*Reliability*— clouds sustain constant operation without disruptions (loss of data, code reset);

\textsuperscript{6} In a shared environment, accountability provides assurance of quality of service, privacy and other attributes,

\textsuperscript{7} See European Commission (2010) for a more extensive discussion and mapping.
Quality of Service (QoS) support – cloud computing can monitor and control many aspects of QoS from basic metrics like operation time or throughput to reliability and other computing and communications requirements.

Agility and adaptability – this is a ‘real-time’ version of elasticity in response to a wider range of changes such as power outages, network congestion and other changes that force alterations in the type of resources, quality of service, data routing. Typically, this implies a degree of autonomy for specific parts of the cloud;

Availability – cloud systems can (or should) provide continuous access without signs (including performance lags) of disruptions, changes in location or resources.

Economic Factors
Commercial prospects for cloud computing are strongly influenced by economic factors.

Cost reduction – Users face lower set-up, maintenance and updating costs, hardware changes, need for capacity investment and training. Data centres provide scale economies of operation and innovation (instant critical mass), security and hardware and support personnel human capital (also in terms of efficiencies of learning) amortisation.

Pay per use – this refers to flexible charging both for the quantity and composition of services and the appropriate amount of QoS or privacy, security and trust support, and to users’ freedom to substitute in-house alternatives.

Hardware, software and technology independence – users – even those developing and running their own applications (PaaS) or computing environments (IaaS) - can gain access to the cloud from a wide range of access devices, operating systems, software, etc. This can weaken the incumbency of many dominant hardware and software providers and increase cloud users’ choice among cloud providers at the same time.

Shorter time to market – both SMEs providing cloud-hosted services and larger firms can benefit by reducing the time and financial overhead associated with new offerings.

Return on investment – the costs of moving business operations to the cloud may be substantial and the costs of reversing the process even higher. Sustainable economic benefits may not be automatically guaranteed and the (perceived) reversibility of cloud adoption may be essential to efficient deployment.

Converting CAPEX to OPEX – this is frequently cited as an important economic advantage and thus a principal driver of cloud adoption by SMEs and households.

Technological Features
Finally, the implementation of the cloud depends on specific technological features that are important in assessing both the impacts of cloud deployment on citizens and consumers and the need for and efficacy of intervention.

Virtualisation means that a wide variety of computing environments (hardware and software) can be ‘simulated’ on the cloud. This ability to replicate a familiar environment hides the complexity of the cloud from users and increases flexibility, providing ease of use, infrastructure and location independence and adaptability;
Multi-tenancy means that different users share an instance\(^8\) of the same software, which serves their needs by partitioning the data so that they cannot see each other. It is distinguished from single-tenancy in which different users have dedicated copies of software, hardware, etc. and from virtualisation, in which software is used to provide a virtual simulation of a separate machine.

Data management procedures are especially important for storage and retrieval clouds, where data are flexibly distributed and accessed across a range of replicated resources. They control, for example, the location of data and the balancing of different customers’ demands for access and processing capacity.

With specific regard to multitenancy, recent discussions of the economics of the SAP Business byDesign cloud offer\(^9\) highlight specific economic implications. One is a ‘public good’ aspect: the software used to supply multitenanted users is common to all of them – if it goes down, they are all affected\(^10\). By contrast a problem affecting single-tenanted users is limited in impact. This does not necessarily lead to one-size-fits-all either; many ‘tenancies’ are highly configurable to make instances fit the needs of single users. Providing software in a single-instance multi-tenanted way allows many development, management and deployment costs to be distributed across the customer base, which in turn encourages providers carefully to address user needs in order to attract a sufficiently large group of tenants. The essential consumer issue is therefore the degree to which multi-tenancy aligns the interests of (esp. SaaS) providers and cloud consumers.

The exploitation of these features leads to a set of distinct advantages for business and personal cloud users as summarised in Table 2.

**Table 2: Business and consumer benefits**

<table>
<thead>
<tr>
<th>For business</th>
<th>For consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economies of scale, efficient capacity utilisation (pay only for what you use vs. average 30-40% utilisation of processing power) –use of shared facilities can mitigate ‘natural monopoly’ problems (predation by rivals with large IT facilities and low average costs) in non-infrastructure layers</td>
<td>Cheap or free services (sometimes ad-supported or beta versions)</td>
</tr>
<tr>
<td>Maximal incentives to innovate – immediate access to critical mass, limited risk of stranding</td>
<td>Mobility, ubiquity, panoply and convenience</td>
</tr>
<tr>
<td>More efficient competitive identification of good solutions since</td>
<td>Ease/speed of access</td>
</tr>
</tbody>
</table>

---

\(^8\) They use the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism.

\(^9\) This is an SaaS offering to businesses (see http://www.sap.com/solutions/products/sap-bydesign/index.epx) that made extensive use of multitenancy to address scalability issues that had limited market uptake (see http://www.zdnet.com/blog/projectfailures/sap-business-bydesign-taming-the-multi-tenant-beast/7302).

\(^10\) See Bardoliwalla et. al. (2009).
For business

rivals compete on a common platform for users with low switching costs, flexible sourcing

Rapid scalability, “OS neutrality” levelling computing playing field

Potential improvement in reliability and Quality of Service

For consumers

Latest/best functionality

Real time scalability

Market situation

There are a range of projections for the overall growth of the worldwide cloud market. Unless otherwise noted, all figures apply to worldwide markets (due to the difficulty of assigning users and providers in the cloud to specific locales). These consider a range of measures:

The importance of cloud services in overall IT spending (up to 10% in the short to medium term, according to IBM\(^\text{11}\));

Sales of cloud services across all deployment types (according to Gartner\(^\text{12}\), these were expected to grow 16.6% to $68.3 billion in 2011 and to more than double to $148.8 billion by 2014);

Revenues from enterprise public cloud services (according to Analysys Mason (2010), they will grow at a CAGR of 22.1% over the period 2012-2016, concentrated in already-developed markets)

Consumer use of cloud-hosted backup/storage sites (growing at 27.89% over the period 2009-2015, according to ABI Research).

Note that these figures do not include the unmonetised value of cloud services. This may be particularly important in relation to B2C services; according to ABI Research practice director Larry Fisher, “The consumer value proposition for many Cloud Computing applications is simple; they’re free. Most of the 1000+ US consumers responding to a 2010 ABI Research survey said they were hesitant to pay anything for use of a cloud-hosted service site.” The popularity of services free at point of use does not mean either that they are costless to deliver or that suppliers along the value chain are not paid for their efforts; instead, the market is producing a rich variety of alternative business models ranging from ad-supported services to services offered in exchange for personal information.

Market analysis also suggests a series of shifts among the different cloud deployment strategies. According to a recent North Bridge survey\(^\text{13}\):

---

\(^{11}\) IBM “Shift Happens” Chapter 4.

\(^{12}\) Gartner 2010 at: http://www.gartner.com/it/page.jsp?id=1389313
Private clouds serve 24% of current cloud users, of whom 27% plan to switch to hybrids within 5 years and 21% plan to switch to public clouds – top providers are VMware, Amazon, Microsoft, Rackspace, and Google;

Public clouds serve 37% of current users, of whom 42% plan to switch to hybrids within 5 years and 12% plan to switch to private clouds – top providers are Acquia, Cloudera, Assistli, Nasuni and Eucalyptus; and

Hybrid clouds serve the largest proportion (39%) of current users; none of these plan to switch to purely private or public clouds.

It appears that public clouds in the strict sense could gradually give way to a combination of private and hybrid cloud platforms, perhaps in response to evolving user needs (e.g. a preference for dedicated as opposed to shared software instances) and those platforms’ greater profitability for providers.

The cloud is growing in response to both consumer and business demands. While these may ultimately converge, at the moment B2B clouds are the most mature, and employ a mix of both architectures and deployment strategies, In contrast, B2C cloud computing centres around the SaaS architecture and the following services – figures are global user numbers and date of measurement:

Libraries (where content providers offer media for others to download): e.g. Lovefilm (1.5m, 2011), Netflix (23.6m, 2011) AND Spotify (10m, 2.5m paid, 2010).

Applications:
  - Hosted email is far and away the most popular cloud-hosted B2C service: e.g. Windows Live Hotmail (360m, July 2011), Yahoo! Mail (302m, August 2011), Gmail (193m, end of 2010).
  - Google Apps (unknown, claimed 25m, March 2010
  - Flickr (50m, 2011), Picasa (est. 0.5m, 2011)

Games: Castleville (33.6m, end 2011), Farmville (31.6m, end 2011), DRM elements of Steam (30m users, end 2011) – figures are monthly average users.

Online storage (where consumers can upload, store and access media they may ‘own’): Wikipedia lists 72 providers, including: iCloud (150m, 2011), Dropbox (25m, June 2011), SkyDrive (17m, October 2011), Amazon Cloud Drive, SoS online backup.

The report also considers a range of drivers, barriers and shaping influences on cloud adoption and performance, which are used to identify the regulatory issues.

Potential Issues and interests for telecommunications regulators

The report describes a range of issues of potential regulatory concern. To identify them, we have in mind a regulator whose remit resembles that of the Netherlands (OPTA) or the UK (OFCOM), though it should not be taken as a legally accurate description of either or a recommendation. The key elements are a combination of sector-specific and competition powers and a ‘converged’ view of the sector and its up- and down-stream connections.

As a result, the issues of most concern are aspects of cloud development that: threaten to harm specific consumer or citizen interests; are unlikely to be wholly resolved by market forces; and fit within the current remit of telecom regulators or could be considered candidates for an expanded role. Many of these are not original to the cloud, but are exacerbated or complicated by specific aspects of cloud development.

A second set of issues concern the implementation of potential solutions to cloud-related problems or raise general implications of the cloud for regulation rather than unique or direct harmful consequences of the cloud that telecom regulators can and should consider. They are discussed in detail in Chapter 4; the following table briefly summarises them in relation to the selection framework. A more detailed version of this Table is given in the main body in Chapter 4, prioritised according to the potential severity, immediacy, relevance to regulators and necessity of intervention. Because it is difficult to quantitatively measure or weight these factors, the issues are banded as High (shaded blue) Medium (shaded green) or Low (unshaded) priority.
Table 3: Overview of policy issues

<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Direct</th>
<th>Indirect</th>
<th>Extended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen and consumer issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer switching and mobility</td>
<td>Consumers may be tied to cloud service providers by limited portability of data and applications, restricted interoperability, lack of information</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
| Copyright and IPR                           | i) Questions over whether Cloud Service Providers may be liable for actions of users and hosted service providers;  
ii) Questions over ownership of user-generated content;  
iii) Concerns that content-matching services may serve to legitimise unauthorised content copying                                                                 | ✔      | ✔        | ✔        |
| Unfair and potentially anti-competitive contract terms | Standard form SLAs are efficient for large numbers of consumers but prevent bargaining. This raises switching costs and can lead to lock-in, damage competition or promote potentially anticompetitive market segmentation. More serious for cloud because providers ‘have’ user data. | ✔      | ✔        | ?        |
| Security, reliability, resilience capacity   | Concerns: a) transparency of cloud providers’ practices; b) security and reliability of services; c) data loss and unauthorised release - even when not illegal, this can create significant harm, especially when data owners are not aware; d) Data security includes e.g. infrastructure resilience (continuity), authentication. | ✔      | ✔        | ?        |
| Crime                                       | Users of cloud-hosted services may face an increased risk of a range of criminal threats: Identity, Data theft; Fraud; Malicious system, processing or data interference; Data loss or unauthorised release.                                           | ✔      | ✔        | ✔        |

D = Direct - cloud issues that affect communications value chain; I = Indirect – issues beyond communications sector affected by the regulated (communications services) layers; E = Extended – areas affecting regulatory objectives but requiring an extension of authority.
<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Consumer empowerment</th>
<th>Rating guidelines</th>
<th>Rating rationale</th>
<th>Remedies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Privacy may be weakened by indirect relationships with cloud-hosted service providers who hold personal data, limited visibility, obsolete legal roles, privacy-invasive technologies and business models.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ?</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Communications as a Service (CaaS)</td>
<td>Integrated or converged video, voice and data communications and associated services that overlap with existing regulated communications but are not limited to communications service providers. Policy issue: whether/how to regulate them.</td>
<td>✓ ✓ ✓ ✓</td>
<td>✓ D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising and marketing</td>
<td>Consumers may not be fully informed of what they sign up to; may see repeat of problems with e.g. broadband or mobile. Providers may be unable to certify, deliver or even inform consumers about the services they expect and those they receive.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud as a utility (including risk of market foreclosure)</td>
<td>Cloud computing share technical, economic and societal features with other utilities (e.g. scale economies, universal service potential). Policy issues: potential monopolistic foreclosure, social case for Universal Service (quality, affordability, open access) regulation</td>
<td>✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location and jurisdiction</td>
<td>Locations are hard to verify and constantly changing; this raises consumer protection and jurisdictional issues.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ?</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Locus of control</td>
<td>Difficult to identify points of leverage for effective intervention; existing regulation could be undermined by cloud-hosted alternatives that operate outside the regulatory sphere. Also, control is different in different architectures and deployment models.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>D, I, E</td>
<td></td>
</tr>
<tr>
<td>Consumer information, transparency of CSP practices</td>
<td>Linked to mobility, but important to other interests that depend on consumer choice, e.g. identity management, which is central to consumer choice and protection; if individuals cannot know or verify the identities of those with whom they transact, it may be hard to enforce rights Includes adverse impacts of unfair cloud contracts and advertising and marketing practices.</td>
<td>✓ ✓ ✓ ✓</td>
<td>✓ ?</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Issues</td>
<td>Description</td>
<td>Consumer empowerment</td>
<td>Business advantage</td>
<td>Market evolution</td>
<td>Rating</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Complexity of the cloud</td>
<td>The cloud’s inherent complexity and adaptability challenges conventional regulation.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>Certification and other self- and co-regulation</td>
<td>There are currently a variety of such ‘market-provided’ ways to address a range of concerns; may require national monitoring, and/or enforcement and/or be multiple, inconsistent, ineffective, costly, unmanageable, or anticompetitive.</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓</td>
<td>✓ Y</td>
<td>I</td>
</tr>
<tr>
<td>Cloud neutrality</td>
<td>Cloud should be OS, hardware, software. neutral; but this may be restricted for purposes of efficiency. As with net Neutrality, it is an empirical question whether non-neutrality is harmful and whether harmful non-neutrality can be countered.</td>
<td>✓</td>
<td>✓ ✓</td>
<td>✓ N</td>
<td>I</td>
</tr>
<tr>
<td>Consumer/SME similarities, regulatory heritage and convergence</td>
<td>In the cloud, both SMEs and users are potential cloud-hosted service providers therefore consumer harms thus occur in both B2B and B2C. A related issue is the ‘fit’ of communications, privacy, regulation with the cloud environment.</td>
<td></td>
<td></td>
<td>Potentially applies across the board</td>
<td>D</td>
</tr>
<tr>
<td>Trust</td>
<td>Security (esp. for firms, including SMEs) and privacy issues may reduce trust in cloud-hosted services, affecting their uptake; alternatively they may lead to “privacy/security as a service” innovations</td>
<td>✓ ✓ ✓</td>
<td>✓</td>
<td>✓ N</td>
<td>E</td>
</tr>
</tbody>
</table>
### List of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPU</td>
<td>Average Revenue Per User</td>
</tr>
<tr>
<td>Autonomic computing</td>
<td>where the IT environment manages itself based on perceived activity</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring your Own Device - the practice of letting employees choose the devices they wish to use for work within an organisational environment</td>
</tr>
<tr>
<td>CaaS</td>
<td>Communications as a Service</td>
</tr>
<tr>
<td>Co-location</td>
<td>the placing of customer owned equipment is placed in a data centre owned by a third party</td>
</tr>
<tr>
<td>CHSP</td>
<td>A provider of services hosted in the cloud</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>De-perimeterisation</td>
<td>a term for the evolving approach to consider measures beyond firewalls and Intrusion Detection Systems as sufficient to provide for security and where security must be applied consistently throughout the organisation instead of only at the edges</td>
</tr>
<tr>
<td>Elasticity</td>
<td>capacity to stretch and contract (in the specific context of cloud computing, to cope with demand)</td>
</tr>
<tr>
<td>Firmware</td>
<td>software embedded on a memory chip or device which has no end-user functionality</td>
</tr>
<tr>
<td>FRAND</td>
<td>Fair, Reasonable and Non Discriminatory</td>
</tr>
<tr>
<td>HaaS</td>
<td>Hardware as a Service</td>
</tr>
<tr>
<td>Homomorphic encryption</td>
<td>the ability to conduct processing on data without having to decrypt it</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>software that manages a number of instances of virtualised machines. For example, a hypervisor could run multiple operating system images on the same hardware.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>Latency</td>
<td>delay in message transmission</td>
</tr>
<tr>
<td>Managed Service Provider</td>
<td>a firm that manages a set of services on behalf of a client. A common example being IT support where the client does not have its own IT support team</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>the exclusion of the ability for the transmitter (human or machine) of a message to deny that they were the originator of the message</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PIPA</td>
<td>Protect Intellectual Property Act (United States)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a service</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SME</td>
<td>Small to Medium Enterprise</td>
</tr>
<tr>
<td>SoA</td>
<td>Service Oriented Architecture: the concept that instead of designing information systems in an organisation based around customised applications developed and hosted internally, such services (e.g. HR) are brought into the organisation</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol a protocol specification for the exchange of structured messages in web services</td>
</tr>
<tr>
<td>SOPA</td>
<td>Stop Online Privacy Act (United States)</td>
</tr>
<tr>
<td>USA PATRIOT Act</td>
<td>Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act</td>
</tr>
<tr>
<td>Virtualisation</td>
<td>the creation of a virtual (rather than actual version of something) such as an operating system, server or a storage device.</td>
</tr>
<tr>
<td>VNO</td>
<td>Virtual Network Operator</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>WS</td>
<td>Web Services</td>
</tr>
<tr>
<td>XaaS</td>
<td>Anything as a Service (where x represents a placeholder for an offered service or utility)</td>
</tr>
</tbody>
</table>
Despite the increasing prevalence of terms such as ‘cloud computing’ and ‘the cloud’ in the computing trade and scientific literature, there remains a wide range of competing views as to what actually makes up cloud computing. For example, Oracle’s CEO Larry Ellison commented in 2009 that:

‘The interesting thing about Cloud Computing is that we have redefined Cloud Computing to include everything that we already do’. He went on to say in the Wall Street Journal that ‘A lot of people are jumping on the [cloud] bandwagon... There are multiple definitions out there of “the cloud”’.15

Jonathan Weber from Time Online expressed similar sentiment, stating that ‘Cloud computing’ is a buzzword, ‘the concept, quite simply, is that vast computing resources will reside somewhere out there in the ether (rather than in your computer room) and we’ll connect to them and use them as needed.’16

From the perspective of many users, cloud computing involves the storage or processing of data in some dispersed and delocalised setting. The term originates from networking schematics which had a cloud as the representation of the Internet (or another network) beyond the parts of the network in focus. So another simplistic way to understand cloud computing is of ‘Internet based computing’.

1.1 Interpretations

The cloud may be defined in various ways. These differences are potentially significant; they reflect the perspectives of various stakeholders involved with the cloud, which may lead to coordination problems in identifying problems and implementing solutions. For the purposes of identifying the essential characteristics and important varieties of the cloud, however, it is useful to start with a definition current in policy circles proposed by the US National Institute of Standards and Technology (NIST) which discusses the now eponymous ‘5-3-4 model’. This consists of five attributes, four service models and three usage models. NIST defines cloud computing as:

15 Armbrust, Fox et al. (2009) p.3.
16 Gan and McMurray p. 4
“a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

The NIST definition very narrowly articulates the technological qualities of cloud computing but also recognises that cloud computing is not so much a technology as an approach or model encompassing a variety of aspects.

1.1.1 Essential characteristics and features

The five essential characteristics identified by NIST are:

- **On demand self-service** – the ability for the user to provision computing capabilities automatically
- **Broad network access** – capabilities that are available over the network through standard mechanisms (e.g. via IP).
- **Resource pooling** – the cloud provider dynamically pools and allocates computing resources (such as processing memory, network bandwidth) to offer to multiple users
- **Rapid elasticity** – capabilities can be rapidly and elastically provisioned to quickly scale up and down. These capabilities can appear to be unlimited
- **Measured service** – cloud systems possess a metered capability allowing resources to be automatically controlled and optimised.

