INTERNATIONAL TELECOMMUNICATION UNION

GSR 2012 Discussion Paper

Demystifying Regulation in the Cloud:

Opportunities and Challenges for Cloud Computing

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October 2012.

TABLE OF CONTENTS

1 DEMYSTIFYING REGULATION IN THE CLOUD: OPPORTUNITIES AND CHALLENGES FOR CLOUD COMPUTING

Professor Ian Walden, Queen Mary, University of London and Baker & McKenzie

1. Introduction

> "The rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the information technology (IT) industry, but it will also profoundly change the way people work and companies operate. It will allow digital technology to penetrate every nook and cranny of the economy and of society, creating some tricky political problems along the way."
>
> Source: Economist, 'Let it rise', 23 October 2008.

With the emergence of ubiquitous broadband connectivity, cloud computing offers an alternative platform from which Information and Communications Technologies (ICT) providers can offer powerful and innovative new services, while providing users with the opportunity to gain access to computational resources and applications beyond those traditionally feasible. It challenges our perception of how to utilize and exploit ICT to engage economically and socially more efficiently and effectively. Uncertainties over the legal and regulatory treatment of cloud computing may, however, act as an obstacle to its adoption.

This paper considers the cloud computing phenomenon, from a technical, market and social perspective, and examines its legal implications, the role of regulation and regulators and how policy makers can create an environment conducive to its take-up.

2. Cloud technologies

Cloud computing has emerged over recent years as the latest manifestation of networked computing. It represents a shift in computing power from so-called 'thick client' solutions, whereby the applications used are present on personal computers while the data may be hosted and shared on a remote server, to a 'thin client' environment, where both the applications and the data reside on the remote server. This trend is being made possible by the widespread availability of fast resilient communication networks over which data can be transmitted. To an extent, the shift represents a return to the early years of computing, when mainframes dominated the environment and where access took place through 'dumb' terminals.

Cloud computing is not a single technological solution, but is rather an umbrella term used to describe a range of different technologies and market offerings. Numerous definitions of cloud computing exist[1], often reflecting the different perspectives of providers and users. The ITU, for example, defines cloud computing in the following terms:

> "A model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and ser-

vices), that can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud computing enables cloud services."[2]

For the purposes of this paper, the following definition is used:

"Cloud computing provides flexible, location-independent access to computing resources that are quickly and transparently allocated or released in response to demand.

Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.

Charging is commonly on an access basis, often in proportion to the resources used."[3]

Examining the different elements of this definition in further detail helps to better understand how cloud computing differs from other forms of IT services, such as outsourcing. First, 'flexibility' means that the computing resources are available to the user as and when needed, on-demand, with the associated efficiencies for both the user and provider, rather than fixed and dedicated for the customer[4]. Second, 'location-independence' is possible as a result of the 'death of distance'[5] made possible by modern communication networks, such as the internet. Third, 'virtualised' services means that the resources created for users, such as storage, operating systems and applications, are distinct from the underlying actual physical resources on which they operate, such as a server farm. Virtual machines emulating physical machines. Fourth, the actual physical resources provided by the service providers are 'shared' by the customers, again resulting in more efficient use of the infrastructure. In certain situations, the customer may be unwilling to share with other customers, due to security concerns. As such, 'private' cloud services may be utilized, whereby the resource is dedicated for a single user or shared by a restricted community rather than available to the public', or a 'hybrid' cloud service, where certain resources are restricted, while others are public[6]. Finally, the reference to 'charging' reflects the fact that 'public' cloud services are generally purchased on a commodity-basis, on the provider's standard terms and conditions, rather than individualized and negotiated agreements, as is usually the case in IT outsourcing.

2.1 Cloud opportunities

What is driving the take-up of cloud computing? As with any area of business, the ability to reduce costs and increase productivity often lies at the heart of the decision to adopt cloud solutions. Cloud computing offers general business and organizational benefits, as well as benefits in the exploitation of ICTs[7].

Similar to IT outsourcing, cloud computing can offer users substantial cost savings over traditional models of ICT ownership. From a cloud user's perspective, such savings can arise in four key areas:

- Labour costs, as fewer ICT-dedicated personnel are required by enterprises;
- Energy efficiencies, from not having to operate the hardware resources to service the needs of the enterprise;
- Real estate, from requiring less space for the ICT equipment, and
- Usage licences, through the shift from End-user licences to service-based delivery[8].

It is these cost savings and others that have led policy makers to enthusiastically embrace cloud computing: "The medicine needed for our credit squeezed economy"[9].

The scalability of cloud services enables increased productivity and improved responsiveness to changing customer demands and market conditions. It reduces risk for organizations, enabling them to trial new ideas and processes without the need to invest heavily in new technologies. In particular, cloud can facilitate new means of collaborative working practices, reflecting in part models from the open source community, both within and between organizations.

2.2 Cloud challenges

What barriers exist to the uptake of cloud computing? One leading concern is data security, the trust, reliability and dependency in moving data and applications to a remote third party. While such concerns are real and need to be adequately addressed, as discussed further below and in the paper on cloud privacy[10], they are in part also cultural, requiring a change in attitude about how to use ICT systems. In 1999, Scott McNealy, then head of Sun Microsystems, made the infamous statement about online privacy: "You have zero privacy anyway. Get over it!". This could be rephrased for a cloud environment as: "Everything is shared. Get over it!". Altering cultural attitudes to embrace innovative ICT solutions can sometimes be as difficult as addressing the technical challenges.