1.1.2 Roles

The actors in the cloud landscape play a variety of roles. These are not separated; due to the complexity of the cloud value network, an actor (a specific firm) may play multiple roles at the same time.

**Cloud Service Providers** host and manage the underlying infrastructure and offer different service models (e.g., SaaS, PaaS, IaaS - see 1.1.3) to cloud-hosted service providers, cloud consumers, the cloud service brokers or cloud resellers. Cloud brokers and resellers can also act as “Cloud service providers.”

**Cloud Resellers, Brokers or Aggregators** aggregate cloud providers’ platforms to provide their customers with larger resource infrastructures or a wider range of enhanced features. This relates to community clouds (see 1.1.4) insofar as cloud aggregators provide a single interface to a merged cloud infrastructure. They can combine the economic benefits (see Section 2.1.1) of global cloud infrastructures with attention to local customer (esp. SMEs, individuals or community groups) needs by providing highly customised, enhanced offers that include access to applications in important industry sectors. This resembles the software and consulting industries; by connecting their customers into a “cloud ecosystem”, the aggregator can allow customers easily to identify emerging business models and computing needs, and to locate and exploit solutions provided by other customers. Conversely, customers who have such solutions can use the ‘ecosystem’ as a platform from

17 NIST
which to offer them on wider (e.g. global) markets. This role can be filled by a form of sectoral spread or diversification in which aggregators concentrating on one sector (e.g. education) serve their customers by reselling cloud services provided by cloud service providers tied to another sector (e.g. healthcare), leading eventually to mergers or acquisitions\textsuperscript{18}. Reselling may also act as a way for Cloud service providers to develop new markets, by choosing local IT consultancy firms or resellers of their non-cloud products to resell their Cloud-hosted products in a particular region. Cloud brokers also negotiate between providers and users of cloud services, but without owning or managing the whole Cloud infrastructure. They may add extra services on top of a Cloud provider’s infrastructure to make up the user’s Cloud environment\textsuperscript{19}.

**Cloud-hosted Service Providers, Adopters or (Software, Service) Vendors** enhance their own services and capabilities by using platforms supplied by cloud providers or cloud resellers. This enables them to e.g. scale their services to dynamic demands, which is of considerable value in contested markets and for start-ups who often cannot estimate the demand for their services. Their cloud enhanced or cloud-hosted services thus effectively become software as a service.

**Cloud Consumers or Users** make direct use of the cloud capabilities. Unlike cloud resellers and cloud adopters, they do not use the cloud to improve services and capabilities they offer to others, but instead use the storage, computing, communication functions and services to execute complex computations, host flexible data sets. At the moment, this role tends to be filled by private cloud users e.g. larger enterprises that outsource their in-house infrastructure (including high-performance computing) to reduce cost and delay and the risk of lock-in to outdated methods and technologies and by specialised communities such as game developers. In the future, this end-user role is likely to expand, esp. in the B2C area, and to converge as users combine the roles of provider and consumer (becoming “Prosumers). Cloud hosted email applications (such as Windows Live Hotmail or Google’s Gmail) are the two main cloud-hosted services used by consumers (as private citizens).

**Cloud Tool Providers** do not actually provide cloud capabilities, but provide or develop supporting tools such as programming environments, virtual machine management.

**Comment: clouds as two-sided markets**

Cloud consumers may use cloud services on their own and/or as a way of gaining access to cloud-hosted services. Therefore, these roles and distinctions can be related to the “two-sided market\textsuperscript{20}” view of networked cloud computing, according to which providers (of content, services, etc.) interact with their customers over facilities provided by third-party platform providers. In this context, the cloud service providers are the platform providers, the providers of cloud-hosted services play the role of one ‘end’ of the market (analogous to content providers or merchants) and the other ‘end’ consists of cloud consumers (providers

\textsuperscript{18} For example, Verizon’s reselling and subsequent take-over of Terramark and in the B2C space, both BT and Belgacom licensing the OnDrive games platform

\textsuperscript{19} For illustration, such a broker could build and offer an SaaS service to customers created on a cloud service provider’s PaaS or IaaS platform.

\textsuperscript{20} Weyl 2010
of cloud-enhanced services and other end users). This perspective highlights the fact that the market power of the platform provider (its ability to extract rents from its subscribers) derives as much from the gains from trade arising from the complementarity of cloud-hosted services on one side and cloud-enhanced services and other uses on the other as from the cloud services themselves. As a result, cloud service providers may subsidise or provide targeted services to encourage the presence on their platforms of specific cloud-hosted services in order to attract, retain and even lock in subscribers.

In Figure 2, the cloud service providers (CSP A-C) provide services to both providers of Cloud-hosted services (CHSP 1-3) and Cloud consumers (User i-l). These services (storage, virtualisation, etc.) are indicated by blue arrows pointing away from the CSPs. The Cloud-hosted service providers make their services available on the platforms (blue arrows pointing into the CSPs). Both CHSPs (e.g. CHSP 1) and consumers (e.g. User i) may use the cloud and cloud-hosted services they consume to provide cloud-enhanced services (black arrows). CHSP 3 and Users j and k are ‘multi-homed’ (they subscribe to more than one cloud service provider). The economic significance of this richness of ‘two-sided’ relationships derives in large measure from “indirect network externalities.” These are additional to the benefits of ‘one-sided’ relations between cloud consumers and cloud service providers, which allow cloud consumers to benefit from economies of scale, reduced CAPEX, continual updating etc. The ‘two-sided’ benefits of connecting to a cloud platform operated by a cloud service provider come from the opportunity to connect to others ‘over’ the platform – in particular to gain access to cloud-hosted services. This potential for connections creates positive externalities, because the demand for connections to the cloud is increased by the presence on a given platform of other CHSPs and consumers with whom one can interact. If these externalities are strong enough, the conventional analysis of service contracts must be modified as described below.
The cloud service provider may therefore serve two (or more) different types of subscriber. This creates a pair of issues: i) a chicken and egg start-up problem (CHSPs are attracted by Users and vice versa); and ii) a need to balance demand (making the service more or less attractive to one type of user will make it more or less attractive to other types as well). As a result, profit-maximisation suggests that one group will generally be treated differently than the other (even if the costs of serving them are the same) because it is more profitable to subsidise the most ‘attractive’ side of the market (even offering the cloud service for free) and to recoup any losses by charging the other side more for services and implicitly for access to the others.\(^{21}\)

1.1.3 Service Models

Cloud (and cloud-hosted) services are delivered to users in different service models - architectures that offer varying technological capabilities and business models. These differences are significant both for the eventual commercial and economic impacts of cloud computing and for the different ways in which power and responsibility are divided within them. The three service models identified by NIST are:

**Software as a service (SaaS)** – the cloud consumer uses the provider’s applications located on a cloud infrastructure available through various client devices; most commonly via a web-browser. The consumer has little or no control over the underlying cloud infrastructure. Examples include Gmail or SAP ERP\(^{22}\);

**Example: Google Docs** is a free Web-based office productivity service that allows users to create and edit documents (word processing, spreadsheets, and presentations) online. The service also creates opportunities for real-time collaboration with other users. While it is free to use 1GB of space on Google Docs, any additional space is priced at $0.25/GB per month. Documents are saved on Google’s servers with a revision history kept of past edits.

**Platform as a Service (PaaS)** – the cloud user can deploy their own or acquired applications using programming languages and tools supplied by the cloud provider. The consumer is able to exercise control over deployed applications and application hosting environment configurations e.g. Microsoft Azure, Force.com and Heroku (both owned by Salesforce.com), Engine Yard, AppFog, Mendix, Standing Cloud and Business ByDesign\(^{23}\);

\(^{21}\) This has specific implications for competition regulation, which we do not develop here, as they are familiar from other two-sided market contexts and because the current focus is on consumer rather than competition policy. We do briefly note that competition between platforms alters – but does not remove – asymmetric treatment of different types of subscriber. See e.g. Armstrong and Wright 2005 or Evans 2008.

\(^{22}\) There are far too many examples to give a definitive listing; the Gmail B2C offer can be found at mail.google.com and the B2B SaaS offer SAP ERP (formerly MySAP) can be investigated at: http://www36.sap.com/solutions/business-suite/erp/index.epx.

**Example: Google App Engine**

lets users build apps on Google’s scalable infrastructure. At its launch, commentators noted that: ‘What makes these offerings so interesting is their promise to turn enormous amounts of operational competency and accumulated economies of scale (which are enormous in Amazon’s and Google’s cases) into a highly competitive new software platform, akin to Windows or Linux, except entirely hosted off-premises and on the Internet.’ The engine supports app development in several languages and programming environments (Java, Python, Go). There are no start-up costs and the initial (freemium) allocation provides the storage, bandwidth and CPU power needed to serve 5 million page views/month. The Google AppEngine can be run on customers’ own hardware using the University-developed open-source AppScale application.

**Infrastructure as a Service (IaaS)** – the cloud user has the capability to provision processing, storage, networks and other basic computing resources and is able to deploy and run arbitrary software including operating systems and applications. Although the consumer does not manage or control the underlying infrastructure control can be exercised over operating systems, storage and deployed applications and possibly limited control over networking (e.g. host firewalls) e.g. Amazon Web Services, OpenStack (Rackspace), CloudStack (open source) and vCloud Express (VMware).

**Example: Amazon’s EC2**

the Amazon Elastic Compute Cloud (EC2), a ‘Web service that provides resizable compute capacity in the cloud. It is designed to make Web-scale computing easier for developers. Amazon EC2’s simple Web service interface allows users to obtain and configure capacity with minimal friction. It provides users with complete control of computing environment. Amazon EC2 reduces the time required to obtain and start new server instances to minutes, allowing users to quickly scale capacity, both up and down, as computing requirements change. Amazon EC2 changes the economics of computing by allowing users to pay only for capacity that they actually use.’

These are illustrated in Figure 3: going up the vertical axis, abstraction increases and customer control decreases. In this figure, vertical integration refers to integration ‘up the stack’ from infrastructure through platforms run on that infrastructure to services delivered over the platforms. Horizontal integration refers to integration and interoperability within a given layer, e.g. among different SaaS offerings allowing for the ability to recombine or choose among different ‘modular’ services. From a market perspective, therefore, vertical integration involves takeovers, expansion or coordination along the computing value chain and horizontal integration refers to takeovers, expansion or coordination within layers of the value chain.

---


The extent of customer control is described in Table 1.

Table 4: End-user control under various delivery models

<table>
<thead>
<tr>
<th>Control over:</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>(minor(^2^7))</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hosting environment</td>
<td>No</td>
<td>Possibly</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Operating systems</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Servers</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
</tr>
<tr>
<td>Network</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
</tr>
<tr>
<td>Cloud infrastructure</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Additional service models continue to be identified, including the following.

**Hardware as a Service (HaaS)** – dedicated firmware accessible via the Internet e.g. XEN and VMware; in effect this lets consumers obtain IT hardware, even up to the level of complete data centres, on a rapidly scalable and metered (pay-as-you-go) basis. In this case the user could acquire a data centre without actually having to invest in building one.

**Example: Xen\(^2^8\)** operates like a virtual machine monitor, able to provide services that allow multiple computer Operating Systems to execute on the same hardware concurrently. According to the company, an important benefit of the Xen Hypervisor is its neutrality to various operating systems.

**Communications as a Service (CaaS)** – converged\(^2^9\) communications and associated services (e.g. voice over IP, contact centre applications\(^3^0\), voice conferencing) available from

---

\(^2^7\) Basic user configuration settings only.


\(^2^9\) Hofstader (2007) defines converged communications as: “video; voice; and data; accessible over multiple devices – wire-line telephone; mobile or smart phone; and PC”

\(^3^0\) Including interactive voice responses (IVR), automatic call distribution (ACD), call recording, multimedia routing (e-mail and text chat) and screen pop integration.
multiple devices. The provider is responsible for hardware and software management and guarantees Quality of Service.

**Example: Cisco Messaging Interaction Center**[^31] a scalable integrated messaging and communications system offered to businesses, health care and higher education organisations which combines voicemail, data messaging, telephony[^32] voice over IP and other services with the customers’ email system[^33]. It requires little or no customer investment, can be scaled as necessary and is marketed in part as a way to simplify organisation transition to VOIP telephony.

### 1.1.4 Deployment models

Cloud services provide a common platform for gaining access to shared cloud-hosted functionalities, services and applications. Some have their origins in the provision to a wider range of users of shared services formerly provided within large corporations; others arose specifically to address the needs of more-or-less homogeneous groups of users. It is therefore not surprising that they differ in terms of their openness or ‘deployment strategy.’ NIST identifies four deployment models for cloud computing:

**Private cloud:** the cloud infrastructure is operated solely for an organisation and may be managed by the organisation or by a third party and may be physically located within an organisation’s premises or offsite. Resources are provided to trusted users or customers via single-tenanted environment (technically, this means that each user has their own instance of the application or service involved); they are typically owned and/or leased by enterprise involved. Customers do not have direct access to functionalities; to them, this resembles Software as a Service. A consumer-facing example is provided by the eBay/PayPal transaction environment.

At the enterprise level, 24% of current users of cloud computing are using private clouds. Out of these, 27% plan to switch to hybrids within 5 years and 21% plan to switch to public clouds – top providers are VMware, Amazon, Microsoft, Rackspace, and Google[^34].

**Public cloud:** the cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services. These services are offered to multiple clients who want the advantages of shared-costs, elastic provision and accountability[^35]. In public clouds, the distinction between user and provider may be blurred; both personal and enterprise users may employ cloud functionality supplied by others and/or offer their own services to other, external users. As platform services, public clouds are provided to all comers on open access terms but compared to other network utilities, they are (at the moment): more competitive, free of universal service obligations; and willing to offer a wide range of quality of service and pricing. Examples include:

[^31]: [http://www.inin.com/ProductSolutions/Pages/Messaging-Interaction-Center.aspx](http://www.inin.com/ProductSolutions/Pages/Messaging-Interaction-Center.aspx)
[^32]: Including VOIP, PBX, Centrex
[^33]: Currently, this works for Microsoft® Exchange Server, IBM Lotus Notes® and or Sun iPlanet™ Mail Server.
[^34]: Source: North Bridge 2011 survey (see footnote 12)
[^35]: In a shared environment, accountability provides assurance of quality of service, privacy and other attributes,
Amazon Elastic Compute Cloud (EC2), IBM’s Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

**Hybrid cloud:** the infrastructure is a combination of two or more clouds which remain unique but work together using technology that allows data and applications to move from one to the other. They are used in common by a restricted group of users. While firms can outsource significant parts of their IT infrastructure to others over public clouds, this often entails losing control over the resources used and the distribution, management and even the location of code and data. To achieve appropriate levels and patterns of control, hybrid clouds can be deployed using a mix of private and public cloud infrastructures.

| 39% of current cloud users employ Hybrid clouds; none of them plan to switch to purely private or public clouds. |

Not included in the classifications above, but of potential further policy interest, is another category much discussed in the trade literature:

**Community cloud:** the infrastructure is shared by several organisations and supports a specific community with similar or shared requirements, and participants offer a portion of their computing resources to a virtual cloud. Most public cloud providers offer their own infrastructure to customers; while they could resell other providers’ services or access to others’ infrastructure, they generally do not form large, cross-boundary aggregate infrastructures. In principle, local communities and SMEs could usefully combine their infrastructures to form community clouds. These can have a private or public character; Universities, SMEs or local community clouds could join together to build a private community cloud or resellers (e.g. Zimory) could pool different providers’ cloud resources for resale. Community Clouds are not very common, though some initiatives have been started for research communities (e.g. CERN’s Research Grid, the UK’s National Grid Service (NGS), the New Zealand Government Infrastructure as a Service initiative).

**1.1.5 Other perspectives**

Vaquero et al undertook a meta-analysis of 20 different definitions of cloud computing in 2009 and arrived at the following characterisation that cloud computing is:

“… a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and /or services). These resources can be dynamically re-configured to adjust to a variable load (scale) allowing also for an optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customised service level agreements.”

Still others have approached understanding differently. Berman (2008) talks about how cloud computing might be understood in one of two perspectives: an inside and outside based view. In the outside view, cloud computing shifts functions once performed by computers at the edge of a network (e.g. as nodes such as desktop PCs) to the core. Taking the inside view, cloud computing can ‘pull in’ data and applications from a range of

---

56 Source: North Bridge 2011 survey (see footnote 13)
57 Vaquero, 2009
locations (on the public Internet, for example) into one seamless whole. Berman’s interpretation in particular draws attention to characteristics such as the distinction between better performance of existing functions and new capabilities (the efficiency/effectiveness), the impact upon business models and organisational ecosystems (e.g. moving to a Service Orientated Architecture approach); faster, better, cheaper delivery of IT related goods and services and finally more effective relationship and information management.

**Technology in the Cloud: What is virtualisation?**

Virtualisation is a trend that highlights the creation of a virtual, rather than actual, version of something, for instance hardware platform, network resources, operation system, a storage device, among others. Virtualisation centralises administrative tasks while at the same time enabling greater resource utilisation and scalability.

The cloud can be decomposed in a wide variety of ways. The following figure from a 2010 European Commission Expert Group Report shows an overview of the main dimensions and aspects relating to Cloud Computing.

![Dimensions of the Cloud](image)

*Figure 4: dimensions of the cloud*

Source: European Commission (2010)

This figure illustrates the complexity of understanding the landscape since it includes a range of stakeholders, has differing features and benefits and can be compared to other relevant aspects of contemporary computing. The actors identified above are briefly discussed in the following sections.
1.2 **Actors, roles and revenues**

1.2.1 **Value chain diagrams**

A generic value chain diagram for cloud services is shown in Figure 5:

![Figure 5: Simplified value chain](image)

However, this is too simple for many purposes and may provide a misleading view of the relationships among the parties ‘homed’ in different stages, not least because many actors play multiple, non-contiguous roles. For instance, because cloud services are delivered over the Internet, various telecommunications value chain geometries may be embedded in (at a minimum) the “network connectivity and hardware” component or extend throughout parts of the value chain.

In addition, major players are not hard-wired to a particular role, service model or deployment model; rather, they tend to pursue a ‘cloud strategy’ that will, in turn, influence the network of market relationships within which they operate. From the perspective of identifying potential issues of regulatory interest, this suggests that a generic approach to understanding the implications of a particular firm’s activities may produce unexpected results, and that the effects of intervention may reflect or alter the extended value chain.

The available examples mix B2B and B2C cloud offers. As noted above, the B2B sector is currently smaller, but growing faster than B2C. It is not immediately obvious whether B2B offers towards SMEs will more closely resemble the B2C model than the B2B model of so-

---

38 Adapted from Williams (2011).
39 Huang and Hsieh (2011) indicate the evolution of cloud computing from its service model and technological antecedents and analyse the cloud strategy and value networks associated with some key players.
called ‘enterprise clouds.’ The B2C business model has specific implications for the value network as well; the expectations of the use of B2C cloud services based on the freemium model – free use (up to a certain point) supported by ads - suggests that third party advertisers (e.g. DoubleClick) and providers of aggregated analytics (e.g. Facebook) might also fit in the value network model for B2C usage. Moreover, the flexibility of business models means that different users engage with different subsets of this chain, directly or indirectly – for instance, if a cloud services provider evolves into a cloud hosted service or cloud-enhanced service provider, or if a major cloud consumer (e.g. a University outsourcing business processes like email to the cloud) evolves into a provider of cloud-hosted services (e.g. high-performance computing).

---

40 This is not just an historical accident – enterprise clouds – e.g. those used by banks and other financial institutions – tend to be far less concerned with issues of privacy and security, because the combination of legacy security solutions with a private cloud deployment model makes the likelihood and expected severity of security breaches far less, and provides (see discussion beginning on page 33) in addition the benefits of explicitly negotiated SLAs to manage these risks.
CHAPTER 2  Market situation

Having reviewed some of the basic concepts and models for cloud computing, we now turn to analysis of the market situation. We explore such issues such as what and where benefits appear, the degree to which it is possible to discern these being delivered (subject to currently available data), examples of estimates of the market size and drivers of growth, likely future growth and possible examples of changes in consumer behaviour.