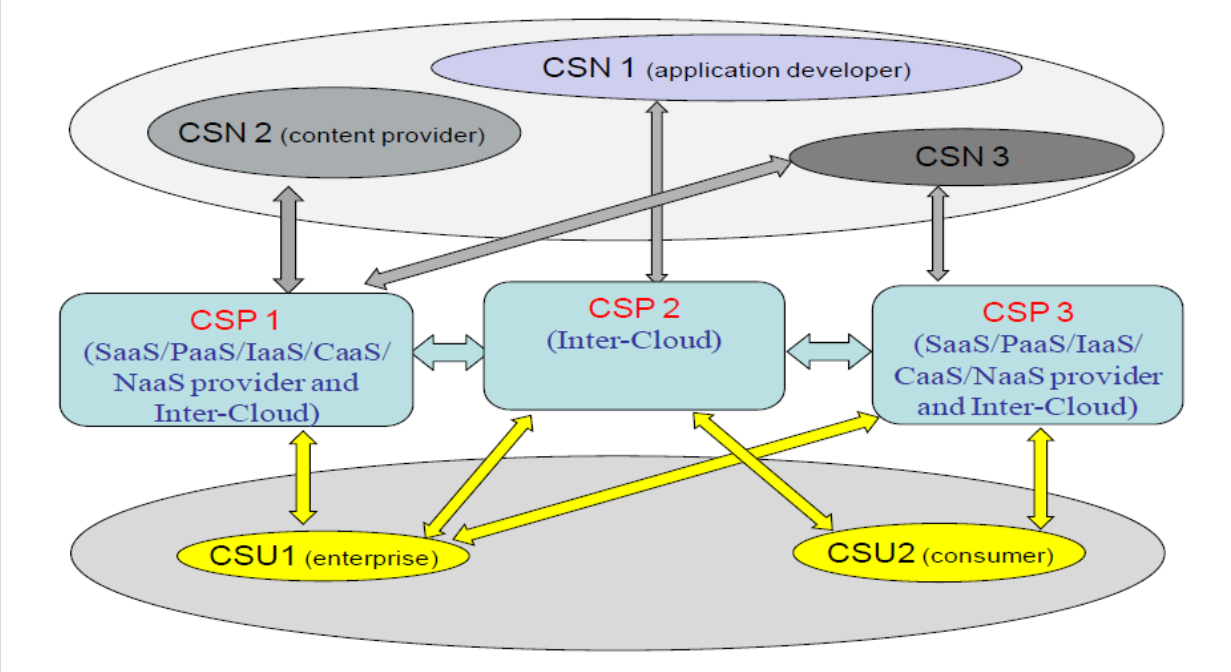
Another barrier for cloud computing is the availability of connectivity and sufficient bandwidth. Accessing a cloud service 'anytime, anyplace, anywhere' requires a robust telecommunications infrastructure and network access. The past 30 years of market liberalization and technical development have enabled this in many parts of the world, especially with the current deployment of broadband next generation networks ('NGNs'), satellite and 4G (IMT Advanced) wireless network infrastructures. However, adequate connectivity remains a problem in all countries, although it remains significantly challenging in the developing world.

For large users, enterprises and public authorities, the adoption of cloud computing is likely to be piecemeal. Users will trial services for particular applications, such as email, before committing wholesale to a cloud solution for most, if not all, their ICT needs. As such, interoperability and compatibility with legacy technology can also be a barrier for cloud users. In IT outsourcing, the provider will generally take on responsibility for the legacy technology and will migrate users on to any alternative solution. In cloud, the user often remains responsible for integrating the legacy systems and the cloud services.

Legal and regulatory uncertainty can also present a barrier to cloud adoption. In large part, these uncertainties arise in a 'public cloud' environment, where users are less able to influence the technical architecture that underpins the cloud service. Uncertainties about information ownership and control may inhibit users from placing their data with third parties. The transborder nature of cloud creates uncertainties about applicable law, similar to that for other internet services. A different jurisdictional approach to key legal issues, such as the protection of personal data between Europe and the US, can generate uncertainties about whether the use of cloud services can be carried out in a compliant manner.

The regulatory characterization and treatment of cloud computing may itself deter its take-up until regulators clarify the situation. Closely related to such uncertainty is the determination of competence in respect of the regulation of the cloud market. If viewed as a telecommunications service, then the telecom regulator can exercise jurisdiction. Conversely, if cloud is seen as an information service, then competence may lie with the ICT regulator, if there is one, or potentially the media regulator. Such sectoral regulation may then have to operate in conjunction and co-operation with horizontal national regulators, such as a data protection authority, in respect of certain issues.

Box 1: Actors with some of their possible roles in a cloud ecosystem



Source: ITU-T FG Cloud Technical Report Part 1, Introduction to the cloud ecosystem *(02/2012).*

3. Cloud markets

Since cloud services are varied, and becoming increasingly differentiated, so the markets that they supply are diverse, from wholesale to retail, business, public sector, as well as consumer. Increasing numbers of IT companies are either establishing new 'cloud' services or are recasting existing services as 'cloud'. The most common categorization of cloud services is into three: Software as a Service ('SaaS'), Platform as a Service ('PaaS') and Infrastructure as a Service ('IaaS'); although the label, 'X as a Service', is now being used for a range of different services[11].

SaaS primarily involves the use of remote applications by end-users, including productivity-related applications, such as Google Docs and Microsoft's Office 365; social networking, such as Facebook and MySpace, and the delivery 'over the top' ('OTT') content, such as video-on-demand services. PaaS are typically targeted at developers, enabling collaborative application development, such as open source software communities. IaaS generally involves the provision of virtual machines, offering processing and storage capacity.

The cloud computing market also comprises layers of different technologies, often supplied by diverse companies within the supply chain (e.g. Apple's iCloud SaaS is hosted on Amazon IaaS). Cloud users' depend on various 'service providers' for their use of the cloud, of which three broad categories are distinguished for the purposes of this paper[12]:

- A cloud service provider ('CSP'), who has a direct contractual relationship with the subscriber to the service, whether offering a SaaS, PaaS, IaaS or other variant;
- A cloud infrastructure provider ('CIP'), who provides the cloud service provider with some form of infrastructure[13], such as server farms and processing capacity, including persistent storage;
- A communication service provider, who provides the transmission service enabling the cloud user to communicate with the cloud service provider.