2.1.1 Benefits and costs and their allocation along value chain

Some of the clearest articulations of the advantages of cloud computing have been focused on the business case for (B2B) cloud computing. In general they revolve around the proposition that firms making the ‘transition to the cloud’ no longer need to run their own IT departments. Organisations find cloud computing attractive because it allows them to reduce expenditure involved in operating the IT department something that is normally seen as a cost centre. Furthermore, the pay-as-you-go model means that not only do organisations not have to invest in capital intensive computing resources (such as servers) but they can also scale supply according to a metered basis, promising efficiency gains. Use of cloud services may have particular attractiveness for SMEs since it allows them to simply account for IT as another on-going, predictable cost, enabling them to focus on their main business model.\(^41\) Furthermore, some of the other inherent structural aspects may further facilitate innovation – such as how cloud computing renders opaque different elements (applications, services, processing, storage, memory networking capabilities) at different levels between SaaS and HaaS. Put differently it is not necessary to be familiar with all the intricacies of a low level operating system in order to build and deploy a production class application. Note: advantages for business users of cloud services include:

**Economies of scale, efficient capacity utilisation** (pay only for what you use vs. on average 30-40% utilisation rates of processing power) – note use of shared facilities can mitigate ‘natural monopoly’ problems in the non-infrastructure layers because small users have access to the same computing functionality as those able to invest in large-scale IT facilities (and may be less prone to IT obsolescence).

\(^41\) See Etro (2009) for a macro-economic study analysing the economic impact of cloud computing and its role in fostering business creation and competition to the reduction of the fixed costs of entry in ICT capital. Model calculations show a significant impact for the European Union with the creation of a few hundred thousand new SMEs.
Greater incentives to innovate – immediate access to critical mass, limited risk of stranding. Since companies can focus more on what is done with the IT rather than the ‘how’. Furthermore, the risk of investments being quickly outdated is minimised.

Efficient competitive identification of good solutions and flexible sourcing: since businesses can take advantage of using computing as a service, they can always take advantage of the ‘best in class’ of services. Furthermore, (subject to the discussion on lock-in) they can flexibly source services, perhaps selecting one cloud-hosted service to fulfil a particular need.

Rapid scalability, “OS neutrality” and levelling of the computing playing field. Outside the cloud, applications might require users to operate a specific operating system stack (combination of computing elements) or a specific mix of architectures (e.g. LAMP – Linux, Apache, MySQL and PHP/Perl/Python is a common mix). Applications developed for the cloud (offered as SaaS or run in a virtualised environment) do not tie users down in this way or oblige them to invest in acquisition, management and integration of these elements into their own computing environments.

Potential improvements over self-provided reliability and Quality of Service. Since cloud adopters are able to take advantage of economies of scale offered by cloud providers, there might be improvements possible with QoS and system reliability (as the cloud provider is likely to have significantly more resources dedicated to this compared to the average adopter or user).

2.2 General impacts

Aside from the specific customer orientated drivers identified above, the European Commission (2010) identified three types of general impacts: non-functional; economic and technological. These are analysed according to both the service models (XaaS) and deployment models (public, private, community, hybrid). Each of these types of impacts forms a key component of the adoption drivers identified above. We present these characterisations below, along with a description of their nature.

2.2.1 Non-functional

These are the impacts on the computing functionality available of the adoption of cloud computing

Elasticity – this involves the ability to adjust the computing resources to the demands made of it, including changes in the number (horizontal) and size (vertical) of service requests, and the ability to add and remove resources from the infrastructure⁴²;

Reliability – constant operation without disruptions (loss of data, code reset during computations), generally involving redundancy⁴³ (increasingly via software⁴⁴);

---

⁴² This resembles scaling, but has additional interoperability, stability and reliability requirements.

⁴³ Redundancy increases reliability by providing multiple copies of the same programme, so that failure can be bypassed and (if there are more than two copies) mistakes can be identified.
**QoS support** – runs the gamut from basic metrics like operation time, throughput, to systemic features like reliability and computing and communications requirements. QoS is often the subject of service-level agreements, but these rarely extend beyond cloud service providers to providers of cloud-hosted services. Like reliability, QoS is often associated with some form of redundancy; the use of multiple (n) data centres reduce odds of loss of access from r to r; the networking of these data centres in turn reduces latency\(^{45}\), which mostly depends on router queues;

**Agility and adaptability** – agile systems respond and adapt to changes in real time; compared to elasticity, it involves faster (and unplanned) changes and a wider range of perturbations. On the other hand, resilience and robustness refer to the capability of the system to avoid responding to shocks, or rapidly to resume its prior functioning. The shocks involved might be power or communication network outages, congestion or the failure of part of the hardware system, which might force alterations in the type of resources, quality of service, data routing. Typically, this requires a degree of autonomy;

**Availability** – related to reliability, this denotes the ability to provide continuous access without changing the user’s experience or giving signs (including performance lags) of disruptions. It also means that users will be unaware of changes in the location of storage and processing, in the resources used or in the way data and processing are shifted around to balance the load on the cloud provider’s resources

### Economic aspects

**Cost reduction** – this is certainly a major driver form recent adoption of cloud outsourcing for routine functions. In addition to reduced costs of excess (or obsolete) capacity, the flexibility of using cloud services can reduce the costs of adapting to changing consumer behaviour and reduce IT infrastructure maintenance and acquisition costs. This is not free, however, there are both set-up and continuing opportunity costs (for example increased overhead to manage Service Level Agreements) associated with adapting business operations and models to cloud use. More specifically, generic user cost advantages include: i) lower maintenance and updating cost; less frequent client hardware cycling; reduced need for end-user (spare) capacity investment. Data centres provide scale economies of operation and innovation (instant critical mass), security and physical and human capital amortisation. Additionally, in public clouds the aggregation of demand can diversify away risks of under- or over- capacity utilisation but may magnify systemic risks of e.g. technological choice.

**Pay per use** – this refers not only to the elasticity (see above) aspect of cloud services (especially under usage-based or two-part tariffs) but also to the ability to purchase as much (or as little) QoS or SPT support as needed, and to substitute in-house alternatives where appropriate – providing SLAs are sufficiently detailed and flexible. The shift of IT provisioning from up-front costs to on-going purchases of state-of-the-art services is one of

---

\(^{44}\) This means shifting from duplicate hardware e.g. RAID (redundant arrays of inexpensive hard drives) to duplicate software (redundant file systems).

\(^{45}\) This depends on the ‘dimensionality’ k of the network connecting the data centres: it takes \(2^k\) links to halve the average distance.
the key economic aspects of the transition to cloud services; the same shift can provide much more rapid feedback on the real value to users of specific services and lower the costs of experimentation, increasing both the pace and the benefits of innovation.

**Hardware, software and technology independence** – because computer services are purchased on an as-needed basis, users are better able to economise on investments in physical, IT and even human and organisational capital; this weakens the incumbency of many dominant hardware and software providers.

**Shorter time to market** – this is particularly important for SMEs providing cloud-hosted services and those providing IT-intensive services to outside markets, supported by cloud-hosted services; they can avoid the delay and cost associated with IT infrastructure acquisition, set-up and training. Larger firms can also benefit by reducing the time and financial overhead associated with new offerings;

**Return on investment** – this is increasingly important in the current financial climate; despite healthy revenue figures, however, the trade literature often asserts that some cloud systems do not pay for themselves in the short run (due to e.g. excessive adjustment costs) – this does not prevent their adoption as part of a general trend, but does suggest that sustainable economic benefits may not be automatically guaranteed. A related issue is the appropriate level of return to infrastructure providers, especially the large Telco’s providing the physical infrastructure, who must cope with increasing demands for bandwidth and other service characteristics, but who are also in a position to capture for themselves some of the benefit created by the provision and use of cloud-hosted services, especially for high-value services. An inefficient allocation of costs to ISPs and cloud service providers may distort architectures, deployment scenarios or lead to adverse compensating forms of price and/or QoS discrimination;

**Converting CAPEX to OPEX** – this is frequently cited as an important economic advantage and thus a principal driver of cloud adoption by SMEs and households. The evidence is mixed (see Figure 8); moreover, while minimising CAPEX can improve balance sheets by reducing expenditures with delayed payoffs, cash-rich firms (as at present) may welcome inside investment opportunities. CAPEX can also improve balance sheets by relocating costs to future years, especially when capital costs are low (lower internal ROIC controls). Note also that Cloud service provider savings come from CAPEX, not OPEX, while Cloud users reap OPEX savings from scalability;

**Environmental performance** (energy use and carbon footprint)

On the provider side, additional economic benefits come from demand mixing and sharing - data centres may have higher minimum efficient scale (the level of operations at which average costs are minimised); moreover serving a mix of variable demands may be more efficient than serving the same aggregate volume coming from a single source (the variance of a sum is less than the sum of the variances).

---

46 A form of the ‘Loser’s Curse or excess volatility as noted by Katz and Shapiro.

47 This argument assumes imperfect correlation, which may reflect competitive sorting of providers.
However, these returns are not infinite. Public cloud providers have to charge a risk premium, so big firms may prefer their own clouds; serving their own demands may not in itself serve to smooth the excess capacity problem if their demands are correlated, but they could pair up with other firms, especially if sharing and re-use of large data sets or apps is valuable.

Other economically valuable benefits include ubiquity of [Internet] access, ease of collaboration, possible privacy benefits (from the collective provision of privacy protections), management and learning benefits for data centres and a reduced need for end-user IT management.

2.2.3 Technological aspects

**Virtualisation** – this hides the complexity of the cloud from the user and increases flexibility. It provides ease of use, infrastructure independence, flexibility and adaptability and location independence);

**Multi-tenancy** – users of cloud services typically do not know (and may not care) where data or code are located; conversely, the same resources (even the same data) may be used by multiple users (even at the same time). This has implications for both infrastructures and the data, applications and services hosted on shared resources but provided to multiple isolated users. This raises a raft of technological (e.g. how to deal with simultaneous provision of ‘the same’ data to multiple users while the data are being altered, as in Google docs), data protection, and ‘ownership’ issues.

**Security, privacy and trust**

- Security typically refers to achieving confidentiality, integrity and availability of information and can also entail authentication and non-repudiation;

- Privacy involves both legal and non-legal norms (e.g. data protection regulations), but can be framed by globally accepted privacy principles: i) consent, ii) purpose restriction, iii) legitimacy, iv) transparency, v) data security and vi) data subject participation. It relates to the cloud in part because personal data and logs of computing activity are stored in the cloud, and their processing or use may be at odds with user knowledge, control or societal or legal norms of privacy;

- Trust, a somewhat intangible concept, involves users’ ‘assurance’ and confidence that data, information or processes will function as expected. It can take many forms in the cloud: humans trusting humans; machines trusting machines; humans trusting machines; and machines trusting humans. The necessary trust of the cloud user in the providers of cloud and cloud-hosted services must be matched by their trust in users, especially when they bear potential legal or market liability. Appropriate trust cannot directly be provided, but should result from progress towards security or privacy objectives.

Note: this set of issues can be extended from storage and communication to processing and computation. A critical issue concerns transitivity – if a user trusts a cloud service provider,

---

48 This refers to the applicability of economic and legal rules predicated on exclusive ownership or access.
and the cloud service provider trusts the vendors whose services are hosted on his cloud, it
does not necessarily follow that the user can (or should) trust the vendor. As a result of
limited accountability and visibility and the sheer complexity and pace of change of cloud
services, Security, Privacy and Trust can get lost in the cloud, can keep important players
out of the cloud and can even pollute the cloud; however, the attention these issues receive
and the potential for “Security, Privacy and Trust as a Service” innovation may make these
issues the silver lining as well.

**Data management** – this is particularly important for data storage and retrieval clouds,
where data are flexibly distributed and accessed across a range of replicated resources; their
consistency must be maintained, and the system may need to be aware of data location
(e.g. to manage latencies and variations in workflow demand) even when users are not.
Data management must also address issues of variable data sizes and format, backwards
compatibility and consistency guarantees.

**Enhancements to programming and applications programming interfaces** (APIs) –
these permit developers to benefit from the cloud environment by pushing common
aspects ‘up the stack’ – in other words, while many common programming models require
developers to manage scalability and autonomic capabilities (e.g. self-configuring, self-
optimising, self-healing and self-protecting) themselves, a cloud environment provides
these features in a fashion that allows developers and other users to leave such management
to the system. This is particularly important for ‘opening up’ development to a wider range
of participants (e.g. end-user ‘prosumers’);

**Metered use** – Much of the attraction of the cloud is that users pay only for what they use,
and to scale up or change the services they receive as their needs evolve. Metering the use
of a wide range of resources and services is necessary to enable the required flexible pricing,
charging and billing, which is itself needed to create scalable and elastic clouds;

**Reusable tools** for cloud service development, adaptation and use, following the build-
onece, use-many-times model of object orientated software development, the existence of
re-useable tools for cloud service development (e.g. the Google Apps Engine environment)
is an important technological consideration.

### 2.3 Related Technological and Internet Trends

As we saw in Chapter 1, there are some related areas that share some of cloud computing’s
characteristics or use similar underlying technologies. They include the Internet of
Services[49] and the Internet of Things, grid computing and service-orientated architectures.

**Internet of Things**

The Internet of Things (IoT) is what many have termed the next logical step in the
evolution of the Internet.[50] In the IoT model, everyday objects (through the use of Radio
Frequency Identification and almost limitless IP addresses) can become part of the

[49] We do not discuss this explicitly; see Li et. al. (2008).

[50] Cave et. al. (2009)
Internet, having an online ‘address’. Common examples in the Ambient Intelligent Environment (AmI) include fridges, lights, walls etc. although many use cases have been identified (for example, a refrigerator that can communicate with the grocery store to keep foodstuffs updated) some of these futures still remain visionary. The IoT is related to cloud computing because clouds indirectly offer the capability for the vast quantities of real-time data from sensors and RFID equipped devices, made available by IoT, to be processed, matched up and correlated in new ways.

### The Internet of Things

In addition to music, IT and telecoms industry, a growing sector that is getting fully integrated into the Internet of Things is the car industry. In-vehicle internet access is close to becoming widely adopted. A survey by KPMG looking at future trends shows speech recognition and internet connection with Wi-Fi and 3G will become the norm. More than a third (37%) of the 200 car executives believe ‘infotainment’ in cars is nearly as important as car safety.51 In addition, road safety can be enhanced by real-time allocation of road-space based on processing of car location data, made possible by a combination of Internet based location based services, high performance computing, widespread coverage of high bandwidth wireless networks and cloud-based processing.

The opportunity for physical objects to be easily identified, linked and communicated also enables creative outcomes in other industries, including 3-D printing (additive manufacture) of objects of that people create, draw and realise.52 By using 3-D printing, people can ‘create real, solid objects from digital data by building them up in layers... to create rapid prototypes’.53 Moreover, 3-D printing ‘encompasses a range of technologies – from inkjet heads mounted on gantries that can deposit plastics layer by layer to form intricate models, to more recent laser-based systems that combine metal powders to make durable parts of airplanes’.54

Finally, there are the possibilities afforded by automatic object identification (such as RFID, Near Field Communication and visual markers), ubiquitous connectivity and the use of sensors and GPS data to achieve other social and economic goals. New interfaces linking the physical and digital worlds offer opportunities and innovations to an extent previously unknown.55 By bringing them into people’s daily lives, they inform (and are likely to change) individual and collective decision making in real time. For example by utilising data collected via RFID, consumers can calculate an individual item’s carbon footprint to inform purchase decision making.56

The salient point is that these technologies (from nanotech to cloud computing) become integrated into technological systems; this systemic view provides a consistent basis for analysing the broader economic implications of the cloud.

---

54 See http://www.technologyreview.com/computing/39437/page1/55
55 See Kranz et al (2010).
Grid computing

The phenomena of grid computing is regarded as one of the underlying building blocks of cloud computing. In particular, advances in the development of hypervisors which can manage many instances of virtualised operating systems with high levels of reliability and availability, represent a cornerstone development in cloud computing offerings. Grids refer to a network of computing resources (usually highly homogenous) controlled by a hypervisor that can be used to conduct distributed parallel processing on a wide scale. Grid computing can be seen in a number of computing applications that have captured media interest, including the search for extra-terrestrial life (SETI@home) and computational analysis of protein folding in the search for a cure for cancer (Folding@home). Such applications use spare processing cycles to allocate to computationally intensive tasks, often co-ordinated by highly robust virtualisation software. They often require the installation of a specific client or software on the host machine. The growth in technological sophistication of components (particularly Video Processing Units used to render images and corresponding Video RAM) means that graphics processors can also be used as part of a grid infrastructure.

Service Orientated Architectures

Finally, SoA (Service orientated Architectures) constitute another important but related development. Building from the Object Orientated software development model, SoA takes the idea of ‘build once-reuse many times’ to the organisation. In the O-O model, coders would design building blocks of software to undertake one function. Then, instead of developing software to do the same thing, these could be re-used in other parts of the application. Soon these were placed online, giving any one the chance to use the snippets of software, provided the input and output parameters were known (i.e. the language the software object spoke was known). SoA takes this model and applies it at the organisation level: instead of creating a HR system, for example, this is simply ‘bought in’ as a service. For cloud computing, SoA has got organisations used to being more familiar and comfortable with contracting or buying in services rather than building them in a bespoke fashion.

2.4 Market size and growth (highlights from industry projections)

There are a host of consultant and industry projections concerning the size and growth of aspects of the cloud services market. These cover the range of types of cloud offering but at present mainly focus on the B2B sector. We describe some indicative examples of forecasts and projections below.

57 Link to SETI@home
58 Link to folding at home
59 In 2011 graphics processors were available with similar amounts of RAM as might be installed and made available to the entire computing bus. To see the application of GPU’s to breaking encryption see https://media.blackhat.com/bh-dc-11/Roth/BlackHat_DC_2011_Roth_Breaking_encryptions-wp.pdf
2.4.1 Business to Business (B2B) domain

Estimates of the size of the market proliferate in the Business to Business (B2B) sphere. One possible reason is that B2B constitute early adopters – another is that there is greater call for such market analysis. It may also be that B2B cloud offerings are easier to define. Finally, there is an argument, noting the evolutionary nature of these developments, B2C cloud applications have been in existence for some time and there are already market estimations for Internet hosted email for example. There are wide differences in these predictions, however. Some argue that existing economic situation is driving organisations to adopt cloud computing on the basis of pressures on efficiency. Others suggest that the situation is so poor that any investment in ICT is being deferred until better economic times.

IBM say\textsuperscript{60} that cloud service spending will grow to 10% of all IT spending in the short to medium term.

Telecommunications research firm Analysis-Mason produced annual forecasts that not only provide a breakdown according to value chain roles but also show a progressive upgrading of the forecast as the recession takes hold. According to their 2010 worldwide forecast for enterprise cloud services:\textsuperscript{61}

\begin{quote}
“The global market for enterprise cloud-hosted services will grow from USD12.1 billion in 2010 to USD35.6 billion in 2015 (see Figure 0.1). The year-on-year growth rate will be 43% in 2011, but will decrease to 13% over the next five years. Software-as-a-service (SaaS) will account for 70% of revenue in 2010, while 30% is related to infrastructure-as a service (IaaS). PaaS is not covered. This revenue split will change over the next five years, with IaaS’s share increasing to 40%. By 2015, registered IT and application partners – such as one-tier agents, two-tier agents, systems integrators (SIs), dealers and direct market resellers (DMRs) – will account for 39% of this end-user-generated revenue. IT and application vendors will generate 36% of the revenue, either through web-based sales or dedicated account representatives. Fixed and mobile telecoms operators, and cable TV operators, will take a 23% share, and managed service providers (MSPs) will account for the remaining 2% of enterprise cloud-hosted services revenue.”
\end{quote}

\textsuperscript{60} IBM “Shift Happens” report, Chapter 4

The firm further indicated in a 2011 forecast that the main driver is enterprises’ increasing confidence in the concept of cloud computing. Year on year growth of 40% between 2010 and 2011 was expected to slacken between 2012 and 2016. Most of the growth was estimated to come from developed markets, accounting for 90% of the total enterprise public cloud services revenue. The worldwide revenue from enterprise public cloud services was estimated to grow from USD$12bn in 2010 to USD$40bn in 2016, a Compound Annual Growth Rate (CAGR) of 22.1%.

---

63 Analysys-Mason (2010).
64 Analysys-Mason (2011)
According to Gartner\textsuperscript{65}, worldwide B2B Cloud service sales were expected to grow 16.6% to $68.3 billion in 2011 and to more than double to $148.8 billion by 2014.