Usually, the cloud user will only contract directly with the cloud service provider and the communication service provider, the 'stack' of suppliers comprising the cloud service often being opaque to the user. This, in itself, may represent a risk for the user, since they may not be aware of the chain of contracts that underpin the provision of the service and, significantly, whether commitments entered into by the contracting service provider are adequately reflected down the supply chain. Alternatively, a user may contract with a systems integrator, which provides all aspects of the service, which is more akin to a traditional outsourcing arrangement.

4. Cloud as a regulated activity

How should cloud be characterized from a regulatory perspective? The answer to this question, as in many areas of regulation, is: it depends! The following examines some key areas of regulation, other than privacy and data protection, which are addressed in another GSR Discussion Paper[14].

4.1 Telecommunications law

Of the three categories of provider adopted earlier, clearly the communication service provider will be governed by telecommunication law, national, regional and international. Whether the cloud service provider or cloud infrastructure provider can be so characterized will depend on the nature of the service being provided. Under European law, for example, the primary regulated activities in the communications sector are the provision of 'electronic communication networks' and 'electronic communication services'[15]. The former comprise transmission systems, including 'switching and routing equipment' that enable the conveyance of signals; the latter consists 'mainly in the conveyance of signals'[16]. In many, if not most, cases, while cloud services are dependent on telecommunications networks and services for communicating with their customers, such services are not *per se* characterized as being networks and services. However, a cloud service provider may offer a SaaS application that provides call-handling functionality for an enterprise, which is analogous to a PBX[17], and this could be regarded an either a regulated network or service. In addition, the utility and shared nature of much cloud provision would also render it a 'public' network or service, thereby subject to a broader range of compliance obligations than applicable to equivalent 'private' services.

Uncertainty about the regulatory treatment of cloud services echoes previous experience with other emerging communication technologies, such as Voice over IP ('VoIP'). When VoIP applications first emerged in the mid-1990s for PC to PC communication, they were generally treated as a form of software, rather than a communication service[18]. As VoIP emerged as a major platform for voice communications across public networks and usage became widespread, there was recognition that uncertainty over its regulatory treatment created vulnerabilities for consumers, in areas such as network integrity and emergency call access, and market distortions, undermining the value of network investments carried out by traditional network operators[19]. In response to this uncertainty, regulators, such as those in the EU, kept a watching brief on market developments; developed a harmonized approach to the handling of certain emerging issues of concern, such as numbering, competition rules and applied existing regulations on a technology-neutral basis[20].

Drawing analogies between VoIP and cloud computing is limited to the extent that cloud computing services currently primarily provide remote alternatives to the desktop computer, i.e. terminal equipment at the edges of the network, rather than communication services. However, as noted above, some SaaS applications are specifically designed to replicate network functionalities, which places them within the regulated sphere of telecommunications. In addition, similar to VoIP, the 'born digital' generation may increasingly view cloud services, especially social networking, as the primary communication platform, utilizing 'always-on' connectivity services, which can give rise to regulatory concerns, such as interoperability and data portability, that are similar to issues addressed under telecommunications regulation, i.e. interconnection and number portability[21].

From a public policy perspective, it is arguable whether future telecommunications law may need to recast its traditional regulatory definitions and boundaries; shifting the focus from purely technical concepts, such as the transmission of signals, to a more market-based approach, encompassing the intention of service providers and expectations of the consumer.

4.2 Consumer protection law

In response to most market developments, comprehensive national consumer protection laws, governing issues from advertising to mandatory rights and obligations, will usually be sufficient to control unfair and abusive practices. However, such laws may need to be reformed and updated to reflect the general shift from traditional products and services to embrace the unique challenges of digital information and services, such as cloud.

In addition, sectoral consumer protection laws may also sometimes be necessary to address the particular needs of the sector. In telecommunications, for example, regulatory best practice has meant that most liberalized markets have adopted some level of sectoral rules governing the relationship between service providers and subscribers. Such consumer protection rules are generally designed to meet one of two objectives. First, certain rules facilitate market liberalization and help maintain competition from a demand-side, such as number portability and transparency obligations. Second, the nature of telecommunication as a 'utility-like' service[22], similar in kind to energy and water, has meant the governments have recognized the need to intervene not only to ensure access, through universal service policies, but also to regulate the terms of such access, through imposing minimum standards in the contractual relationship.

While the cloud computing market is not directly analogous to the telecommunications sector, policy makers have recognized a potential need to intervene[23]. On the one hand, as noted earlier, communications-like cloud services, such as social networks, are viewed by many as critical platforms from which to engage in social and economic activity, offering services upon which they are increasingly dependent. On the other, as noted below, market developments may result in the emergence of data-handling practices designed to inhibit consumers from exercising choice and moving between service providers.

As cloud services become widespread, consumer protection authorities are increasingly being called upon to intervene to protect the interests of consumers from abusive and deceptive practices. In the UK, for example, the Advertising Standards Authority has found against a cloud hosting provider who misleadingly advertised 'unlimited packages', when limitations in server capacity meant that certain customers had been unable to utilize the service[24]. Similarly, a web-hosting company was held to have mislead by claiming a '99.99 Uptime Guarantee', which it could not substantiate in the face of a customer complaint that they had suffered 3 significant network failures in a 3 month period[25]. While in France, a court has held that a Facebook user is not bound by the dispute resolution provision in Facebook's standard terms that requires all disputes be brought exclusively before "a state or federal court located in Santa Clara County"[26]. The court ruled that the provision was not brought sufficiently to the attention of the user to be binding, in breach of the French Code of Civil Procedure[27].

Another concern that cloud users may have when placing data in the cloud is the possibility of 'lock-in', where it becomes difficult to retrieve the data in a suitable format to enable it to be moved to a competing provider. Data portability is an emerging issue in the cloud computing sector that has relevance for competitive nature of the cloud market as a demand-side measure; similar in nature to number portability obligations in telecommunications[28]. Migration from one cloud service to another may be restricted pursuant to the terms of an agreement with a cloud service provider or difficult due to technical incompatibility[29]. Moreover, were a service provider to include in its standard terms conditions that constrain a customer from porting, replicating or backing-up data, this would raise concerns from a competition law as well as a consumer protection perspective. Such terms may be deemed to be in breach of competition law if they either are not necessary for providing the service, result in barriers to entry, distort competition and harm consumers. Rights of data portability would reduce lock-in effects and require competitors to compete for their existing customers as well as increasing their customer base.

The European Commission is aware of the potential harm that may arise from a customer's inability to port their data, but grounded in concerns about individual privacy, rather than from a competition law or consumer protection perspective. In January 2012, the Commission published a proposal to reform the current regime in the European Union[30]. Among other things, it contains a proposal that a right of data portability be recognized as an individual right within a privacy context. According to the Commission, an individual should have the right to withdraw his own personal data and "any other information provided by the data subject", from an application or

service and transfer such data into another application or service, as far as this is technically feasible.[31] To facilitate such portability, the Commission has reserved the right to specify the 'electronic format' in which the data should be provided, as well as the "technical standards, modalities and procedures for the transmission" of the data[32].

Recognition of data portability as an individual right *per se* would mean it is not necessary to evidence a resulting harm to competition. The Commission proposal suggests that the simple fact that customers are being prevented from transferring their personal data from one application or service to another would be enough to justify action aimed at forcing providers to guarantee data portability, if it would be technically feasible. Thus, regulating data portability in the cloud computing sector could prove to be more effective and straightforward via the enforcement of data portability rights under the umbrella of data protection policy than via the enforcement of competition law.

4.3 Competition law

Consumer issues concerning data portability may reflect broader concerns about the competitive nature of the cloud market, which may trigger intervention by competition regulators. Provider 'lock-in' may occur within any segment of the cloud market, SaaS, PaaS or IaaS, inhibiting the movement of data, applications and/or services. Anti-competitive effects may arise from a range of behaviours[33].

It can result from a lack of industry standards or, conversely, the development of de facto standard attributable to a marker leader, such as Amazon APIs[34]. Restrictive licence conditions may also as a result undermine competition. In April 2010, for example, Apple imposed restrictions pursuant to the terms and conditions of its licence agreements with independent developers of iPhone Apps. Apple required the exclusive use of Apple's native programming tools and approved languages for the development of iPhone Apps. Imposing such restrictions was considered by the European Commission as a conduct which could result in harm to competition for platforms that competed with Apple's Apps platform. As a result of preliminary investigations by the Commission, in September 2010, Apple voluntarily announced the removal of the restrictions, therefore allowing third-party application development environments to be used to submit Apps, resulting in greater flexibility to developers.[35]

Market participants in related sectors may constrain customers from move to a cloud platform. In July 2010, for example, the European Commission launched an investigation regarding IBM's computer mainframes.[36] IBM is being investigated for two practices in this sector: tying its mainframe hardware to its mainframe operating system and discriminatory behaviour towards competing suppliers of mainframe maintenance services.[37] IBM is being suspected of using its dominance in the mainframe operating system to leverage its position in the hardware market.[38] If proven, IBM's conduct is likely to make it more difficult for existing customers to migrate their data and applications to public cloud services, which do not require the purchase of vast amounts of hardware and software as IBM's private clouds.

Public procurement practices may be another source of anti-competitive behaviour. An example of this situation can be found in the US case of *Google v United States Interior Department*.[39] In October 2010, Google filed a claim against the U.S. Interior Department alleging that its public procurement practices illegally distorted competition by requiring, in relation to a US$59 million contract for ICT services, messaging technologies to be based on Microsoft Business Productivity Online Suite, therefore excluding Google from public procurements and restricting competition. The court granted an interim injunction in favour of Google and stated that the U.S. Interior Department's public procurement practices violated competition rules, therefore requiring the defendant to modify the procurement criteria.[40] Although the judgment did not find bad faith or wrong doing by Microsoft, it in effect brought to a halt the deployment of Microsoft's Business Productivity Online Services cloud computing solution and e-mail system at the U.S. Interior Department. The decision was intended to avoid lock-in effects and harm to competition given that without a preliminary injunction, the award would put into motion the final migration of Interior's email system, achieve 'organizational lock-in' for Microsoft, and cost Google the opportunity to compete.[41] The court therefore considered the possible harm to a competitor and to competition resulting from the network effects that would have been created by giving preference to Microsoft in public procurement.

Finally, it should be noted that there may be competition issues not only in the service cloud, but also in the infrastructure layers upon which cloud services are built and depend. In particular, there may be competition issues at the network level, which impinge on end-user access to cloud services, from unbundling issues to 'network neutrality'. Access to cloud services is provided by telecommunication companies that have historically been part of concentrated markets, which have developed from previous State-owned incumbent monopolies[42]. Connectivity, in terms of availability and affordability, is a concern not only in developing economies, but also in countries where the policy of market liberalization has not sufficiently eroded the market power of the incumbent operators. These issues are being addressed by telecommunications policy makers and regulators, through policies such as 'open access' that ensure fair and equivalent access for service providers, including cloud, to bottleneck facilities at an infrastructure level[43].

Telecoms regulators in many jurisdictions are highly experienced at working with industry to manage the process of number portability, especially in determining the technical, operational and cost implications[44]. As such, were data and application portability to be pursued as part of a policy initiative to promote cloud computing, whether under the auspices of competition law or consumer protection, it would obviously make sense to build on such experience.

4.4 Environmental concerns

As well as being directly subject to a regulatory regime, such as for telecommunications, the provision of cloud services may trigger other regulatory concerns. As noted earlier, one key advantage of cloud services is the efficiencies achievable by the cloud user in terms of equipment and real estate. On the other hand, however, the large data centers operated by CSPs and CIPs consume vast amounts of energy, which raises its own concerns in terms of energy and environmental policy. A recent report by MusicTank, for example, argues that 'close-to-consumer' cloud storage solutions may be needed to reduce the environment impact of online music streaming services. The report suggests that YouTube alone accounted for 0.1% of global energy consumption[45].