Finally, according to a 2010 survey of US consumers by ABI Research\textsuperscript{66}, revenue related to consumer use of cloud-hosted backup/storage sites will grow from almost $75 million in 2009 to more than $372 million in 2015, at a CAGR of 27.89%. According to ABI Research practice director Larry Fisher, “The consumer value proposition for many Cloud Computing applications is simple; they’re free. Most of the 1000+ US consumers responding to a 2010 ABI Research survey said they were hesitant to pay anything for use of a cloud-hosted service.”

From this, we can see that B2B computing generates a fraction of the revenues currently produced by B2C cloud computing, but is likely to grow much faster.

2.4.2 Business to consumer cloud services

While Business to Business (B2B) uses are the most mature, and employ a mix of both architectures and deployment strategies, Business to Consumer (B2C) cloud computing currently centre upon SaaS architecture and involves a range of services, encompassing library type services (accessing content offered by a cloud provider), applications (like web hosted email) and storage. Because some telecom regulators have a specific mandate in this domain, we go into further detail of B2C cloud offerings.

Examples of cloud-hosted services include those that allow you to access libraries of content from the cloud. Popular examples at the moment include Lovefilm, Netflix, Spotify, and Amazon’s Kindle e-Book service. Each normally allows the storage and cataloguing of acquired content with delivery via the Internet (either streaming or via download). Very often such services will include an element of synchronisation to keep content up to date across different devices. This is becoming increasingly sophisticated with the possibilities for services such as Apple iTunes Match to extend iTunes’ synchronisation by cataloguing user-owned content and providing licensed copies across different devices (whether the original was legitimately or illegitimately acquired).

The growth of web-hosted email reflects the complexity of understanding what cloud computing is. Although web-based email has been around for some years, it is a clear example of a cloud hosted service.

Table 5 below indicates some recent usage figures for three of the most popular Internet hosted email services: Windows Live Hotmail, Yahoo! Mail and Gmail.

<table>
<thead>
<tr>
<th>Provider</th>
<th>Users</th>
<th>Date</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Live Hotmail</td>
<td>360m</td>
<td>Jul 2011</td>
<td>Official Microsoft blog</td>
</tr>
<tr>
<td>Yahoo! Mail</td>
<td>302m</td>
<td>Aug 2011</td>
<td>Independent data quoted by Yahoo!</td>
</tr>
</tbody>
</table>

\textsuperscript{65} Gartner Group (2010)

\textsuperscript{66} ABI Research (2010).
Other notable cloud-hosted services include photo sharing websites where users can upload, edit, store and share photos or media. Examples include Flickr (50m users) and Picasa (0.5m users). Still more types of popular cloud-hosted applications in the consumer domain include games: perhaps the most well-known is Farmville, (which runs on the Facebook platform). Other such applications such as Soundcloud, an online audio distribution platform that allows users to upload audio with a distinct URL (as opposed to e.g. Youtube or Myspace) for purposes of collaboration, promotion and distribution. Further examples include those that are a combination of storage, licensing, and community – Steam with its 30m users is perhaps the pre-eminent example. Steam may be considered as a licensing as a service application in addition to allowing the consumer to purchase, store and download games. Other less well known applications include consumer ‘information management’ (e.g. Evernote, which allows the user to keep track of notes across a range of devices) financial software (e.g. Quicken Online) and password keepers. Splashup, Picasa Web Albums, Photoshop Express and Jaycut are cloud-hosted applications that can handle photo and video editing tasks.

Storage is generally seen as currently one of the most compelling cloud-hosted services on offer to individual consumers. Examples of storage services include Apple’s iCloud, Dropbox, SkyDrive, Amazon’s Cloud Drive, and SoS online backup. These services offer either unlimited or for a fee limited space ranging from 25GB (Sky Drive) to 2GB (Dropbox) with further capacity (e.g. up to 100GB with Dropbox) available for a fee. In general although each of these services does ‘storage’ each has its strengths and weaknesses: some have a better implementation of syncing or others like Amazon’s Cloud Drive are claimed to be more suitable for playing music (Cloud Drive is regarded as a support service for its Cloud Player service).

---

67 39m active users in mid July 2011
68 5m registered users (2011)
69 Steam is a social networking service that allows digital distribution of games (much like Direct2Drive and GamersGate) but also allows users to connect and play, providing cloud-hosted ‘licensing as a service’ – by the end of 2011 it had 30M users, representing 178% growth year-on-year, and hosted 1200 games Up to 6M users play each day, with as many as 3M playing simultaneously. The company has had substantial sales growth as well, driving considerable infrastructure expansion to meet user demands for bandwidth.
70 Up to 150m users in 2011 (Gartner)
71 25m users in June 2011 according to Wired
The breadth and variety of consumer services or applications is indicated in Table 6: 

Table 6: Examples of consumer cloud services.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox</td>
<td>A multi-platform, multi-system data sync software.</td>
</tr>
<tr>
<td>Facebook</td>
<td>The largest social network web application/service (over 750M users).</td>
</tr>
<tr>
<td>Twitter</td>
<td>The largest micro-blogging service for consumers (and businesses)</td>
</tr>
<tr>
<td>SmugMug</td>
<td>App for storing and sharing images, with user-customisable galleries and printing &amp; framing options.</td>
</tr>
<tr>
<td>Aviary</td>
<td>Online image editor</td>
</tr>
<tr>
<td>Onlive</td>
<td>Delivery of games via the cloud.</td>
</tr>
<tr>
<td>Hulu</td>
<td>US-based broadcast TV content store.</td>
</tr>
<tr>
<td>Netflix</td>
<td>Online movies and TV shows.</td>
</tr>
<tr>
<td>Groupon</td>
<td>Social shopping service.</td>
</tr>
<tr>
<td>Grooveshark</td>
<td>Music library with free access and optional paid subscription.</td>
</tr>
<tr>
<td>Evernote</td>
<td>Data sync tool compatible with multiple platforms using a note and notebook concept to organise notes and data (including images, files.).</td>
</tr>
<tr>
<td>Sliderocket</td>
<td>Presentation web app that outperforms desktop versions.</td>
</tr>
<tr>
<td>Penzu</td>
<td>Online personal journal and online diary.</td>
</tr>
<tr>
<td>Threadsy</td>
<td>Converged email and social media app.</td>
</tr>
<tr>
<td>Yelp</td>
<td>Reviews of all kinds - 41 million users as of December 2010.</td>
</tr>
<tr>
<td>Office 365</td>
<td>Cloud subscription version of Office that starts at $6 per user a month.</td>
</tr>
<tr>
<td>Google Apps</td>
<td>Competitor to Office 365, sold to businesses for $50 per user per year.</td>
</tr>
<tr>
<td>Cloud Drive</td>
<td>Web-based storage service on Amazon’s secure servers.</td>
</tr>
<tr>
<td>iCloud</td>
<td>Converged service offering: iTunes in the cloud (music, video), Contacts, Calendar, Mail, Photos; Apps, Books, Documents; and Device backup</td>
</tr>
</tbody>
</table>

According to a KPMG survey of 9,600 consumers in 31 different countries, consumers in the UK are more reluctant to embrace the cloud with 53% reported saying that they use cloud-hosted storage solutions compared to 65% globally.

In the same survey, 48% expressed high concern about security and privacy. A similar percentage (51%) expressed concern about their ability to retrieve data from cloud services.

In the United States, the Pew Internet and American Life Project surveyed American consumer attitudes to cloud computing in 2009. This found that 69% of online Americans use webmail services, store data online or use software programs. This survey also identified that many consumers are using cloud computing without necessarily being
aware of it. Table 7\textsuperscript{72} from the findings indicate the popularity of some different types of activities amongst Internet users.

<table>
<thead>
<tr>
<th>Activities</th>
<th>% of Internet users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using webmail services such as Hotmail, Gmail or Yahoo! mail</td>
<td>56%</td>
</tr>
<tr>
<td>Store personal photos online</td>
<td>34%</td>
</tr>
<tr>
<td>Use online applications such as Google Documents of Adobe Photoshop Express</td>
<td>29%</td>
</tr>
<tr>
<td>Store personal videos online</td>
<td>7%</td>
</tr>
<tr>
<td>Pay to store computer files online</td>
<td>5%</td>
</tr>
<tr>
<td>Back up hard drive to an online site</td>
<td>5%</td>
</tr>
</tbody>
</table>

This survey also identified the drivers for those Internet users reportedly using cloud computing:

- Ease and convenience are seen as a major reason by about half of respondents (51%)
- 41\% of cloud users say that an advantage is being able to access their data from whatever computer they are using
- 39\% cite the ease of sharing information as a major reason to use applications or store data

<table>
<thead>
<tr>
<th>Activities</th>
<th>18-29</th>
<th>30-49</th>
<th>50-64</th>
<th>65+</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is just easy and convenient</td>
<td>56%</td>
<td>52%</td>
<td>50%</td>
<td>37%</td>
</tr>
<tr>
<td>I can access this information from whatever computer I am using</td>
<td>51%</td>
<td>42</td>
<td>34</td>
<td>19</td>
</tr>
<tr>
<td>I can easily share information with others</td>
<td>45%</td>
<td>38</td>
<td>39</td>
<td>27</td>
</tr>
<tr>
<td>I won’t lose this information if my computer fails</td>
<td>35%</td>
<td>35</td>
<td>34</td>
<td>18</td>
</tr>
</tbody>
</table>

\textit{Source: Pew Internet & American Life Project April-May 2008 Survey. N=1,553 Internet users. Margin of error is +/- 3%}

Conversely, users surveyed by the Pew study reported high levels of concern when confronted with scenarios involving uses of their data.

\textsuperscript{72} \textit{Source: Pew Internet & American Life Project April-May 2008 Survey. N=1,553 Internet users. Margin of error is +/- 3%}
• 90% of users say they would be concerned if the company holding their data sold it to another party;
• 80% say that they would be concerned if companies use their photos or other data in marketing campaigns;
• 68% of users say that they would be very concerned if companies providing these services analysed this information and then displayed ads to them based on their actions.

2.4.3 Growth drivers and barriers
What may drive the uptake of cloud computing in the future? Whilst predictions of technology enabled developments are very difficult to do, it is possible to identify some broad trends, relating to both innate technological developments, the outlook for B2B shifts and socio-economic changes which may serve to drive or stifle uptake. These trends illustrate a combination of enablers (common infrastructures) and trends that require or will use cloud computing for their continuation (e.g. utility computing). We present these in an illustrative fashion, by way of pointing out some related strategic aspects of how the technology landscape may evolve.

On the technology side, in a futures based study, four clusters of technology related trends have been identified (Cave et al, 2009). These could affect the uptake of cloud services amongst companies and consumers alike. The first two are clearly directly related to the perception and inherent qualities of cloud computing as described in the sections above, but here we reflect upon the broad strategic implications of these characteristics.

Development of a common communications infrastructure (based around common standard protocols such as IP)– which can be accessed through different devices and technologies, removing sources of exclusion and discrimination, allowing supporting technologies such as social networking or Twitter to ‘draw in’ new people and uses and put them in greater touch with one another. Technologies that are directly associated with this trend are: increasing bandwidth; increasing processing power and performance; Increasing electrical power and performance. Related technological development are the increase of internet capacity (transition from IPv4 to IPv6).

Evolution towards computing as a ubiquitous utility – one aspect is to increase the general availability and benefits of computing by putting it on the same footing as water, power and telecommunications. It also demonstrates the degree to which ‘merely quantitative’ advances on processing, storage, develop qualitative transforming power precisely by being interconnected through the network. In addition, access to utility computing creates new demands for connectivity and reduces digital divides associated with differences in access to computing and storage. The mobilisation of shared computing resources seems likely to shift asymmetric ‘client-server’ forms of connectivity (see text box example) towards a more symmetric set of peer-to-peer relationships. The underlying technologies associated with this trend are: increasing digital storage capability and decreasing cost per byte; faster computation; evolving computer architecture; grid computing; cloud computing; XaaS. Related technological developments are: open source software; more internet capacity.
Changing the client-server relationship: the CHP example. Typically, energy distribution networks connected a few large generators from a much large group of consumers. Management of the network lay in the hands of the grid operator, who balanced the flows and kept the network in operation by ensuring the generators were ready to meet whatever demands were made. Therefore, both the generation of power and the operation of the network favoured generators over users. With the advent of user-operated generating capacity and ‘Smart Meter’ tools for active demand management consumers (and communities) can become significant generators, actively contribute to network management and bargain more effectively with suppliers. There are two connections to cloud computing: first, ‘community’ management of power demand and supply is beginning to use the cloud to collect and share information and to forecast demand and supply for individual users; second, cloud brokerage and community clouds link together users’ resources in an exactly analogous way, letting cloud users become cloud suppliers and letting them take an active role in managing network traffic.

The convergence of humans and computers - making both the machine and human ‘ends’ of the network smarter changing the need for active traffic monitoring and management in the network itself and producing new geometries of power and control – for instance, the degree to which the end-to-end principle still implies that the network will not take an active role in traffic prioritisation, etc. On the other hand, the electronic enhancement of human experience (e.g. via new input and output interfaces.) creates a potential need for social connection – in the same way as advances in stand-alone platform-based computer games laid the foundations for today’s on-line gaming and associated social networks, we might anticipate the growth of cloud-hosted extensions of these models. Technologies that are directly associated with this trend are: increased deployment of nanotech; cognitive computing; cybernetics, specifically cybernetic organisms; immersive virtual environments; decreasing size and increasing capability of embedded sensors. Related technological developments are: cheaper, faster and smaller RFID technology; more tools for personal identification and authentication; immersive virtual reality environments.

The emergence of the Intelligent Web: describing the deployment of existing technologies providing ‘intelligence’ to the protocols, structures and internal functions of the Internet itself, rebalances responsibilities and contributions of different stakeholders to overall socioeconomic impacts and creates a powerful ‘pull’ factor for further technological, economic, financial and social innovation. Technologies that are directly associated with this trend are: convergence of applications; more, easier and better creating & sharing tools; Web 3.0 tools. Related technological developments are: localisation of applications; decreasing size and increasing capability of sensors.

Again, turning to B2B predictions of what will drive demand (which are more prevalent than B2C predictions), the 2011 North Bridge survey (see footnote 13) of US based enterprise cloud users shed light on the current attitudes.
10% of the sample regarded clouds as too risky ever to use
26% were waiting for cloud services to mature
40% were using clouds on an experimental or pilot basis;
11% were using clouds to handle spikes in demand on their in-house and/or directly outsourced IT infrastructures; and
13% had fully adopted the cloud for mission critical services and functions.

Within this group, drivers for adoption in the near future follow the following pattern:

Figure 8: Drivers of cloud adoption

This indicates that innovation, competitive pressures, data and service mobility (access from anywhere) and more sophisticated use of cloud computing (cloud application programming interfaces (APIs)) will become increasingly important. These are potentially interesting from a policy perspective; in particular, innovation produces new uses and raises new concerns; mobility is already regarded as a significant challenge in location-based regulation (esp. privacy) and more sophisticated uses (and movement from SaaS to PaaS and IaaS) will change the way ‘consumer’ harms are identified and dealt with.

The same survey measured the barriers inhibiting adoption by the 36% not currently experimenting with or using cloud services:
We stress that these data apply to business users and enterprise cloud services. However, there is some overlap with consumer interests, not least because the boundaries between consumers and business users are not sharply drawn in public clouds. These data indicate that some consumer issues are already creating barriers to cloud development; lock-in and interoperability limit consumer mobility and raise switching costs. But broader ‘citizen’ issues such as privacy and security are also important, though they are more concerned with the way the market delivers value than the operation of the market itself. However, as B2B cloud computing is growing faster than B2C uses\textsuperscript{73}, the balance among these weights will change.

### 2.4.4 Demand-side shifts

It is possible to identify some broader socio-economic shifts which may affect the demand for cloud computing, and which may in turn shape its evolution. We highlight some of these in detail\textsuperscript{74}, starting at the broad level.

**Increasing mobility** is one aspect, particularly with respect to the move away from tertiary or manufacturing based economies to urban city dwelling and service based economies (driving reliance upon technology as a key element of the production of wealth). It increases demand for location- and platform-independent cloud services. However, this is a broad socio-economic change which drives many different facets of ICT uptake, not specifically cloud computing.

**The increasing portfolio nature of work** is a second shift; for example, knowledge workers no longer stay with one firm or career during their working life but move more rapidly among different jobs in the same or different careers. As a result, mobility of data

---

\textsuperscript{73} See Section 2.4.1

\textsuperscript{74} For further information on the B2B aspects see. IBM “Shift Happens” report: https://www-304.ibm.com/easyaccess1/fileservlet?contentid=214791
and reducing sunk investment of data creation (and setting up appropriate IPR arrangements) will become more important.\(^{75}\) This will build demand specifically for crowd-sourced employment services like Amazon’s Mechanical Turk and Fiverr where the Internet can efficiency facilitate bringing together supply and demand. A related shift factor originating on the demand side comes from the increasingly blurred boundary between the professional and private spheres. The increasing use of telework and remote working by post-urbanised, knowledge based economies in Western Europe and North America and the Far East might affect and drive preferences for citizen/consumers to be able to shift their information, business contacts or intellectual property between these two spheres and between different jobs in their career portfolio, which builds demand for interoperable storage and processing services provided over public (or at least B2C-orientated) clouds.

**Implications for the erosion of B2B and B2C boundary\(^{76}\)**

Although consumer protection rules place B2C relationships on a different footing than B2B relationships (even for very small enterprises), the boundary may be eroding. Some B2C services are already being used for B2B (e.g. marketing on Facebook and Youtube) and B2C services will increasingly adopt features demanded by B2C users (e.g. agility, mobility) and vice versa (e.g. trust and security). Moreover in the current economic climate, citizens may use the cloud for start-up ‘self-employed’ activity:

i) Self-employed people building businesses on cloud-hosted business process outsourcing;

ii) Self-employed people setting up as cloud-hosted service providers or app developers (thus inducing more cloud, broadband, telecommunications demand from their clients); and

iii) The creation of cloud portals for connecting micro enterprises with potential partners and clients, including the possibility of creating new forms of virtual enterprise or ‘electronic enterprise zones’ or hybrids in which large firms can supply managerial and ICT-related services over the cloud without dominating the supply chain.

In relation to enterprise cloud service adoption, there is a potential for an arms race\(^{77}\) leading to over- or under-investment in cloud hosted capabilities. This arises in part from network externalities\(^{78}\). More sectors and firms have to make full use of cloud-hosted capabilities to enhance their services and to serve geographically dispersed markets, regardless of whether this delivers value to those firms or customers. Firms who follow the trend may contract for resources or surrender control over their data and ICT operations

\(^{75}\) http://www.guardian.co.uk/commentisfree/2012/jan/22/self-employment-proper-jobs-cameron?!NTCMP=SRCH

\(^{76}\) Some see the distinction between B2B and B2C clouds as indicating an explicit and specific contract as opposed to a standard-form SLA; others see this as a distinction without a difference (Verstraete 2012).

\(^{77}\) See e.g. Temple (2002).

\(^{78}\) Katz and Shapiro (1994)
with little commercial return; others may lose market share. For example, adoption of CaaS (see 1.1.3) allows firms to provide automated contact centre facilities, which may be taken as a marker even when those facilities are under-utilised, in the same way that back-office automation and website creation have in some cases ‘overshot.’ On the positive side this may reduce the costs of entering this arms race and thus the costs of failure or expansion, thanks to cloud scalability and ‘pay-for-what-you-use’ contracts;

The possibilities afforded by ubiquitous broadband networks coupled with app based ‘data mashing’ (the publication, matching and cross referencing of previously disparate large public interest data sets) might afford opportunities for **citizen engagement in the political or democratic process.** Although a relatively indirect link this is certainly one that is being taken up by the Open Data movement (e.g. see data.gov). In turn, there are opportunities for greater bottom up engagement in the broad process of governance;

Conversely, these induced changes in cloud adoption and provision can trigger changes elsewhere in the economy, which can in turn affect the relative attractiveness of cloud vs. non-cloud services by altering the price and performance of e.g. communications services. Growth in consumer demand for cloud services may lead to **increased demand for bandwidth,** possibly heightened awareness of privacy, or increased demands for continuity of access, with an accompanying slightly smaller increase in demand for security. This might lead to further changes in the timing and sensitivity of consumer broadband demand; to a certain extent this can already be seen with the ‘smartphone revolution’ and sale of 3G/3.5G spectrum. The extent of this will reflect the balance between costs of high speed access to storage held on the cloud and the (currently very high) prices of home storage capacity possessing comparable levels of resilience and reliability.

Other behavioural or social changes may also affect cloud-hosted services (either inhibiting or enabling their use):

**Changing attitudes to personal and public spaces.** In a narrow sense this is contained within the current discourse on personal data protection, but also concerns the familiarity and ease which consumers of the future have with online public spaces. Current philosophical thinking for example of Victor Mayer-Schonberger discusses the ways in which there are evolving expectations of privacy (whether that is to the extreme that many technologists often claim that ‘privacy is dead’).

**Perceptions and attitudes to information:** namely that the sheer volumes of information being produced, along with the ubiquity of the means to access it has perhaps created an expectation that content (by which a consumer might understand as information) should be free, further challenging the existing legal frameworks concerning licensing and copyright protection. Although there is some limited contradictory evidence to this (e.g. some music content creators releasing work for free and asking consumers to pay what they think it is worth) on the whole this might exacerbate the shift from revenues being generated from the distribution of content to the ‘experience’, further challenging existing intermediary business models. For example, it is already possible to observe how many performance artists regard revenues from live performances to be more lucrative than the distribution of recorded work. This hurdle to subscription-based content provision services that may make low-priced cloud options more attractive.
More specific aspects include (Dziri; 2011 and HP Corp, 2009):

Increased consumer uptake of cloud-hosted services may also strengthen B2C use of CaaS offerings; this can affect demand for and the economic viability of conventional and in this case even Internet-based voice telephony. For example, by way of further evidence, recent surveys describe how the myriad of communication capabilities evolve over time (Comscore, 2011) teenagers were using email less and less compared to SMS and IM. This is an effect of the availability of converged cloud-hosted communications services, but will trigger shifts in the communications market that may either reinforce the emergence of CaaS as an important B2C cloud service or – by squeezing the margins of telecommunications firms and ISPs providing other forms of VOIP – limit the communications and Internet services on which clouds rely.

Demand for content storage may alter the level, effectiveness and market impact of copyright (and IPR more generally) enforcement activity. Content stored in data centres might be easier to search and monitor than in home machines (but obviously requires a presumption of guilt). This might also apply to law enforcement (witness Google’s Transparency Report metrics of numbers of law enforcement requests per country).

There may be a shift in consumer demand away from simple SaaS (e.g. email) to cloud-hosted services further linked down the ‘stack’ (e.g. PaaS). This is consistent with the rise of the ‘prosumer’ and the general labour market changes described above (e.g. rising cloud-facilitated self-employment). This can already be seen in the popularity of cloud-hosted storage services. This increased demand for storage services strengthens the business case for offering high performance storage and processing on a shared services basis. This in turn may contribute to changes in the market for home software and hardware in the direction of the ‘thin-client’ model; the home market will become more competitive on the basis of price rather than features and the markets for different end user devices (e.g. smartphones, tablets, PCs) will increasingly overlap. Of course, the resulting increase in shared processing-intensive services creates additional security and privacy issues.

We may witness a further levelling of the playing field as regards social media creation and participation in cloud hosted social networks; giving everyone access to industry standard processing power through cloud-hosted service might trigger new waves of user led innovation. These innovations would be facilitated by the rising functionality of cloud services and (planned) increases in high speed broadband access. As a result, existing controls on businesses offering social media and social networking may be bypassed. This applies to e-commerce as well; the availability of cloud hosted data and software may increase the speed, sophistication and volatility of a wide range of online markets (including financial markets).

Consumer sophistication in the use of cloud-hosted services may shift the architecture of cloud computing services from SaaS to PaaS, where users create their own applications and where, in consequence, the cloud provider is less able to control the resulting functionality, risks. This could raise consumer protection and empowerment issues if users lack the information and understanding needed to make these choices or if their use of these resources creates new privacy risks. On the other hand, increasing use and availability of PaaS tools for application creation might extend and deepen the so called app market – one of the most important and dynamic elements of the mobile communications sphere.
CHAPTER 3  The threshold for regulatory interest

‘In the end, the convenience, reduced upfront costs, and impressive scalability offered by the cloud computing model will have to be balanced against the users’ expectations of data control, data flow and disaster recovery requirements.’ Wittow and Buller (2010)

Given what is known about cloud computing, why are regulators interested? Drawing on the UK example, the Communications Act 2003 stipulates:

**Ofcom’s Role**

”3(1) It shall be the principal duty of Ofcom, in carrying out their functions;
(a) to further the interests of citizens in relation to communications matters; and
(b) to further the interests of consumers in relevant markets, where appropriate by promoting competition”

Ofcom’s specific duties fall into six areas:

- Ensuring the optimal use of the electro-magnetic spectrum
- Ensuring that a wide range of electronic communications services – including high speed data services – is available throughout the UK
- Ensuring a wide range of TV and radio services of high quality and wide appeal
- Maintaining plurality in the provision of broadcasting
- Applying adequate protection for audiences against offensive or harmful material
- Applying adequate protection for audiences against unfairness or the infringement of privacy”
3.1 **Regulatory mandate in respect of cloud computing**

The framework used includes both citizen and consumer interests, but in ways that only indirectly involve what is most often noted about the cloud. In the UK case, the cloud primarily affects Ofcom’s first two specific duties.

Access to the cloud – and particularly mobile access– has specific characteristics that affect spectrum utilisation overall. The importance of this is shown by the urgency attached to the spectrum scarcity impact of new services and devices in the current UN International Telecommunication Union (ITU) World Radio-communication Conference.79

The societal importance of the wide availability of high speed broadband data services is likely to be magnified by their use to gain access to cloud-hosted storage and processing.

Cloud-hosted content delivery may complement or compete with broadcast content distribution, possibly raising issues of harmful or offensive material, unfair treatment or invasion of privacy. This can be seen simply in terms of content delivery, but probably goes beyond this to involve the communication needed to gain access to this content – not least because the hosts are not necessarily in a position to control (or even verify the legality of) such content80 and because access to this content may be used in other markets (e.g. providing data repository and retrieval services or using them to manage supply chains)81.

3.2 **Framework for understanding the implications**

These issues may be organised according to a simple, consumer-orientated framework82. We draw on the UK example because it represents one of the more profound examples of converged regulation83 and therefore tends towards the outer limits of what is currently possible – and thus provides a relatively future-proof basis for classification.

1. **Is there consumer or citizen harm**84?

   **Citizen harms** include (Ofcom 2010):
   
   - Do the development of cloud services and cloud-hosted services affect citizens’ *access to critical telecommunications services*?

---


80 This was an issue in the recent shutdown of Megaupload ([http://www.megaupload.com/](http://www.megaupload.com/)) by the US Department of Justice, with the consequent loss of users’ stored material.


82 This draws upon Ofcom’s Draft Annual Plan (Ofcom 2011a) and Statutory Duties (Ofcom 2003).

83 For a comparative analysis of the implications of convergence, see

84 the classes of harm derive from Ofcom’s consultation documents and consumer policy
To what extent does Cloud Computing affect or impinge upon the information and skills needed for participation in society?

Does the development and uptake of cloud computing create or exacerbate general citizen protection risks e.g. to the functioning of other critical infrastructures, national security, disaster recovery, emergency management?

Specific consumer interests include (Ofcom 2006 and 2011b):

- **Benefits of competition** in and through communications markets for consumers (including SME users of cloud services and cloud-hosted services) via improved technical and allocative efficiency, cost, quality and innovation;

- **Consumer protection** from financial and physical harm, unreasonable annoyance and anxiety (anti-fraud, critical QoS, privacy, security); and

- **Consumer empowerment** in the form of access to the information and tools necessary to make informed choices (transparency, accountability).

2. Is ‘the market’ likely to mitigate or eliminate this harm? Are there in existence examples where the market is providing solutions or something that at least meets an identified or articulated need?

3. Does the area fit within the regulator’s current remit (do they have the necessary tools e.g. regulatory obligations on suppliers, consumer information services, assistance to switching, compliance monitoring and enforcement)? Generically, these tools comprise:

- **competition policy**: ensuring that competition policy takes sufficient account of consumer interests and behaviour;

- **consumer protection**: protecting consumers against financial and physical harm, unreasonable annoyance and anxiety; and

- **consumer empowerment**: equipping consumers to obtain the best deal.

4. Is new intervention required? This is the last test along what may be considered a logical thread: if the implications affect either citizens (as users of telecommunications services) or consumers but if the market does not appear to be providing a solution (or the solution is ineffectual) and if the area fits within the regulator’s current remit it might be worthwhile to consider some kind of future regulatory intervention (which may or may not include legislation).
CHAPTER 4  
Policy concerns

4.1  Introduction

This chapter analyses a list of issues and concerns mentioned in the literature against the framework set out above. These (intentionally) reflect a mixed bag of 'things to consider'. Some are ‘issues’ that can easily be identified with very specific consumer and/or citizen ‘harm’ and which qualify for consideration because they appear to fall within current regulatory remits or to impinge directly on areas of existing intervention. Other ‘implementation’ concerns are more diffuse, comprising aspects of the cloud that affect the severity or tractability of known issues, indicate new challenges or opportunities in addressing them or overlap with – but go significantly beyond – current remit and jurisdiction. They are briefly summarised in Table 8 and Table 9 and discussed in more detail below. In these Tables, the final column refers to the match with common regulatory remit: D = direct - cloud issues that affect communications value chain; I = indirect – issues beyond communications sector affected by regulated communications services; and E = extended – areas affecting regulatory objectives but requiring an extension of authority. These are prioritised according to the potential severity, immediacy, relevance and necessity of intervention. Because it is difficult to quantitatively measure or weight these factors, the issues are banded as High (shaded blue) Medium (shaded green) or Low (unshaded) priority.
### Table 8: Citizen and consumer harm issues

<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Access</th>
<th>Participation</th>
<th>Citizen protection</th>
<th>Competition</th>
<th>Consumer protection</th>
<th>Consumer empowerment</th>
<th>Existing regulation</th>
<th>Market solution?</th>
<th>Remit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer switching and mobility</td>
<td>Consumers may be locked into cloud service providers by limited portability of their data and applications, restricted interoperability, lack of information</td>
<td></td>
<td></td>
<td></td>
<td>Ability to switch</td>
<td>Information on competing services</td>
<td>Telecom and broadband switching</td>
<td>N</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Copyright and IPR</td>
<td>i) liability of Cloud Service Providers for actions of users and hosted service providers; ii) ownership of user-generated content; iii) content-matching and legitimisation; etc.</td>
<td>Access to knowledge</td>
<td>Ownership of user-generated IP</td>
<td>Supply of content, (vertical) lock-in of IPR</td>
<td>Threats from pirated content</td>
<td></td>
<td>Anti-piracy</td>
<td>N</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Unfair and potentially anti-competitive contract terms</td>
<td>Standard form SLAs are efficient for large numbers of consumers but prevent bargaining. This raises switching costs and can lead to lock-in, damage competition, reduce efficiency. More serious for cloud because providers ‘have’ user data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security, reliability, resilience capacity</td>
<td>Concerns: a) transparency of cloud providers’ practices; b) security and reliability of services; c) data loss and unauthorised release - even when not illegal, this can create significant harm, especially when data owners are not aware; d) Data security includes e.g. infrastructure resilience (continuity), authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issues</td>
<td>Description</td>
<td>Access</td>
<td>Participation</td>
<td>Competition</td>
<td>Consumer protection</td>
<td>Consumer empowerment</td>
<td>Existing regulation</td>
<td>Marked solution?</td>
<td>Result</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Crime</td>
<td>Range of criminal threats: i) Identity theft; ii) Data theft; iii) Fraud; iv) Malicious system, processing or data interference; v) Data loss or unauthorised release.</td>
<td>Vulnerability of cloud</td>
<td>Depend on cloud for security, safety</td>
<td>ID theft, data loss, fraud.</td>
<td>Identifying trustworthy services</td>
<td>Legal proscriptions may not bind cloud (hosted) services</td>
<td>N</td>
<td>E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy may be weakened by indirect relationships, limited visibility, mismatch with legal roles, privacy-invasive technologies and business models.</td>
<td>Data protection</td>
<td>Indirect monetisation of personal data</td>
<td>Privacy rights; data release may damage interests</td>
<td>Lack of necessary information</td>
<td>DPA, breach notification</td>
<td>? (privacy by design, certify.)</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications as a Service (CaaS)</td>
<td>Integrated or converged video, voice and data communications and associated services that overlap with existing regulated communications but are not limited to communications service providers.</td>
<td>Potential unfair competition</td>
<td>Bypass</td>
<td>?</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud as a utility (including risk of foreclosure)</td>
<td>Aspects of cloud computing share some technical, economic and societal features with other utilities (e.g. economies of scale and potential for universal service)</td>
<td>Universal service</td>
<td>Economies of scale, interoperability</td>
<td>Quality of Service</td>
<td></td>
<td></td>
<td>N</td>
<td>E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising and marketing</td>
<td>Consumers may not be fully informed; may see repeat of problems with e.g. broadband or mobile. Providers may be unable to certify, deliver or even inform consumers about the services they expect and those they receive.</td>
<td>Misleading adverts, unreliable QoS</td>
<td>Possibly BPRs (2008), CPRs (2008).</td>
<td></td>
<td></td>
<td></td>
<td>N</td>
<td>I</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 9: Implementation and related issues

<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Citizen related</th>
<th>Competition</th>
<th>Consumer protection</th>
<th>Consumer empowerment</th>
<th>Existing regulation</th>
<th>Market solution?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location and jurisdiction</td>
<td>Locations are hard to verify and constantly changing; this raises consumer protection and jurisdictional issues.</td>
<td>Location changes may shut down essential services</td>
<td>Ability to switch locations may provide cost advantages</td>
<td>Data loss in unprotected locales</td>
<td>Cannot know where data reside</td>
<td>Not harmonised</td>
<td>?(certified location)</td>
</tr>
<tr>
<td>Consumer information, transparency of CSP practices</td>
<td>Linked to mobility, but important in other areas where interests depend on consumer choice, e.g. identity management, which is central to consumer choice and protection; if individuals cannot know or verify the identities of those with whom they transact, it may be hard to enforce rights.</td>
<td>Authentication</td>
<td>Limits consumer sovereignty, function of reputations, accountability</td>
<td>For electronic communications service providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locus of control</td>
<td>Difficult to identify points of leverage for effective intervention; existing regulation could be undermined by cloud-hosted alternatives. Also, control is different in different architectures and deployment models.</td>
<td>Lack of direct accountability</td>
<td>Inter-platform competition</td>
<td>Migrating from SaaS to PaaS; Liability failures</td>
<td>Hard to negotiate with cloud-hosted service providers</td>
<td>May need to regulate cloud providers; change regulation of communications providers</td>
<td></td>
</tr>
<tr>
<td>Complexity of the cloud</td>
<td>The cloud’s inherent complexity and adaptability challenges conventional regulation.</td>
<td>Consumers may not understand choices</td>
<td></td>
<td></td>
<td></td>
<td>May miss self-organisation, difficulty of decisions</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Citizen related</th>
<th>Competition</th>
<th>Consumer protection</th>
<th>Consumer empowerment</th>
<th>Existing regulation</th>
<th>Market solution?</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification and other self- and co-regulation</td>
<td>Market-provided’ solution for a range of concerns; may require national monitoring and/or enforcement and/or be multiple, inconsistent, ineffective, costly, unmanageable, or anticompetitive.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Varies</td>
<td>Co-reg.</td>
<td>I</td>
</tr>
<tr>
<td>Cloud neutrality</td>
<td>Cloud should be OS, hardware, software. neutral; but this may be restricted to support discrimination.</td>
<td></td>
<td>Vertical restraint</td>
<td>walled gardens</td>
<td>Bypass</td>
<td></td>
<td>N I</td>
<td></td>
</tr>
<tr>
<td>Consumer/SME similarities, regulatory heritage and convergence</td>
<td>In the cloud, both SMEs and users are potential CHS providers; consumer harms thus occur in both B2B and B2C. A related issue is the ‘fit’ of communications, privacy, regulation with the cloud environment.</td>
<td></td>
<td>Untrusted services not used</td>
<td>Does market treat trust failures efficiently?</td>
<td>Reliance on cloud services</td>
<td>Potentially applies across the board</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>Security (esp. for firms, including SMEs) and privacy issues may reduce trust in cloud-hosted services, affecting their uptake or leading to “privacy/security as a service” innovations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N E</td>
<td></td>
</tr>
</tbody>
</table>
4.2 Citizen and consumer harm issues

In this section below we discuss issues of potential citizen and consumer harm (in line with the scheme in Chapter 3 and in the priority order used in Table 8) arising from or exacerbated by the cloud, and potentially lying within regulatory remit. We also consider the extent to which the market or other parties are likely to address the issue.

4.2.1 Limits to consumer switching and mobility

The current lack of cloud service standards/interoperability and cloud service provider policies could lock-in consumers or restrict their ability to mix and match data and services hosted on different clouds. This is more serious than lock-in to a telephone or Internet service provider; switching customers need to maintain access to stored data and may need to ‘join up’ data and applications from multiple providers. This tendency to favour ‘closed’ models and to place minimal emphasis on transparency is a natural development because many cloud service and cloud hosted-service business models started with large firms outsourcing services that were formerly shared within their organisations and supply chains. Therefore, although cloud computing itself is based on the mobility of data and applications within the facilities offered by a single provider\(^85\), mobility between providers remains problematic. This limits competition between the platforms offered by different providers and potentially makes cloud users more vulnerable to the consequences of cloud business failure. Conversely, switching between cloud hosted services on a given cloud provider’s platform\(^86\) may be too easy, resulting in inefficient churn and volatility; indeed, services may change without consumers’ knowledge or consent\(^87\). In principle, the market might eventually resolve the problem. Switching cloud platforms may be facilitated by virtualisation, which makes end users less dependent on the specific hardware, software and operating systems offered by their current cloud service provider; moreover, it is often easy to relocate from one data centre to another, taking advantage of flexibility and scalability. But the success of this solution depends on interoperability and standardisation; as noted the legacy of most cloud service providers favours limited mobility; transparency and self-regulatory standards may create interoperability clusters rather than open competition. In other words, if competition can be restricted by using interoperability as a way to coordinate the activities of providers on a single platform, the range of choice and pricing may be restricted for consumers who are thus locked in because ‘intensive competition’ (on the platform) is suppressed and only ‘extensive competition’ (between platforms and the applications they provide) is available, which increases the disruption involved in switching applications\(^88\). Conversely, if end-users can change cloud-hosted services quickly (or are unaware of such changes), the power of the platform provider is enhanced in much the

---

\(^{85}\) Using virtualisation and data-sharing to provide agile and efficient load-balancing.

\(^{86}\) Although the analogy is not exact, the ‘market for apps’ provides a useful point of reference. Between the two dominant platforms (iOs and Android) there is almost no direct mobility, but each hosts a vast number of potentially competing apps (500000 for iOs, 350000 for Android) offered by a very large number of suppliers (average number of apps/supplier is around 3) – data from EC JRC IPTS.

\(^{87}\) Zittrain (2008)

\(^{88}\) See e.g. Cave et. al. (2009)
same way as a provider of a shared retail space gains extra traction with consumers who prefer a range of choice without the costs involved in exploring other locations. If consumers are unaware of changes in the providers of the cloud-hosted services, they cannot express their preferences effectively and the incentives of providers of cloud hosted services to invest in meeting users’ longer-term needs are weakened.

Cloud-specificity: Consumer switching is an issue across communications and content services, but is sharpened here by cloud providers’ control of subscribers’ data, programmes and activity logs, by limited contractual protection and by complexity of choice.

Prospects for market solution: Very limited, especially for B2C customers. The problem has been commented on for many years, and yet impediments remain, Not in providers’ interests to enhance mobility.

Intervention issues: Regulatory traction with cloud service providers, lack of legal basis to enforce open platforms.