To address environmental concerns, steps have been taken to encourage the operators of such data centres to minimize energy usage whilst providing innovate services offerings. In 2009, for example, the European Commission issued a Code of Conduct on Data Centres Energy Efficiency[46] , which is a set of voluntary measures that may be adopted or reflected in the service contract, whereby the provider commits to achieving certain efficiencies in the design and operation of data centers. Such standards may eventually become mandated through legislation.

Mechanisms for reducing energy costs include building data centers where natural and passive cooling is available. In 2009, for example, Google was granted a patent in the US for the following invention:

> "a floating platform-mounted computer data center comprising a plurality of computing units, a sea-based electrical generator in electrical connection with the plurality of computing units, and one or more sea-water cooling units for providing cooling to the plurality of computing units."[47].

Distributed storage techniques widely used in cloud computing, such as 'sharding' or 'partitioning', mean that data processing loads can also be shifted to geographical zones where power is cheap. Similarly, the flexible architecture of cloud enables redundancy to be reduced to a minimum.

4.5 Jurisdictional concerns

An additional layer of concern for regulators is the transnational nature of cloud computing, which results in a multiplicity of jurisdictions potentially 'competing' to govern the regulated activity. The movement of data into and out of a cloud service will often, as with other network-based applications, result in the data becoming subject to the rules of both the cloud user's jurisdiction and the cloud service provider, as well as any cloud infrastructure providers. The transfer of data out of the user's jurisdiction can be opaque to the user, raising issues of control and, for the national regulator, effective oversight. For some regulated sectors, such as financial services, cloud-related transfers and storage outside the jurisdiction of the regulated entity may itself breach national rules[48].

Issues of national sovereignty mean that national regulators are unlikely to be willing to surrender jurisdiction to a foreign authority, unless adequate mutual recognition arrangements are in place[49]. As such, it will require greater transparency and co-operation between national regulators to resolve conflicts of law and regulation in a cloud environment.

5. Regulatory environment

Given the benefits of cloud, governments have an inevitable interest in both facilitating its adoption in the economy, as well as utilizing it for the provision of its own e-government activities, i.e. the 'G-Cloud'[50]. Government and regulatory intervention in markets can be designed both to constrain harmful behaviours as well as facilitate beneficial behaviours. As such, policy, law and regulation can play an important role in the facilitation of cloud services. This section examines different regulatory aspects in a cloud environment that is inherently transnational, from public policy responses to private law governance through contract; a form of self-regulation.

National telecommunication regulators can, in particular, play a key role in facilitating a regulatory environment conducive to cloud computing. In addition to their experience with respect to number portability, noted above, they will also generally have experience of developing and promoting industry standards and best practice, as well as consumer protection issues, specifically in relation to the provider-consumer contractual relationship. As such, governments should look to take advantage of this experience. While much of the cloud computing market may fall outside the competence of telecoms regulators, the critical need for extensive and robust network connectivity lies directly within their remit.

5.1 Regulation as facilitation

Governments and regulators can facilitate the development of cloud computing; while removing perceived obstacles to its adoption. By improving the environment for the supply of cloud services, the cloud market as a whole will grow. Policy makers are obviously cognizant of cloud computing and its potential economic and social impact and are considering the right strategy to embrace and harness the cloud[51]. The general principle appears to be, as with developments in relation to the internet, to ensure that what occurs in the cloud does not fall outside existing legal rules and controls: "The cloud must be a place where everyone's rights are duly respected and enforced."[52]

But what measures should governments take to facilitate the provision and adoption of cloud computing? The Business Software Alliance (BSA) recently published a survey of 24 countries to identify the level of 'cloud readiness' in countries, based on the domestic policies and initiatives towards cloud computing[53]. Each country was given a score based on an index of seven policy areas that the BSA considers beneficial to cloud adoption: privacy protection, information security, cybercrime measures, protecting intellectual property, ensuring data portability, liberalized trade rules and the necessary IT infrastructure.

The survey identified a sharp divide in cloud readiness between advanced economies, with Japan considered the leader, and developing countries, including India, China and Brazil. For India, poor progress towards a national broadband network is a key factor undermining the adoption of cloud. In China, its restrictive policy on Internet content and discriminatory approach to foreign technology companies is seen as presenting obstacles to cloud, despite dramatic growth in the ITC sector over recent years. Brazil is seen as lacking an appropriate framework for the development of ICT standards, as well as giving domestic service providers preferential treatment in public procurement.

Table: European Cloud Policies

In May 2012, the European Parliament published a study on cloud computing that identified five areas where policy makers should take action to facilitate cloud computing:

- *Address legislation-related gaps* – e.g. providing for the possibility of collective redress against security and privacy breaches in the cloud;
- *Improve terms and conditions for all users* – e.g. develop model contracts to ensure that user interests are better represented;
- *Address stakeholder security concerns* – e.g. the feasibility of independent auditing and certification systems;
- *Encourage the public sector cloud* – e.g. through integrating cloud computing in e-government plans;
- *Promote further research and development in cloud computing* – e.g. on the economic and environmental impact of cloud computing

Source: European Commission, Directorate General for internal Policies, IP/A/IMCO/ST/2011-18, May 2012

To what extent is cloud likely to offer developing countries opportunities for economic growth? In terms of the building of processing capacity, the large server farms that characterize current public cloud provision, developing countries obviously may offer relatively cheap real estate. However, in terms of access to reliable power generation and broadband communications, developing countries often lack the necessary infrastructure. While mobile penetration in Africa is substantial, fixed broadband penetration is insufficient, despite the recent landing of optical fibre submarine cables[54]. A recent study of cloud in Africa, produced a 'Cloud Readiness Index' based on a different range of primary and secondary factors than that used in the BSA survey, including Internet penetration, literacy rates and value lost due to electrical outages, rather than policies[55]. Unsurprisingly, South Africa ranked top, but with Zimbabwe, Sudan, Senegal and Kenya in the top 5.