4.2.2 Copyright and IPR

Cloud storage may make it hard to comply with or enforce copyright and other IP protections. Some aspects of these difficulties in compliance and enforcement are common to environments in which hosted content is made available to others (e.g. Internet web-hosting) but are more difficult in the cloud, where content location may be unknown both to those who provide and use access and may change in response to cloud providers’ traffic and data management. At the same time, cloud providers may not be able to verify the legal status of storage or hosting specific data, or may find a conflict between legal certainty of data location and the technical and economic drivers of cloud provision. There have been many proposals to extend third-party liability for e.g. copyright violation to on-line access providers based on a least-cost-avoider argument. These have thus far been primarily directed at Internet Service providers but may be applied to cloud providers. A recent example provided by the (currently postponed amidst considerable protest) the US Stop Online Piracy (SOPA) and Protect IP (PIPA) Acts. While PIPA in particular concentrated on websites in general, the use of third-party liability highlights both the potential of uncontrolled clouds to disseminate pirated material and the risk that cloud platforms will be targeted by government authorities (from other countries). The threat or certainty of legal action may cause cloud providers and cloud users thoroughly to vet providers of online data storage, backup, and information hosting to ensure that users’ critical data and platform providers’ business continuity will not be damaged. Indeed, given the location-independence (see 4.3.1) of many of these services, US regulators may not provide the necessary deterrent.

89 Zittrain op. cit.

90 Both bills were suspended at time of writing. SOPA would have increased the power of American law enforcement authorities to combat web-based trafficking in counterfeit products and intellectual property; PIPA would have created powers to restrict the activities of websites involved with such activity. One such website that was successfully taken down was Megaupload; the indictment identified the site as hosting user-created clouds for the storage and sharing of content. Similar concerns have been raised in relation to Wikipedia and Craigslist.

91 In the case of consumers, this may come via user ratings.
Other aspects are unique to the cloud, such as content matching services like the Apple iTunes Match service provided with the iCloud. These arrangements legitimise even pirate content and let those rights holders who have licensing arrangements with the cloud service provider recover some payment that would otherwise be lost; on the other hand, it gives dominant providers of matching services a particular advantage in negotiating licensing deals, increases their vertical market power over their subscribers by locking in their legitimised as well as illegitimate content and may crowd out efforts to enforce copyright directly by appearing to provide a ‘light-touch’ alternative to which content owners can sign up. This is reflected in recent market and legal developments suggesting that copyright per se does not seem to be a major concern for end users but features more strongly as regards licensing arrangements between cloud service providers and licence owners. These challenges have arisen from the market; there is no a priori reason to believe that they will not ultimately be met by the market; however, if the market solution has serious adverse consequences for competition in the cloud services market, or departs significantly from the approach being adopted for other web-hosted content, intervention may be necessary.

Cloud-specificity: Not unique to market, but non-transparency of e.g. location makes it sharper in the cloud and some troubling developments (iTunes Match) are cloud-specific.

Prospects for market solution: Limited, and dependent on general changes in IPR protection law and implementation.

Intervention issues: global scope of the problem, conflation of IPR and competition issues.

4.2.3 Unfair and potentially anti-competitive contract terms

Cloud services offered to consumers tend to be governed by standard form ‘take it or leave it’ SLAs. This is an efficient way of serving many small users, but the unequal bargaining power (lack of opportunity to bargain) between provider and consumer creates a risk of unfair and potentially anti-competitive terms. This is potentially covered by the Unfair Terms in Consumer Contracts Regulations 1999. The economic problem is that such terms raise switching costs; if the costs are unreasonable, this can lead to harmful (for consumers and for competition) lock-in. This is potentially more serious in cloud environments where providers also control consumers’ data (and programmes). At a minimum, telecoms (and/or competition) authorities should keep a watching brief to see how easily consumers can switch provider, how much switching costs, how quickly changes of provider are completed, whether their data are safely returned or removed, and whether this is appropriately reflected in contract provisions. More generally, regulators may wish to monitor the way the industry manages this issue to see whether regulatory intervention is required. Related issues arise regarding other contract terms (i.e. aside from

---

92 This service allows users access – for a fixed price - to licensed copies of any content that they place in the cloud and for which the cloud provider has a licensing agreement with the rights holder. Because this access does not depend on the legitimacy of the users’ original content, it provides an alternative (and less expensive) access to this content; this strikes a balance between legitimising violations of IPR and partially monetising content that would otherwise be pirated.

93 See e.g. Zimmerman (2011) for legal analysis of the recent Mp3.com case; or Wittow (2011) and Wittow and Buller (2010) for a broader discussion about liability and consumer protection.
contract termination): when can providers change contract terms, and what rights do users have in such cases; how are complaints dealt with?

The quality, price and functionality of cloud services are governed by Service-level agreements (SLAs), while payments – except in free or freemium models - are controlled by subscription contracts. Despite the wide ranges of user characteristics, consumer concerns and cloud (and cloud-hosted) services, Only a limited range of highly-standardised SLAs are available; these are regarded\(^\text{94}\) as providing insufficient flexibility, an inefficient allocation of responsibility and an excessive assignment of risk to subscribers. This threatens consumer empowerment and dampens the signals that should encourage innovation. By the same token, payment terms currently favour static and easy to understand pricing models such as pay as you use or subscription, but do not generally provide dynamic pricing – i.e. prices that vary with e.g. congestion or tariffs for storage and other services that change automatically in response to changing usage patterns. Taken together, they can reduce consumer surplus, facilitate anticompetitive market segmentation, promote lock-in and reduce efficiency.

*Cloud-specificity*: Service level agreements are particularly important for the cloud, where users’ vulnerability and lack of information are higher than for other Internet services.

*Prospects for market solution*: Limited, as it is not in the interest of providers.

*Intervention issues*: need to reconcile with competition, commercial law and unfair practices regulation; possibly outside remit.

**4.2.4 Security, reliability, resilience capacity**

There is a direct citizen interest in the functioning of critical infrastructures; this may well come to include the cloud. The US Department of Homeland Security defines critical national infrastructures as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The threat can be indirect, as the functioning of other critical infrastructures comes increasingly to depend on the cloud\(^\text{95}\). A current project sponsored by the UK’s Technology Strategy Board\(^\text{96}\) recognises these dependencies as follows\(^\text{97}\):

> “Our critical national infrastructure is increasingly dependent on information systems and the services they support. Cloud computing ecosystems of service providers and consumers including individuals, charitable and public bodies, SMEs, large enterprises, and governments will become a significant part of the way these services are provided, allowing more agile coalitions, cost savings and improved service delivery.”

---

\(^{94}\) Bradshaw, Millard and Walden 2011.

\(^{95}\) An example is provided by the IBM/Cable & Wireless project on the “Smart Energy Cloud” (IBM (2011).

\(^{96}\) See http://www.instisp.org/Document.Doc?id=1570

This kind of indirect dependency is enhanced by the movement of increasing proportions of critical information assets and functions (business and government) to the cloud.

More directly, the cloud itself plays a central role in the critical information infrastructure, as recognised by organisations such as the Centre for the Protection of National Infrastructure (Deloitte 2010) and Chatham House (et. al. 2011).

A related issue of both personal and societal security issue concerns the availability of cloud-hosted data and cloud activity logs for forensic and law enforcement purposes; this issue arises in respect of other Internet activity, but the cloud represents a much larger scale and greater practical difficulties of obtaining access.

There is a corresponding consumer interest in the continuity and quality of service they purchase. This is not limited to personal users, but includes those who sell services over cloud platforms or use cloud-hosted services to deliver ICT-intensive services to others.

Enterprises are particularly concerned about privacy of stored data (including activity logs), compromised virtual machines and data access and service continuity. Lack of transparency of cloud providers’ practices currently prevents service users from being sure that they are meeting security and accountability obligations. In addition, the structure of the cloud may create a unique environment for ‘hosting’ cyber-attacks, propagation of compromised virtual machines and other malware, and identifying and containing malicious traffic.

Beyond the specific consumer interests lies a general economic issue: information security (including access, integrity and prevention of unauthorised access) is among the most frequently-cited concerns for current and potential cloud users and an important impediment to the development of the sector. These security concerns go well beyond protection of personal or proprietary data to include e.g. infrastructure resilience (continuity), authentication. This gives security a stronger consumer orientation. Potential market solutions may be associated with market dominance that creates additional consumer harm.

Cloud-specificity: More important in the cloud, due to information asymmetries, increased dependence, novel threats (e.g. compromised virtual machines)

Prospects for market solution: may be resolved by self-regulation and/or increased transparency.

Intervention issues: mixture of business and consumer interests, overlap with critical infrastructure protection.

4.2.5 Crime

Cloud services can be used for a range of other criminal activities (in addition to IPR theft). While none of these are specific to the cloud, they may take different form there in view of the complexity and non-transparency of the environment. This may be a matter of regulatory interest because communications services are essential to the delivery of cloud services, and may play a vital role in detection and evidence-gathering. Collectively, such criminal activities may threaten citizen access to vital services and general societal

---

59 See e.g. Chow et. al. 2009.
protection interests by increasing the vulnerability of the cloud infrastructure, especially as cloud-hosted services become more important in enhancing citizen security and safety. Consumer interests can be adversely affected by specific illegal activities such as:

**Theft, alteration or denial of access to identity and other data** – individuals whose cloud-hosted identifying information and records are usurped, corrupted or blocked may be unable to use the Internet for a whole range of activities, and may suffer financial loss as a result. This is not unique to the cloud, but the migration of an increasing range of activity to the cloud combined with the indirect and variable contact between users and cloud-hosted providers of data storage, transaction processing may exacerbate problems found on the Internet *per se*, where users and service providers typically have a direct contract or at least a higher degree of visibility than in the cloud. In much the same way, small firms using the cloud for primary storage or backup of sensitive data may find their resilience and security threatened. As a result, their competitive position will be weakened vis-à-vis rivals who do not suffer such losses or who are able to make use of private clouds.

**Fraud** – as the scope of cloud services expands, the potential for their fraudulent use also increases. This is fairly obvious as regards services intended to collect and resell personal information, but is increasingly raised as a possible risk in relation to cloud-hosted financial services and financial advice (e.g. providing access to sophisticated financial models hosted in the cloud\(^9\)). This is not original with the cloud, but may be more severe in cloud contexts due to the aforementioned lack of transparency and the wider availability of highly sophisticated computation intensive tools for implementing such frauds.

**Malicious system, processing or data interference** are known and increasing sources of citizen and consumer harm. They are by no means limited to the cloud, but may be more difficult to detect, prove or prevent because of the complexity of the cloud, the flexibility of the arrangements for storage, exchange, the continual changes in computing and application environments and other factors that make it hard to assemble and interpret evidence. In addition, there may be limited legal traction: existing criminal sanctions against e.g. hacking or interference with networks or data stored in computer systems provide only limited scope for cloud service providers or end-users to take action against cybercriminals; cloud providers could play a vital role in detecting infringements and gathering evidence by applying to their management and activity logs the emerging tools of ‘big data’\(^{10}\).

**Data loss or unauthorised release** is a potent source of potential consumer harm, especially where data subjects are unaware of the breach. The enormous scale, flexible location and other attributes of consumer data holdings of large storage providers make them attractive targets, but SLAs and criminal sanctions designed to improve their performance may be

\(^9\) Resale of financial modelling and machine-trading services to private equity firms is already widespread and is expected to expand into retail investment markets in the near future. Such models are inherently hard to audit and control and existing financial consumer protection rules may struggle to cope with cloud-hosted (and the delocalised) services of this nature.

difficult to enforce. The standard approach (breach notification) has had only limited efficacy in the Internet in general\(^{101}\); it may be even weaker in the cloud, especially if reversibility (ability to leave the cloud) is limited. In any case, notification requirements currently apply only to electronic communication service providers (a definition that does not catch most cloud service or cloud-hosted service providers). There are further potential citizen harms associated with attempted or successful data breaches that lead to loss of service continuity or network integrity.

Cloud-specificity: there are two types of criminal issue here – the targeting of clouds by criminals and the use of cloud infrastructure by criminal elements. The first of these may essentially be an extension of current issues with the attractiveness of large databases to hacking and data exfiltration. The second is much more cloud specific as it concerns the way in which cloud hosted services serve to enable a criminal digital underworld.

Prospects for market solution: given the poor record of crime proofing many technologies, targeted regulatory intervention and improvements in law enforcement capabilities would seem necessary. However regulatory intervention will need to address the root of the problem (vulnerabilities that give rise to exploitation by criminals) and not the symptoms (e.g. by disseminating information about the poor performance of cloud service providers and leaving the rest to the market)

Intervention issues: Telecom regulators with competition powers would clearly have a role in receiving breach notification reports (as under the current arrangements of the EU Article 13a Telecom Package) and it could also indirectly support measures to help improve transparency of security levels in cloud service providers.

4.2.6 Privacy

Cloud services may impair personal data privacy because the user of cloud-hosted services typically does not have a direct relationship with the provider of the service, and may not have a relationship with the cloud service provider, which limits the accountability of those who hold data and the visibility of their practices to data subjects and regulators alike. Existing protections rest on a legal distinction between data controllers and data processors that may be inadequate in cloud environments\(^{102}\) where the roles overlap. Another area of high concern is the extent to which consumers will be unable to exercise their rights in the face of large cloud service providers. This may grow in importance along with the expansion of ‘freemium’ (especially B2C) cloud services provided in exchange for personal information, or ad supported models in which users’ bargaining power is weakened by lack of direct payment. Existing legal frameworks protect the privacy of communications to a degree, but may be less effective as regards stored information or activity logs showing users’ access and processing activity and may do little to ensure the accountability of those processing data in the cloud.\(^{103}\) However, the telecom regulator’s interest may be limited;

---

\(^{101}\) See e.g. Cavoukian (2009) and Dresner & Norcump (2009)

\(^{102}\) See e.g. Cave et. al. (2011) and Ismail (2011).

\(^{103}\) Robinson et al (2011)
other authorities (e.g. data protection or privacy authorities\textsuperscript{104} for \textit{inter alia} data privacy in the cloud) have primary responsibility for privacy \textit{per se} and there may be market solutions in the form of privacy-by-design, cloud-specific privacy-enhancing technologies or the provision of privacy as a service in cloud environments\textsuperscript{105}.

\textit{Cloud-specificity}: issues of accountability and visibility of relationships, who does what with data subjects’ personal data and the roles played by data controllers and data processors are unique to cloud computing because of the dynamic and autonomic properties of cloud service provision as discussed earlier in this report (p. 18).

\textit{Prospects for market solution}: market based solutions may exist in the form of Privacy by Design, Privacy Enhancing Technologies or even Privacy as a Service. However, policy intervention might be required to kick-start take-up or, in the case of insurance against liability from losses of personal data, perhaps even act as an insurer of last resort.

\textit{Intervention issues}: Any policy intervention would need to be undertaken in close cooperation with privacy/data protection authorities and also take into account recent proposals\textsuperscript{106} at the European level which may reduce national freedom of manoeuvre to craft more specific interpretations of EU law in the realm of privacy and data protection.

4.2.7 \textbf{Communications as a Service (CaaS)}

Communication as a Service (CaaS, see discussion on page 7) involves integrated or converged video, voice and data communications and associated services (e.g. VOIP, instant messaging, video conferencing, call recording, message routing) available from multiple devices and offered to SMEs and to a certain extent consumers (e.g. Skype offering voicemail and a variety of other communications services). It is a matter of regulatory interest because CaaS services, which overlap strongly with regulated electronic communications services, are provided by currently-unregulated cloud services providers. This raises consumer and small business concerns associated with potential regulatory bypass\textsuperscript{107} and with the ability of CaaS providers credibly to deliver (in the cloud) communication capability that is service orientated; configurable; schedulable; predictable and reliable. Cloud delivery also meets other consumer or user requirements such as: network security; dynamic provisioning of virtual overlays (to isolate traffic or provide dedicated bandwidth); guaranteed message delay; communication encryption and network monitoring that other forms of communications service may struggle to provide.

\textit{Cloud-specificity}: these issues appear to be specific to the cloud since they conflate some legacy aspects of the provision of a simple pipe with services that are more focused upon managing different types of traffic (video, voice, data) with the associated QoS issues. Furthermore, CaaS, with its need to leverage presence sensing technology (e.g. whether the

\textsuperscript{104} The UK Information Commissioner’s Office has issued Guidelines on this topic: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf.

\textsuperscript{105} See \textit{e.g.} Kroes (2010), Pearson (2009), Itani et. al. (2009).


\textsuperscript{107} Including the possibility of using cloud capability to undermine competition in the communications market.
recipient is on or offline and whether they wish to receive SMS, video or voice communication) has the potential to affect other issues (e.g. privacy).

*Prospects for market solution:* it is not clear how markets might respond to the consumer issues arising if CaaS providers are seen to bypass regulatory regimes. The result may be increasing fragmentation, as different CaaS providers target distinct customer segments interested in specific requirements such as security or QoS.

*Intervention issues:* addressing these concerns would appear to lie directly within many telecom regulators’ remits; this might even require extension of regulatory mandate over CaaS providers.

### 4.2.8 Cloud as a utility – including risk of market foreclosure

While some ‘layers’ of the cloud computing system are potentially competitive, others have strong natural monopoly characteristics including economies of scale and scope in the operation of data centres. As a result, there is a need to ensure that these resources are not used to foreclose the market vertically, while at the same time meeting the costs of the demand for bandwidth and communications services caused by cloud usage – the connection being that the parts of the value chain providing network bandwidth and communications services will assert that the rents they derive from restricted competition are needed to provide the networks and other facilities, and especially for the maintenance and upgrade of the network infrastructure (this is the argument most often made against net neutrality rules, for example). The incentives to foreclose are magnified by the (BYOD or “Bring your own Device”) openness of end-user interfaces, because this increases the costs of provisioning (in order to accommodate arbitrary devices) and reduces the extent to which such costs can be recovered through hardware acquisition charges. The potential costs of meeting demand are magnified by high-bandwidth advanced cloud services, remote storage and retrieval and content-streaming applications. However, on average the telecommunications service providers are able to capture less Average Revenue Per User (ARPU) due to the ubiquity and low cost of alternative ‘added value’ services – as has been seen with the impact of VOIP on voice telephony revenues. This may lead to other structural changes in the form of mergers between dominant telecommunications service providers and cloud providers (e.g. Verizon-Telemark). This vertical integration will try to internalise the externalities between the cloud providers and the Telco networks on which they run, but may not alleviate deadweight loss or increase consumer choice.

There may be additional citizen interests if cloud computing becomes a dominant mode of delivery for critical services and the informational resources necessary for social

---

108 These include: using large servers and high-performance computing to serve larger end-user pools; smoothing capacity utilisation by clustering large and differentiated demands; and exploiting the physical co-location of commercial cloud users to underwrite the installation of dedicated high-speed lines.

109 A detailed analysis of the impact of VOIP on telephony is provided in Biggs (2009). In the case of mobile telephony In-Stat (2009) projected that by 2013, mobile VoIP applications will generate annual revenues of $32.2 billion, driven by more than 278 million registered users worldwide.

110 This creates a practical issue of cloud market definition in applying Ofcom’s competition authority.

111 E.g. power, traffic management or emergency services; see e.g. Bhuvaneswari and Karpagam (2011).
participation; there may in future be a case for UK government to consider expanding the Universal Service Obligations to encompass the cloud-hosted services Internet access as the objective of an expanded definition of Universal Services. However, it does not obviously follow from this that telecom regulators must be centrally involved. In some countries (e.g. Germany) regulation converges around networked industries and utilities; in others (including the UK), communications regulation is unified; access to the cloud flows through the communications network, but e.g. processing and storage are not communication in the strict sense. Even if they were included, would the regulatory control extend beyond platforms to hosted services; and beyond pricing and availability to security or reliability?²¹²

Cloud-specificity: this issue is a more acute version of others that have gone before.

Prospects for market solution: to the extent that cloud computing becomes a public good, the prospects for market solution might depend on the basis for potential intervention (e.g. minimizing foreclosure per se, protecting internal subsidies to deliver widespread coverage or essential infrastructure). Unlike the situation of broadband, where delivery to remote regions required investments which the market would simply not supply, with cloud computing the main fixed capital investment requirements take the form of data centres (which need not be publicly provided) and enhancements to existing infrastructure capacity.

Intervention issues: the inclusion of cloud computing as part of a new Universal Service obligation would undoubtedly fall to telecom regulators (at least in the EU) as the main regulatory actors in this domain.

4.2.9 Advertising and marketing practices

Cloud computing is still in its infancy, so there are both risks and opportunities for the industry in relation to advertising and marketing practices. In the cloud, it is particularly important for providers to earn or capture users’ trust; this would be undermined if providers engaged in the sort of practices used in other parts of the communications and ICT industries (against which many regulators have been active). At a minimum, subscribers should be fully and effectively informed of what they are signing up to. This may not be a problem if the combination of a higher premium on trust and the lessons of experience allow the industry effectively to self-regulate. On the other hand, the complexities of the cloud may leave some providers unable to certify, deliver or even inform consumers about the cloud-hosted services they receive.

Cloud-specificity: these issues are specific to the cloud. However, the complexities of the relationships and interactions among cloud service providers mean that trust would be even more difficult to encourage.

Prospects for market solution: there is a scarcity of empirical data on the extent to which markets might exist for services to protect or manage online personae to ward off advertising. This makes it hard to predict whether such a market might emerge to resolve

²¹² For example there is a current debate about ‘breach notification reporting systems’ since under current EU telecommunication rules they only apply to providers of public e-communications networks
these issues. Furthermore, economic interests representing advertisers who benefit from the broad use of ad supported models for delivering B2C cloud services may outweigh any latent demand for commercial cloud equivalents of the Telephone Preference Service.

*Intervention issues:* as with advertising in other areas, we may see policy intervention (more squarely within regulators’ mandates) to curb the excess of advertising. Ironically, this may result from improved privacy protections since by knowing less about individuals there is more chance that inappropriate (and not just unwanted) advertising material is offered.

### 4.3 Issues with policy and regulatory interventions

In this section, we discuss some issues that are more strongly linked to potential solutions to cloud-related problems or to general issues of regulation rather than unique or direct harmful consequences of the cloud that telecom regulators can and should consider.

#### 4.3.1 Location and jurisdiction

Cloud and cloud-hosted service locations are hard to pin down (especially for users) and constantly changing. Location-based law and jurisdiction are important for consumer and data protection, competition law (establishing market boundaries), and copyright licensing. In other situations, the law attempts to force even foreign providers of services to European citizens to offer equivalent protection\(^{113}\); this may be problematic or unfeasible in the cloud environment. More specifically, issues such as data privacy, freedom from unfair contract terms, etc. may be effectively managed within the UK context, but the cloud operates across borders. Managing these issues will require stronger international cooperation to protect consumers and industry from unscrupulous market elements. When cross-jurisdictional enforcement is possible, it is important to ensure that it is efficient and effective. In general, providers offering services to UK consumers should obey UK consumer protection laws; but this may be difficult to enforce across borders and enforcement across European borders may differ from enforcement against non-EU providers. A related issue is whether such laws can be enforced uniformly or consistently against providers of cloud services, cloud-hosted services or cloud-enhanced services.

In some situations (e.g. data protection, proposals have been made to ensure that rights are protected by requiring providers to hold data in a specific location\(^{114}\). However, by restricting the ability of cloud providers to shift data in response to load and other factors, this may reduce efficiency of the service and reduce competition among providers. However, the macroeconomic returns of attracting data centres are substantial and could deter nations from regulating against consumer harm in return for tax revenues and national employment. Therefore, location is a horizontal issue that affects all aspects of cloud-hosted activity whose regulation varies from country to country. There is a further

---

\(^{113}\) European examples include the Data Protection, Services and eCommerce Directives.

\(^{114}\) Such restrictions may be used to ensure compliance with data protection rules, or to ensure government access to stored data for security or law enforcement purposes; in addition, as Rittinghouse and Ransome (2009) note, “some banking regulators require that customers’ financial data remain in their home country.”
direct source of consumer harm, if data are held in locations with inherently greater risk of loss or criminal attack.

One aspect is well-known from the Internet in general; the contrast between regional telecommunications and the often globalised nature of Internet services. For pragmatic and legal reasons, extending ISP obligations- for example with respect to content piracy -to cloud providers may be problematic.

Other aspects are unique to the cloud; the mobility of data among data centres in different locations (for traffic and quality of service management) and the fact that the locations of cloud-hosted service providers may not be known by any of the parties involved. As noted above for data protection, this could be addressed by legal requirements for location specificity or disclosure of location information, but this may well impair economic and technical efficiency of the cloud model and the costs and benefits are not known. A market-based alternative is the provision of locational certification (or its legal equivalent) by cloud service providers; but monitoring and enforcement may be difficult.

4.3.2 Consumer information, transparency of CSP practices

The mobility issue (see 4.2.1) turns on consumer information, but so does the loss of privity of contract (see 4.3.4) and the potential for market-based, consumer driven solutions to privacy (4.2.6) and security (4.2.4) concerns. There may therefore be a basis for mandated disclosure of a specific set of price, quality of service, security, location. data.

4.3.3 Locus of control

It may be difficult to identify points of leverage for effective intervention; moreover (e.g. applying the General Conditions to VoIP based communications or CaaS) existing regulation could be undermined by cloud-hosted alternatives. In addition, consumer protection and control are different in SaaS, IaaS and PaaS architectures; informed consent is different in private vs. public clouds. This also creates an issue of continuity of consumer protection as B2C cloud users migrate from SaaS to PaaS (where their influence and scope for direct involvement are greater).

4.3.4 Complexity of the cloud

Cloud services are delivered through extended pathways; the user of cloud-hosted services typically does not have a direct relationship with the provider of the service, and may not have a relationship with the cloud service provider. The cloud value chain contains a number of potentially distinct markets that appear to present different competition and consumer protection concerns. Weyl (2010) identifies five separate layers\(^{115}\) and notes the strongly different prospects for workable competition across them. Telecom authorities’ regulatory traction is stronger in e.g. the access market than in the hypervisor market, though it is their combined operation that affects consumer interests.

This view may conform to a many-layered version of 2-sided models of platform competition, where the geometry of the layers (see Figure 4) between the ‘ends’ of the market is constantly changing. Moreover, the ‘ends’ (cloud-hosted service providers and

\(^{115}\) Data centres, hypervisors, operating systems, routers and access. See Weyl (2010)
cloud users) may themselves overlap and change as new services are developed. Therefore, regulation based on fixed roles may be inappropriate.

A more direct consequence that affects the viability of market-generated solutions to consumer issues is the reduction of direct contact and visibility between the ‘ends’ that hinders their efforts to internalise or contract around issues of mutual concern. More generally, the complexity and adaptability of the cloud pose challenges to conventional forms of regulation and to the way harms are measured and remedies crafted.

4.3.5 Certification and other forms of self- or co-regulation

Certification by individual firms or self-regulatory bodies provides a ‘market-based’ solution that potentially addresses a number of concerns including privacy\(^\text{116}\), security, resilience\(^\text{117}\) and QoS\(^\text{118}\) (especially for public clouds). Ideally, such arrangements should be international in scope. In order to be effective, they may require national regulatory monitoring and/or enforcement. However, the market may produce multiple and inconsistent guidelines and certification regimes, of doubtful efficacy, high cost, limited manageability, or potential to harm competition.\(^\text{119}\) This issue is not specific to the cloud; the danger of lock-in by dominant platform providers may be greater. The potential for certification to produce suboptimal or harmful results may be greater in the cloud – especially in public clouds where the demand for assurance by customers is highest, and where recognition (or co-regulatory enforcement\(^\text{120}\)) by government can increase the leverage of a particular standard or create a form of ‘Potemkin regulation’ which is more apparent than real. On the other hand, self- and co-regulation do have advantages over formal regulation in being better-informed about changing market and technical conditions, lower-cost and (under some conditions) more effective\(^\text{121}\).

4.3.6 Cloud neutrality

The relationship of cloud-hosted service providers, cloud platform providers and cloud users creates a two-sided market. While users may expect to use hosted services independently of their own hardware, software and operating system, the hosting of these services on a particular platform may be highly restricted, and can provide an additional basis for the kinds of discrimination cited in the net neutrality debate\(^\text{122}\). In that setting, pricing and quality of service discrimination by type of content was seen as a potential source of competitive harm and consumer disempowerment; this danger would seem to be greater when discrimination can be backed by technological and interoperability

\(^{116}\) E.g. TRUSTed Cloud – see http://www.truste.com/privacy_seals_and_services/enterprise_privacy/cloud-certification.

\(^{117}\) See http://cloudcomputing.sys-con.com/node/1378183

\(^{118}\) Lachal (2010)

\(^{119}\) On these latter two points, see Cave, Marsden and Simmons (2008)

\(^{120}\) In the domain of privacy certification, the US Department of Commerce promises to enforce violations of the self-certified compliance of US firms with data protection principles. See Cave et. al. (2011) for a discussion of the evidence surrounding its effectiveness.

\(^{121}\) Cave, Marsden and Simmons (2008)

\(^{122}\) Marcus et al (2011)
restrictions. The market can generally solve the problem of unjustified price discrimination by consumer sovereignty (switching and bargaining power) and by arbitrage – in this case resale of cloud services. This is far harder if rivals can be excluded, affiliated service providers favoured and consumer sovereignty restricted by artificially-high ‘technical’ barriers. There may therefore be a basis for requiring cloud service providers (or the electronic communications service providers who support them, if distinct) to price their services on a strictly accountable cost basis, without discriminating between different uses or services hosted on the cloud, offering hosting on a Fair, Reasonable and Non-Discriminatory (FRAND) basis, including charges, quality of service and ‘visibility.’ This would also have to consider whether cloud service providers could implement throttling (as some MNOs are doing with data plans) in anticompetitive ways (though we are unaware of any evidence on this point).

4.3.7 Consumer/SME similarities, regulatory heritage and convergence

Both SMEs and personal users are potential providers of cloud-hosted services, and are therefore affected by issues at both ‘ends’ of the cloud value chain. In addition, despite the apparent differences between B2B (including SME) and B2C cloud services (see footnote 76), both types of user are vulnerable to the same privacy, security, consumer protection, risks; consumer harms thus occur in both B2B and B2C cloud services. As a result, it may be desirable to take steps to ensure consistency of approach as the two markets develop. A related issue is extent to which legacy forms of communications privacy (esp. for individuals) and security (for businesses including SMEs) regulation work together in the cloud environment.

4.3.8 Trust

Finally, cloud-hosted services (especially storage and processing) are attracting the interest of regulators from the perspective of trust because they establish further perceptual distance between the data subject and data, which renders the consumer even more powerless in the face of broad scale service offerings scaled to meet mass demand. In particular, the one size fits all service models of many cloud providers are seen as a key indicator of the loss of consumer power to cloud service providers.

---

123 See Marcus et al. (2011)
124 This is addressed in the ICO Personal Data Guidelines referenced at footnote 104.
125 Robinson et al. 2010, Rittinghouse and Ransome (2009), GAP (2011)
This concluding section raises some issues arising from specific areas where cloud-like service and technology developments abuts other forms of activity or policy concern. The discussion is meant to be provocative rather than analytic, but makes allusive use of theoretical results. It discusses one concrete application and briefly mentions others as a basis for discussion.

5.1 Computer-based financial trading

Recent scholarship on the economics of cloud computing by e.g. Yoo 2011, Weinman 2011 has noted the interaction between the mathematical and technical aspects of computational and communication dynamics and the economic functions (including quality of service) on the other. Of course, the connections don’t stop there; variations in quality of service in terms of e.g. latency or packet loss have been implicated (or at least heavily invoked) in the net neutrality debate\textsuperscript{126} and might be expected to spawn a variety of different business models and forms of market segmentation. But this is not directly linked to cloud computing \textit{per se}. Another development of somewhat greater ‘centrality’ concerns the proliferation of computer-based algorithmic and high-frequency trading\textsuperscript{127}. This, too, is an area where the technical performance of ICT systems rubs up against the informational and economic performance of market systems. The most obvious illustration was the 2010 ‘flash crash’ in which a flood of orders placed by a ‘rogue algorithm’ increased the latency with which quote data propagated through the network. Other programmes, trading on stale data (but unaware of the delay) created a feedback loop that lead to a quite staggering (albeit brief) collapse in stock values within a couple of minutes. This had a variety of long-term effects: some reallocation of money (when prices and the aggregate values returned in less than half an hour, not all of the money was in the same place as it had been before; the institution of ‘circuit breaker’ rules to suspend trading when prices moved too far and fast for ‘normal’ trading in order to allow the transients to even out; and a change in the responses of both traders and their programmes to similar

\textsuperscript{126} See e.g. Marcus et. al. 2011

\textsuperscript{127} For a comprehensive assessment of the state of the art and a balanced treatment of many aspects, see the working papers commissioned by the UK Department of Business, Innovation and Skills as part of a Foresight project on the Future of Computer-Based Trading, available from http://www.bis.gov.uk/foresight/our-work/projects/current-projects/computer-trading/working-paper.
events (so-called ‘normalisation of deviance’ leading to underreaction to unexplained spikes in volatility). The episode has not been repeated on the same scale, but instances of unexplained volatility continue to occur for brief periods and within small clusters of assets. The system of computer algorithms linked by high performance networks is representative of a range of cloud-like infrastructures, and such crises could occur in other domains where computation is distributed and where exchanges of information occur too fast for systemic equilibration or human scrutiny. Such events echo well-known results from complexity theory for self-organising systems; in many models discontinuities are heralded by a sudden loss of degrees of freedom (in other words, excessive synchronisation). Even if such systemic accidents can be prevented, the underlying dynamics open the door to new forms of manipulation (nudging the market when it is approaching the edge of a cliff – it will either tip over or will be ‘regulated’ back onto safe territory; either movement creates speculative profit opportunities).

This, in turn, could point the way to ‘macroprudential’ ways of regulating toughly coupled clouds (looking out for self-organised criticality or excessive centrality), imposing appropriate speed limits or creating automated trades that dampen explosive fluctuations.

How does this relate to the cloud? In the first place, the storage and processing of vast arrays of spatially distributed data draws on cloud architectures (at least private or community clouds). This is particularly true of the data centres used to facilitate hedge and derivative trading; they tend to be located at specific points in space which balance the speed of information flow and trade execution with the density and importance of different exchanges. In other words, understanding the dynamics of such interactive clouds involves spatial as well as the logical and economic topology and structure. Secondly, today’s problems are mostly associated with the highly efficient operation of relatively unsophisticated algorithms; all the complexity comes from their interaction.

There is an important economic lesson in this: when it was common knowledge that markets were slow, noisy and otherwise imperfect, the collective use of efficient markets as a common point of reference meant that weak-form efficiency (at least) was widely confirmed. As markets come closer to the theoretical ideal of frictionless, instantaneous and nearly-costless trading, fine-grained behaviour appears to depart ever further from that ideal.

There is also a danger for the future. At present, only a few large institutions have ready access to sophisticated models, large amounts of relevant data and costless high-speed trading opportunities. Much trade still goes through institutional channels and most investors have only indirect connections to the fast lane of the financial superhighway. Therefore, a form of self-interested self-regulation has tended to prevail. The results are not equitable or efficient, perhaps, but are far better than the more apocalyptic predictions in the wake of 2008/9 and 2010. But cloud computing (e.g. Amazon’s EC2) brings near-
supercomputer capability within the reach of almost everyone; it is impossible to anticipate the systemic consequences.\(^{128}\)

5.2 **Supply chain repositories**

An increasing range of economic activity results in the collection of vast amounts of data that originate with different stakeholders during the active phase of the project or activity, but that may be of great value to others and at much later points in time. Examples include:

- CAD/CAM data for the design of complex systems (e.g. aerospace vehicles, buildings, etc. This can be used as the basis for managing contractual compliance claims, diagnosing operational problems, modifying, improving or extending such systems, etc.

- Operational (in-service) data for equipment, which can be used to determine whether it was being operated within design parameters, as inputs to future design, etc.

- Oil and gas exploration and drilling data, which can help in assessing companies’ declared valuations (hence market performance and costs of capital) and in predicting the productivity of other plots and future resource availability – and which can thus influence other policies, auction prices, etc.

- Laboratory randomised controlled trial and clinical data for use of pharmaceuticals and medical equipment, which can be used to assign liability, make diagnostic and medical care funding decisions, evaluate patent holdings, etc.

Because such repositories offer storage, processing and query capabilities on a local public goods basis, their deployment structures and business models resemble those of cloud computing.

5.3 **The app ecosystem**

As noted above, some cloud geometries provide platforms for app developers (or users writing their own apps) to expose them to a wide range of engaged potential clients. The results should favour innovation; instant critical mass, low development, exit and entry costs and potentially fierce competition, because users who remain on the same platform face very low switching costs. The ‘thin client’ nature of cloud access further lowers costs and produces a kind of technological or software neutrality; users with many types of system can try the apps, and compare them with applications ‘native’ to their system. In this way, intensive competition is balanced with extensive competition, which should minimise adverse lock-in. The numbers of apps and the number of apps per developer seem to bear out the expectation of an atomistically competitive market. And yet, the

\(^{128}\) The word anticipate is intentional; strong emergence is sometimes defined as system behaviour that cannot be anticipated, but can be predicted – in other words, behaviour that can only be predicted with sufficient information about specific instances or realisations, rather than theoretical possibilities. Ball et. al. 2010.
behaviour of major cloud platform providers appears to conform to the predictions of two-sided market theory, or to the vertical control exercised by major providers of cloud-hosted content and some highly successful app developers have quite publicly left major app market places. Of course, the analogy is not exact; it conflates apps offered over the cloud (but destined to run on tablets and smart phones) with apps developed and run entirely within clouds. But there are clearly some issues of competition and innovation policy that need further investigation.

5.4 Privacy issues

The discussion in Section 4.2.6 covers some of the main features of privacy in the cloud. But future uses may raise other issues, particularly at the intersection of privacy and security and in relation to jurisdiction. Two specific topics are: the use of the cloud to infringe non-data privacy and agency relationships to circumvent privacy protections.

Privacy is generally interpreted as coextensive with data privacy, but increasingly extends to privacy of action (the ability to make decisions without undue or occult influence) and subjective privacy (the right to be let alone). People using the cloud, like the computer trading algorithms mentioned in Section 5.1, exchange information and respond to news and to the results of data processing. If they do not, or cannot effectively audit or understand the source and selection of the news or the basis of the processing, their apparent freedom of action may mask profoundly damaging behavioural manipulation. Indeed, they may be co-opted into helping their manipulators; if the response of a cloud user to particular information or a particular framing of information reveals private signals about their interests or cognitive stance, they can be led through a sequence of operations resulting in decisions that, while voluntary, serve others’ interest rather than their own. This is not limited to attacks on private (i.e. individual) people; similar ‘nudges’ can be used to set of waves of contagious behaviour for a variety of reasons (some quite benevolent).

Many countries have privacy rules that they seek to enforce; most are more vigilant for their own citizens’ privacy than the privacy of foreigners. But communications or computation in the cloud, as noted in Section 4.3.1, do not respect such boundaries. For efficiency, data may be stored and processed in a variety of regimes; some may have specific weaknesses in their privacy protections and it may not even be possible for users to know, let alone control, the location of their data. But geographic flexibility is central to many cloud advantages. Even worse, many interactions in the cloud that implicate privacy rights involve more than one person. If national privacy rules differentiate between citizens and non-citizens, it is possible for a government whose constitution prevents it from spying on its own citizens to obtain the information it needs by spying on foreign citizens with whom they interact, or to enter into reciprocal arrangements with the governments of other countries to conduct surveillance on each other’s citizens.

Recently, some cloud providers have been supplying locational controls in response to demands by e.g., US and German authorities; however, such controls have thus far mainly been provided to governments rather than citizens.
This issue is not cloud-specific, but has a particular relevance because most of the existing rules concentrate on communication in the formal sense of email, website visits and other observable transactions, and may not have traction over interchanges taking place within data centres.
REFERENCES


Comscore (2011) Email Evolution: Web-based Email Shows Signs of Decline in the US While Mobile Email Usage on the Rise http://www.comscore.com/Press_Events/Press_Releases/2011/1/Web-based_Email_Signs_of_Decline_in_the_U.S._While_Mobile_Email_Usage_on_the_Rise


A. Introduction and key features

This section develops some likely scenarios in order to aid understanding of the development of and linkages among the issues identified in the main body of the report.

Scenarios are logically consistent and feasible depictions of future developments. They are not predictions, but anticipate possible resolutions of current uncertainties in what is hopefully a holistic and useful way.

Scenarios for policy analysis are constructed (implicitly) on the basis of several distinct components:

- Exogenous uncertainties outside the control of decision-makers that may nonetheless prove important in determining the success of their strategies.
- Policy levers - near-term actions that comprise the strategies decision-makers want to explore.
- Relationships - potential ways in which the future (in particular attributes addressed by the measures) evolves over time based on decision-makers' lever choices and resolution of the uncertainties. A particular choice of exogenous uncertainties and relationships represents a future state of the world.
- Measures - performance standards used by decision-makers and other stakeholders to rank the desirability of various scenarios.