A similar 'Cloud Readiness Index' for Asia evaluated 10 key attributes across 14 countries, including international connectivity, power grid quality, business efficacy and global risk, which incorporated the presence of earthquake fault lines[56]. It found that Japan led the region, with Hong Kong, South Korea and Singapore following closely behind, although for different reasons. Hong Kong was seen a becoming a data hub for north Asia, due to its international connectivity, with many data centres locating there. By contrast, South Korea's position was being driven by an ambitious cloud strategy involving government funding of up to US$2 billion by 2014.

In April 2012, the ITU published a study on cloud computing in Africa, which contained ten recommendations of measures to be taken to facilitate cloud computing:

1. *Effective regulatory progress* – including the need to adequately address data protection and security concerns;
2. *Maintain a regulatory watch* – to ensure that states are aware of regulatory best practice;
3. *Careful preparation of cloud computing outsourcing contracts* – including robust clauses on data security and availability;
4. *Conformity with existing provisions* – cloud contracts should also reflect other minimum regulatory requirements;
5. *Establishment of data centres in Africa* – to reduce the cost of bandwidth and increase speed of access;
6. *Quality of data centres* – to ensure data centres are service orientated, agile, automated, well protected and ecologically sound;
7. *Introduction and/or upgrading of regulation* – such as data protection laws
8. *The launch of training programmes*
9. *Cross-border standardization and regulation* – the need to participate in cloud standardization initiatives[57]

The successful implementation of these recommendations will depend on action by, and co-operation between, a range of government departments and regulatory entities, including telecommunication authorities. An effective data protection regime, for example, relies on a statutory framework supported by an independent supervisory authority. While it can facilitate trade in services with developed nations, particularly in Europe, a data protection regime also imposes additional costs on domestic businesses, which can be unpopular in the short term. Creating a favourable regulatory environment without recourse to overly bureaucratic interference is a challenge for all jurisdictions and regulators.

5.2 Contractual arrangements

Private law regulation through contract offers service providers and users a self-regulatory mechanism for generating a framework of legal certainty and security in cloud computing. Cloud contractual arrangements come in varying shapes and sizes, but will generally comprise four distinct components, whether in a single agreement or a set of linked documents (generically referred to as the 'cloud contract')[58]:

- Terms of service, detailing the key features of the relationship, both cloud-specific and general boiler-plate provisions (e.g. choice of law);
- Service level agreement, detailing the service features being provided, the standards that they should meet (e.g. service uptime) and any compensation mechanism where the standards are not met;
- Acceptable use policies, detailing permitted or impermissible conduct by users (e.g. copyright infringement);
- Privacy policy, detailing the approach taken to the processing of user data, particularly consumers.

The terms of a cloud contract can be distinguished into cloud specific-provisions and standard terms; although of equal importance in terms of defining the provider-user relationship. The former provisions generally focus on two key aspects, (a) the treatment of the data submitted by the cloud user into the cloud service, including issues of data ownership, integrity, preservation, disclosure and location; and (b) the specifications of the 'service' being offered to the cloud user, such as service availability. The standard terms will include such matters as provider liabilities, dispute resolution and applicable law.

From a public policy perspective, however, self-regulation through contractual agreements can raise concerns when market practice facilitates a situation where contracts do not present a fair balance of liabilities and responsibilities between cloud providers and users, especially SMEs and consumers. In this circumstance, regulatory intervention in the freedom to contract may be necessary to rebalance the relationship. In the telecommunication sector, regulation may determine, for example, the minimum contract terms offered to a consumer[59]; obligations to meet certain standards for quality of service[60]; and compensation arrangements for a failure to meet a performance standard[61].

In the consumer market, CSPs will generally dictate the terms on which the service is offered. Such standard terms and conditions are inevitably biased in favour of the provider, even though they may vary considerably according to the markets from which the cloud provider originates; e.g. providing hardware (e.g. IBM), software (e.g. Microsoft), outsourcing, communications services (e.g. Rackspace) or retail products (e.g. Amazon)[62]. At the enterprise level, a recent study suggest that service providers are increasingly being forced to negotiate agreements in order to win the business and, therefore, are conceding on issues in favour of the user[63]. The issues, on which most negotiation took place with respect to the terms of service, were provider liability, service level agreements, data protection and security and intellectual property rights. In terms of the mechanism of agreement itself, the right of service providers to unilaterally amend service features and termination rights were also key areas of dispute. The study suggests that while enterprise cloud contracts will remain distinct from the consumer segment, some of the concessions achieved in enterprise negotiations are likely to trickle down into the provider's standard terms of business[64].

Another obvious influence on the contractual environment for cloud services is the public procurement practices of public administrations, as they are often the single largest purchaser in the emerging cloud market. As public authorities embrace cloud services, such as for the provision of eGovernment services, they, similar to enterprise users, are in a good position to negotiate more favourable terms and conditions with cloud service providers. In the US, for example, the Chief Information Officer, within the Office of Management and Budget has issued best practice guidance for the acquisition of cloud services[65]. The guidance addresses the selection of a service, the service level agreement, end-user agreements, e-discovery and record-keeping issues. Inevitably, a key concern for the public sector is that of security in the cloud.

6. Ensuring a secure cloud

A secure cloud environment can be seen as having two main dimensions. First, the user will be concerned that the data, applications and resources are available as and when they are required. Second, users will want assurance that their data cannot be accessed and obtained by an unauthorised person. Availability may concern the data centres on which the data and service resides or the communication networks over which the data and services are accessed. While the former lies within the control of the CSP and will generally be addressed in the contractual agreement with the user, such as service level guarantees, the latter may lie beyond the control of either the CSP or the user, particularly when accessing over the public internet. The less robust the public internet, the greater the vulnerability of cloud users. As such, the communications infrastructure in developing countries is therefore a key factor in the take-up of cloud computing and sectoral regulators have a key role to play.