Scenario space is structured around different possibilities for the state of the world. For present purposes, we identified the following dimensions:

- Sovereignty over cloud regulation: national, international, market/self-regulation
- Locus of power in cloud services: Telcos (current EU situation), Google/Amazon (current US situation), Hypervisors (Vmware, MS/Citrix)
- Balance of cloud deployment models from regulatory perspective: public (consumer and citizen harms (incl. privacy), private/enterprise (competition), hybrid
- Architecture of (future) Internet: cloud as niche/overlay on current architecture or cloud-centric architecture (as in NSF NEBULA architecture).

Although these dimensions define a large number of potential scenarios, for present purposes we concentrate on those that are most plausible for the near-term and relevant to the UK context.

These are summarised in Table 10, briefly described in the next section, and related to the Issues in the final section.

Table 10: Scenarios

<table>
<thead>
<tr>
<th></th>
<th>Cloud-max</th>
<th>Nothing new</th>
<th>Another critical infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power:</td>
<td>Google/Amazon</td>
<td>Telcos</td>
<td>Hypervisors</td>
</tr>
<tr>
<td>Deployment:</td>
<td>Hybrid</td>
<td>Public clouds</td>
<td>Private/enterprise (provider responsibility)</td>
</tr>
<tr>
<td>Architecture:</td>
<td>Cloud-centric</td>
<td>Niche/overlay</td>
<td>Niche/overlay</td>
</tr>
</tbody>
</table>
B. Short descriptions

Scenario 1: Cloud-max

Key elements: Regulation adopts coherent Internet regulatory framework and co-regulates

Background

The cloud continues to develop under the existing framework of regulation, becoming increasingly central to the architecture and governance of the Internet. As a result, emergent issues tend to be managed through a combination of market solutions and self-regulation, both to take advantage of the information and agility of market and other non-government stakeholders and to forestall formal regulation; self-regulation is also 'protected' by increasingly global scope of the industry.

The balance of market (revenue, innovation) and governance power lies with the dominant players of the global Internet from which the cloud emerged; major B2C service providers such as Amazon and Google, who were able to move their own operations to the cloud and take their customer base with them and were thus able to leverage their ‘big data’ processing capability to dominate the provision of services. In this sense, this scenario is a natural extrapolation of current developments in the US.

As the cloud develops and its service platforms expand, existing B2B (enterprise) and B2C cloud service models come together in hybrid clouds. This addresses users’ and cloud-hosted service providers’ different security, control, etc. needs with a combination of shared resources and proportionate self-regulation. At the same time, the development of a common architecture adapted to a wide range of cloud users’ needs allows different types of users to innovate and to adapt their cloud service usage accordingly.

But the defining characteristic of this scenario is the cloud-centric nature of the Internet. In this scenario, the cloud has become the dominant mode of computation, data storage and information-intensive communication and transaction systems. This has specific implications for the way the Internet itself is organised, and for the severity, incidence and management of policy issues.

Highly mobile Internet users are not permanently affiliated to specific physical data centres because this inevitably involves latency, which is particularly unwelcome because an increasing proportion of critical applications use real-time audio and video communication. In this scenario, cloud providers use data migration and caching to serve their users. Users connect to the closest data centre, which then contacts the user’s home data centre to satisfy security requirements and obtain the needed data. The user then invokes computational services in the remote data centre; if she moves again or returns home, her data migrate to the new location. For efficiency, the overhead of migration is reduced by hiding the details of individual data items, transferring instead whole archives or virtual disks, which may be encrypted or otherwise secured; this simplifies the transfer mechanism and clarifies access and liability arrangements. Furthermore, each user has complete freedom to structure a virtual disk according to their preferences. Caching involves transferring data only when accessed; the remote data centre then keeps a copy for future access requests. This fits the general pattern (most data access requests involves a small fraction of the user’s data) but requires the system to ‘see’ and handle individual data items and the creation and use of metadata such as access times. Various combinations are possible to balance user preferences and requirements with cloud service providers’ capabilities and cost structures. To support mobile users and allow migration between data centres owned by different providers, computational services and data storage must be standardised and an economic model agreed. For example, cloud service providers might apply “roaming” charges for data transferred to or from remote data centres owned by other providers, operate ‘peering’ arrangements or restrict customers to its own or affiliated data centres. These choices raise the potential stakes for consumer mobility and jurisdictional issues.
This scenario also has implications for the structure of the supporting Internet itself. One plausible candidate is provided by the Nebula project funded by the US National Science Foundation under its “Future Internet Architecture” programme. A high-level view is shown in Figure 10.

Unlike the current architecture in which the core handles a vast array of requests of all sizes from individual TCP connections, the core will primarily handle traffic among data centres in the form of bulk data transfers. It will have to be continuously available, highly reliable and secure – in this sense, the core at least becomes a critical infrastructure (see Scenario 3). The necessary connections will be semi-permanent and high-capacity, so currently-critical functionalities (e.g., automated dynamic switching and circuit provisioning) will become far less important. The access layer will allow users to connect to the core from a wide range of wired and wireless ‘thin client’ devices; this creates an additional functional requirement for consistent authentication must be consistent. In the current Internet, the each network controls the connection and authentication of users; in the future, cloud service agreements will allow users to specify connection and access preferences (e.g., to choose lower-cost access with reduced performance or vice versa). When a user moves within range of a local access network, the system will ask the user’s provider to authenticate access, which will be approved or denied based on user preferences. The transit layer connects access networks to the nearest data centres. This differs from current arrangements in routing traffic to data centres rather than individual hosts and in allowing applications to request paths that meet specific security or data location requirements – though not specific paths. This reduces some of the lock-in problems associated with the use of private clouds to handle sensitive traffic and instead allows the potential emergence of “as-a-service” elements within the transit layer itself. A final architectural element that affects the policy issues is the degree of intelligence and control placed in the data and storage centres. Storage centres will be able to authenticate and implement data transfers without the need for intermediary computers and potential transfer bottlenecks; similarly, users’ ‘home’ data centres will manage user authorisations for file sharing and keep track of the location of migrated data.

**Rationale for regulatory intervention**

The transformation of the Internet creates an ostensible basis for a re-examination of regulatory mandates and duties; as an increasing proportion of communications traffic flows through an Internet organised around data migration and caching, and as users increasingly take control of the nature, functionality and quality characteristics of their services it is no longer obvious that a regulatory model based on communications services delivered point-to-point or on a broadcast basis by communications service providers with significant market power provides the most effective form of governance, or indeed that the existing allocation of regulatory responsibilities is appropriate. However, pending such long term and

---

130 Adapted from Pan et. al. (2011)
radical change, many of the central aspects of the scenario – even those that impinge on consumer interests directly – would seem to lie outside current responsibilities.

**Scenario 2: Nothing new**

**Key elements:** Patch up and extend existing regulation in piecemeal fashion (as currently structured)

**Background**

This scenario largely continues the trend of cloud development as currently experienced in the UK.

Regulatory sovereignty will continue to be exercised according to existing specific mandates (perhaps with *ad-hoc* approaches in certain areas) - this may create a race to the bottom among cloud service providers confronted with a wealth of potentially contradictory requirements (especially at the pan European level), possibly exacerbated as national regulatory agencies strive to attract profitable data centres.

The dominant deployment model will be the public cloud, as currently offered to B2C users and increasingly small and medium-sized enterprises. The strongest influence on cloud development (and the lion’s share of revenues) flow to the providers of telecoms infrastructures, who are increasingly able to add cloud services to their triple- and quad-play packages – though in many cases acting as cloud service brokers or cloud resellers to take advantage of the global scope and extensive developments of existing cloud-hosted service, cloud service and middleware providers. This will squeeze the margins available to the current crop of big names (witness Google trying to merge personal data from all its offerings) with smaller firms acting as niche and some competing on luxury/ease of use (e.g. Apple). Service offerings will primarily provide a mix of ‘computer replacement services’ – largely SaaS and storage, with some growth in CaaS as a result of the increased uptake of cloud services by SMEs. PaaS will remain a niche offering, used primarily by providers of cloud-hosted services and cloud-enhanced services. High-value and high-security enterprise uses will remain largely separate due to continuing concerns about security and control in public clouds. Because they are governed by internal provision and/or negotiated B2B SLAs, they raise few additional regulatory concerns. On the positive side, the rapid expansion of public cloud services and the relatively high returns to network providers combine to increase private sector willingness to pay for creating and maintaining the necessary high-speed communications infrastructure. Finally, the future Internet will continue to support cloud services as one among a host of uses; it is an open question whether the promise of greater security and reliability will drive cloud computing to become a central use case influencing the architecture and performance of the Future Internet.

Under this scenario, existing regulatory approaches continue to try to address consumer and citizen harms, based on a reactive and *ad-hoc* approach to events (e.g. outages or losses of personal data from the cloud). Largely in view of the dominance of players coming under telecommunications NRAs, regulation throughout the world is coordinated primarily at the national level; in view of the continued share of public clouds, this focuses primarily on consumer concerns as assumed in the main body of the Report.

Describing the scenario as merely a continuation of the *status quo ante* without new regulatory intervention overlooks the possibility that things may change due to future ‘shocks.’ A major incident like a cloud based version of the recent Sony Online Entertainment loss of personal data from the cloud; or alternatively, global efforts to reinforce existing models of copyright licensing and enforcement may trigger either a marked strengthening or weakening of regulatory activity in this area. Possible first signs of disillusionment, ahead of the much vaunted Facebook Initial Public Offering, can be seen with the tailing off in numbers of Facebook users (although this might also be due to saturation or diminishing returns).

Existing regulatory regimes may continue to operate in sub-optimal and fragmented fashion with telecommunications regulators adopting a consumer protection perspective, data protection authorities looking into how cloud service providers address privacy and data protection obligations and security and law enforcement agencies providing guidance on managing the risks of cloud use. As the cloud spreads
and becomes more sophisticated, this separation may no longer provide adequate governance, especially if cloud development and provider business models are strongly driven by specific incidents.

**Rationale for regulatory intervention**

In an increasingly-complicated and contested regulatory space, it is an open issue as to whether regulators can ensure that their perspectives are appropriately reflected in the decisions of other regulatory (including self-regulatory) bodies, and that, in turn, it is able to take other policy objectives appropriately into account when exercising its own powers.

**Scenario 3: Clouds as a new critical infrastructure**

*Key elements:* Security, continuity, reliability trump economic efficiency; citizen harms outweigh consumer harms.

**Background**

Currently, cloud computing is viewed as an unlikely candidate for critical infrastructure, due to perceived security weaknesses (confidentiality, availability and data integrity) and regulatory interest. However, these concerns apply primarily to public clouds. In other sectors (e.g. financial services[^131], healthcare) we already see increasing use of and reliance upon private clouds. As margins in some of these highly regulated sectors become ever thinner, owner-operators of critical infrastructure will seek cost savings where possible, making private cloud deployments an important use case. Regulators might need to consider whether they can adequately identify and control use of cloud computing (and even whether it is necessary to require critical infrastructure owner-operators not to use cloud computing). Another example comes from bio-surveillance, where Google[^132] is using analytics in the cloud to predict more accurately global disease pandemics through analysis of user generated content across its B2C cloud platforms. Such initiatives compete with ‘traditional’ government supported bio-vigilance efforts, for example the European Centre for Disease Prevention and Control. Should these cloud based sources of ‘intelligence’ (used for a variety of requirements, even traditional intelligence[^133]) become *de-facto* then they would constitute a critical infrastructure and therefore be of greater regulatory interest. There is also the use case of cloud computing being used as a way to conduct Disaster Recovery/Business Continuity Management (DR/BCM) tests since it is possible to easily have a ‘hot site’[^134] parked in the cloud to test BCM plans and procedures. The implications are stark; should these need to be activated, they then might become central to the resilience of the operations of critical infrastructure (in addition to being instrumental in providing a level of assurance regarding the success of DR/BCM planning).

Firstly (and most importantly), in relation to sovereignty over cloud regulation, it is clear that in some of the highly regulated Critical Infrastructure sectors (telecommunications, finance and energy), pre-eminent regulatory roles are already established. However, the broader use of cloud computing in these domains might require interaction with those more qualified to advise on the security and resilience aspects (e.g. in the UK the Centre for the Protection of the National Infrastructure). As efforts develop to move from national definitions, policy and regulation of critical infrastructure (e.g. via self-regulatory ‘light touch’ approaches in the US and UK) to supra-national approaches (e.g. with the revision of the EU European Critical Infrastructure Directive) regulatory sovereignty might move to be more international.


[^132]: E.g. Carneiro and Mylonakis (2009)


[^134]: A mirror image of IT systems ready for instantaneous activation in the event of a failure in main systems
With respect to the concentration in cloud services, the B2C and enterprise characteristics of this scenario point to the large systems integrators and major IT companies trying to move into the enterprise space as the dominant firms. However, for the foreseeable future control will remain with the dominant providers of hypervisor middleware that determine the resilience and availability of cloud services as a whole (currently, this is VMWare, but the Microsoft/Citrix alliance is also likely to play a large role).

From a regulatory perspective, the critical infrastructure core of cloud deployment is primarily provided as private/enterprise clouds; with the regulatory protection afforded by their centrality, they are able to compete successfully for citizen and consumer business as well. This reinforces the status of cloud service providers, because the impacts of a loss of critical infrastructure might be most clearly felt by citizens and consumers (according to the broad definition of critical infrastructure as those vital infrastructures whose loss would have major economic or social impacts), both in terms of B2C cloud services and through the growing reliance of other critical national infrastructures on cloud-hosted services (see further Sections 3.2 and esp. 4.2.4).

The Future Internet dimension is less important in this scenario, because the criticality of cloud computing is likely to be seen as a development of the current status of telecommunications and Internet services.

**Rationale for regulatory intervention**

Although the examples are within the scope of B2B and enterprise use of clouds the implications of an outage go beyond managing business interruption. If critical infrastructure fails, then there are broader implications for society such as economic damage and possible other human related impacts.
## C. Relation to issues

Table 11: Citizen and consumer harm issues in three scenarios

<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Cloud-max</th>
<th>Nothing new</th>
<th>Another critical infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer switching and mobility</td>
<td>Consumers may be locked into cloud service providers by limited portability of their data and applications, restricted interoperability, lack of information</td>
<td>Medium concern; mobility is at the core of the new architecture, but business models may restrict migration.</td>
<td>High concern: existing cloud models continue to evolve toward fragmentation of service offerings and high switching costs. Regulators find it difficult to determine if ad-hoc efforts by firms (e.g. Google’s Data Liberation Front) are honest or a form of regulatory foreclosure.</td>
<td>Low concern: consumer has little say or consequence for cloud based services using CII. However, for citizens there are similar impacts as might be considered by vulnerabilities in SCADA systems. Regulators have trouble intervening to link use of the cloud to citizen harms.</td>
</tr>
<tr>
<td>Copyright and IPR</td>
<td>i) liability of Cloud Service Providers for actions of users and hosted service providers; ii) ownership of user-generated content; iii) content-matching and legitimisation; etc.</td>
<td>The use of bulk transfers and the detailed accounting kept by users’ ‘home’ data centres limit regulatory concern.</td>
<td>Pressure from copyright owners and publishers (as shown by lobbying efforts for SOPA, PIPA, IP-Protect and ACTA) suggest that those providing content matching services ‘in the cloud’ may come under increased interest.</td>
<td>n/a</td>
</tr>
<tr>
<td>Unfair and potentially anti-competitive contract terms</td>
<td>Standard form SLAs are efficient for large numbers of consumers but prevent bargaining. This raises switching costs and can lead to lock-in, damage competition, reduce efficiency. More serious for cloud because providers ‘have’ user data.</td>
<td>Cloud service agreements must allow customised access, transfer, and other preferences to be negotiated and enforced; otherwise the benefits of the new architecture will be limited.</td>
<td>Continued absence of regulatory intervention on trying to establish more balanced standard form SLAs for consumers</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Issues</strong></td>
<td><strong>Description</strong></td>
<td><strong>Cloud-max</strong></td>
<td><strong>Nothing new</strong></td>
<td><strong>Another critical infrastructure</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Security, reliability, resilience capacity</td>
<td>Concerns: a) transparency of cloud providers’ practices; b) security and reliability of services; c) data loss and unauthorised release - even when not illegal, this can create significant harm, especially when data owners are not aware; d) Data security includes e.g. infrastructure resilience (continuity), authentication.</td>
<td>Security and reliability concerns are concentrated in the core and access layers; this scenario allows end-to-end security of data transfers, so the critical uncertainty concerns the resilience and security of the network itself (data centres are a secondary source of concern).</td>
<td>Reported interpretation of consumers concerns continues to suggest that security and confidentiality are high on the list and for certain instances cloud service providers play to this market. However, in general the limited bargaining power remains. We may see market entrants appearing who aggregate consumer concerns about security to repackage demand to enable ‘class level’ negotiation with cloud service providers.</td>
<td>Interest will come from the regulators in this respect: consumers won’t know about it since details will be buried deep in organisational IT architecture (but consequences may be felt more broadly).</td>
</tr>
<tr>
<td>Crime</td>
<td>Range of criminal threats: i) Identity theft; ii) Data theft; iii) Fraud; iv) Malicious system, processing or data interference; v) Data loss or unauthorised release.</td>
<td>Should be managed within the core network where access requests and processing are located.</td>
<td>Possible blurring of the boundaries between criminal data centre operations (‘bullet proof hosts’) and plain incompetent cloud based service providers. Test cases may appear for cloud based crime-ware.</td>
<td>Greater concern of data theft (IPR losses) and data manipulation arise the interest of regulators</td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy may be weakened by indirect relationships, limited visibility, mismatch with legal roles, privacy-invasive technologies and business models.</td>
<td>Access and activity logs are a potential weak point; market value of private information combined with prevalence of market/self-regulation magnifies this vulnerability.</td>
<td>Current approaches to privacy regulation, despite agreement on broad global principles mean there is enough of a mismatch that a gap exists for some Identity as a Service (e.g. intermediaries). Increased regulatory interest (e.g. by the UK ICO toward Google) may catch bigger firms but there remain enough other players for invasions of privacy to constitute a concern for regulators</td>
<td>Privacy is trumped by security (only in private clouds). ISP role becomes more of interest to regulators to ensure access to clouds as ‘basic’ right (e.g. in respect of ISPs doing DPI).</td>
</tr>
<tr>
<td>Issues</td>
<td>Description</td>
<td>Cloud-max</td>
<td>Nothing new</td>
<td>Another critical infrastructure</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Communications as a Service (CaaS)</td>
<td>Integrated or converged video, voice and data communications and associated services that overlap with existing regulated communications but are not limited to communications service providers.</td>
<td>Some proposals for unification of communications regulation across conventional and (cloud-centric) Internet channels as an extension of the 'converged regulator' tendency of recent years.</td>
<td>Possibility of extending communications service definitions and regulation on an application-specific basis (as with VOIP to date)</td>
<td>Specific need to examine implications for emergency communications, continuity of consumer communications.</td>
</tr>
<tr>
<td>Cloud as a utility (including risk of foreclosure)</td>
<td>Aspects of cloud computing share some technical, economic and societal features with other utilities (e.g. economies of scale and potential for universal service)</td>
<td>Strong case for utility regulation of core services and 'common-carriage' rules for transit traffic (bulk data transfers).</td>
<td>n/a</td>
<td>Strong concern: regulators will be ever interested in the extent to which they can establish oversight of cloud service providers operating in the CII space (witness current discussion in US over regulation for cybersecurity)</td>
</tr>
<tr>
<td>Advertising and marketing</td>
<td>Consumers may not be fully informed; may see repeat of problems with e.g. broadband or mobile. Providers may be unable to certify, deliver or even inform consumers about the services they expect and those they receive.</td>
<td>Consumers face new choices of access, migration, caching preferences; potential for confusing 'roaming' pricing</td>
<td>Consumers may be faced with fragmented market, resulting in trusted brands expanding their dominant position. An independent Which? type organisation may appear (e.g. broadbandchecker) to provide easy to use interpretation of cloud service offerings</td>
<td>n/a</td>
</tr>
</tbody>
</table>