Responsibility for security obviously depends as much on the cloud user as the service providers[66]. Encryption, for example, may be applied by the communication service provider to create a secure transmission tunnel to and from the cloud service, while the cloud provider will generally encrypt the data being stored. The user, however, is also capable of applying their own layer of encryption to prevent any of the 'stack' of service providers having access to the data in an intelligible form, if there is a lack of trust[67]. Currently, however, while users can encrypt data while stored in a cloud service, it is not technically possible to maintain such encryption while actually processing the data in an application, which represents a potential vulnerability. In addition, for service providers to be able to provide support services to the customer, they may require access to user data in the clear. The proliferation and deployment of cryptographic techniques is a regulatory matter in many countries, e.g. under export control regimes, which may impact on cloud service provision as much as other uses of ICT. However, such issues are beyond the scope of this paper[68].

6.1 Information ownership

Cloud security is not only about data confidentiality, integrity and authenticity; it is also raises concerns about information ownership. In most legal systems, while information per se is not recognized as a kind of personal property, there are a range of legal entitlements granted over information, from personal data, such as data protection laws, to intellectual property rights, such as copyright and patents. In a cloud environment, users entrust their data to a cloud service provider, often located in a foreign jurisdiction. As such, users will want reassurance that such entrustment does not alter their rights in the submitted data, thereby undermining its value, or the rights of third parties, which could expose them to liability.

While a user will be seeking reassurance; from a CSP's perspective, they will require adequate contractual rights or licensed permissions to be able process and manipulate the submitted data in the normal course of the provision of the service, including generating multiple copies for security purposes. The scope of rights or permissions demanded by the CSP may be an area for negotiation in enterprise agreements, while creating concerns for consumers subject to a CSP's standard terms[69]. In addition, the CSP will generally demand warranties and indemnities from the user that they do not place any data into the cloud service without the relevant permissions, which could expose the CSP to secondary infringement liability.

An ownership issue may also arise with respect to the meta-data generated by the use of the cloud service and the information derived from this data[70]. For the CSP, the ability to derive value from this meta-data may comprise

part of the economic rationale for the service, hence the prevalence of 'free' services within the consumer cloud market, while cloud users may be concerned that such data can reveal their commercial secrets or personal data. Under the telecommunications law of many countries, controls are imposed over the ability of service providers to use the meta-data (e.g. 'traffic data') generated by customers through the use of their communication services[71]. Such controls recognize both the potential value of such data, as well as the potential for undue interference. As cloud computing becomes more widespread, consideration may be given to the need for similar such regulatory controls over the meta-data generated through the use of cloud services.

As noted above, one aspect of the uncertainty over information ownership in the cloud arises from the fact that the data will often be transferred out of user's jurisdiction to be held on servers residing in foreign jurisdictions, about which the user may have little, if any, knowledge about the legal rules. For governments, this risk to data sovereignty is often one they are not prepared take[72]. One innovative approach to addressing this concern has been to utilize traditional national and international rules governing diplomatic immunity[73] to extend the domestic law of the cloud user to encompass the physical data centers in the foreign territory where the cloud service is located[74]. While such an approach requires a willingness on behalf of the government of the country hosting the data centres to surrender sovereignty in this manner, it is an example of how legal techniques can be used to directly facilitate economic development.

6.2 Data retention and deletion

Mention has already been made in this paper of the potential concern that a user may have about their ability to port their data into and out of a cloud service, due to formatting constraints; as well as the data access rights necessarily granted service providers in course of the provision of support services. A third access-related issue is the treatment of user data once they have terminated a cloud service. From the user's perspective, they will have two concerns:

- Will they be given adequate opportunity to retrieve their data and applications from the cloud service?
- What steps will the service provider take to delete copies of the user data?

On the first issue, research has found that some providers offer customers a certain grace period following termination during which the customer can manage the transition of the data and applications out of the service; while others assert that data will be deleted immediately[75]. On deletion, some 'free' providers reserve the right to delete data in dormant accounts; while others retain data from terminated accounts for limited periods to enable customers to change their minds. What appears absent in most agreements is detail about the actual technical measures taken by providers to delete data, which could vary from allowing it to be overwritten over time, with the associated security vulnerabilities, to warranties of compliance with public standards[76].

Data protection regimes generally impose obligations that address both the retention and deletion of personal data. Such rules can be used to improve commercial practices in the area. Consumer protection law may also be used to ensure that consumers are not unfairly deprived of an adequate opportunity to retrieve their data upon service termination.

6.3 Security standards

Ensuring that cloud computing occurs in a secure environment is obviously not just a concern for users, but is also a concern for governments trying to facilitate the take-up of cloud. Security is obviously one element of the service being provided to the user; therefore it will be addressed in the contractual agreement. However, obtaining security assurances on a generalized basis, however, will require the development of standards against which cloud service providers can be judged. There are existing security standards that cloud service providers may adopt and utilize in a cloud context, such as ISO/IEC 27001 for information security systems[77] or SAS70[78], both of which provide for external auditing and certification. Secondly, cloud-specific standardization initiatives are being pursued, such as the Cloud Security Alliance[79], which is developing mechanisms, such as the CloudTrust protocol[80] designed to promulgate best practice in the industry and transparency for cloud users. Within the ITU-T, Study Group 17 has

been working on cloud security since April 2010, developing guidelines and requirements in a number of areas, including identity management[81]. The need for audit rights and accountability practices to be embedded in the cloud environment may be driven in part by the demands of regulators to which the cloud user may be subject, whether sectoral, such as in the financial services sector, or horizontal, such as data protection authorities.

A third source of cloud security standards is the public sector. In some countries, public authorities are beginning to adopt cloud computing solutions offered by the private sector, but only where those services have been externally accredited as offering sufficient levels of assurance[82]. Given the scale of public procurement on the market for IT products and services, such government-led security standards can be expected to have a significant influence on market developments. However, they may also generate an obstacle to the market for cloud computing if they are over-specified, undermining the cost benefits of cloud computing by imposing requirements for unnecessarily stringent standards; as recently noted:

> "Recognize that technology and process standardization that are an inherent part of the public IT cloud experience are among the fastest ways to reduce complexity and drive improved IT and business efficiencies; conversely, understand that opting for anything customized beyond the standard technology or process offered by a cloud service provider will quickly change IT deal economics back closer to what they have been in the past, before cloud."[83]

In addition, advisory bodies have published guidelines on security and privacy, designed to promulgate good practice without mandating compliance[84]. In Europe, ENISA, for example, identifies eight security-relevant parameters that should be addressed, measured and subject to specific procedures when negotiating with a cloud service provider, including service availability, incident response, data life-cycle management and log management[85].

6.4 Law enforcement access

When placing data in the cloud, users inevitably have concerns about unauthorised access to such data; exposing state or commercial secrets and breaching individual privacy. While such threats are viewed as primarily emanating from organized crime, access by law enforcement agencies in the course of an investigation (or indeed litigants in the course of a civil claim) has itself become a heightened privacy and security concern, particularly in relation to the threat of action by US authorities under the 'Patriot Act'[86] in a global market where US-based cloud providers dominate[87].

Cloud users, particularly from the commercial and public sector, will have three key concerns about law enforcement access to data held in the cloud. First, the data itself may represent significant commercial value, which needs to be protected from unauthorised disclosure. Second, the data will often be held outside the user's jurisdiction, subject to legal rules and procedures with which the user is unfamiliar, creating uncertainty about the governing framework. Third, the placing of data in the cloud may itself represent a breach of legal obligations owed by the user towards a third party, such as the data protection rights of customers[88].

As noted earlier, location independence and the use of shared resources is a feature of cloud-based services. For sensitive data, therefore, cloud computing may not offer a solution or at least the public cloud. Even where service providers offer users the ability to determine the location of their data, such as Amazon, which offers users the choice of placing their data in a Europe or US cloud, the reality of 'follow-the-sun' support for such services will generally mean that the data remains accessible by persons outside of the stated location. In April 2011, for example, Dropbox was forced to change the wording used in a 'help' article to reflect an amendment made to its terms of service. It had stated that "Dropbox employees aren't able to access user files"; part of the security assurances made to its customers relating to its use of encryption. However, its terms incorporate a provision enabling it to hand over user data in compliance with a valid court order, which required it to clarify that its employees are 'prohibited' from accessing user files, rather than being unable to access them[89].

While good security is key to the development of cloud computing, it also represents a new challenge for law enforcement agencies (LEAs) in terms of investigation criminality. On the one hand, accessing and obtaining forensic

material in a cloud environment raises issues about the legality and enforceability of LEA actions in as transnational environment. On the other hand, the tools that LEAs have traditionally used to obtain data may need to be updated to reflect the cloud environment. In Europe, for example, the European Telecommunications Standardization Institute (ETSI) is currently developing a draft standard for lawful interception of cloud services, building on previous standards developed for telecommunication providers[90].

The ability of LEAs to access cloud data will generally depend both on the legal framework in the requesting and requested jurisdiction, as well as the contractual terms under which the cloud service provider offers its service. Traditionally, the obtaining of evidence from a foreign country is carried out under treaty-based mutual legal assistance ('MLA') procedures, which ensure full judicial oversight. However, such procedures are notoriously slow and cumbersome, not suited to digital investigations. As a consequence, more flexible procedures were adopted in the Council of Europe Convention on Cybercrime[91] in 2001, which are applicable in a cloud environment. The Convention is an instrument of public international law and embraces over forty member state signatories, including non-European countries such as the United States.

As well as providing for MLA procedures, the Convention also permits a domestic LEA to obtain data from a foreign source without the need to go through MLA in certain circumstances. Under Article 32, a domestic LEA can obtain foreign data where the data is "publicly available (open source) stored computer data" or where the domestic LEA "obtains the lawful and voluntary consent of the person who has a lawful authority to disclose the data..". The latter is most relevant to a cloud environment and is concerned with the persons who have authority over the data. The cloud user could obviously grant authority, but is unlikely in the course of a criminal investigation. However, the cloud service provider will also generally reserve the right, in the user service contract, to disclose user data in certain circumstances. Such circumstances can range from a high threshold, such as the receipt of a valid court order, to a low threshold based on the service provider's discretion or perception of its best interests.[92] Whether a cloud service provider will disclose customer data will obviously depend on a range of factors, including the country making the request, the nature of the offence being investigated, and the type of the data being requested. However, as noted above, the current market dominance of US cloud providers has focused attention on the ability of US LEAs to access cloud-based data. From a user's perspective, preventing such disclosure in all circumstances is only possible where the user implements its own security measures, such as encryption, thereby rendering any disclosed data unintelligible. Otherwise, contractual procedures can be agreed with the service provider ensuring that, where permissible, the user is given prior notification of any request for disclosure, to enable them to pursue legal recourse preventing such action[93].

7. Proposed Recommendations

This discussion paper has examined the emerging trend of cloud computing and its regulatory treatment and implications. As with other areas of ICT development, regulation can facilitate the adoption of cloud computing by establishing an environment in which both providers and users have certainty and trust. Based on the preceding analysis, the following recommendations are addressed to regulators as representing some common practices, which may become 'best practices' for the regulation of cloud computing:

- **Broadband infrastructure and open access:** Cloud computing is dependent on an ample and robust communications infrastructure to which service providers have access on a non-discriminatory basis. Regulators need to consider taking measures to ensure that communication providers do not engage in conduct designed to, or having the effect of, constraining the provision of cloud services for reasons that are not transparent, objective, non-discriminatory and proportionate.

- **Cloud standards:** The development and widespread adoption of appropriate national, regional and international technical and organizational standards are required to address a range of concerns among cloud providers and users, including the integration of legacy systems with cloud interfaces; data and application portability and security.

- **Security:** The adequacy of the organizational and technical security measures implemented by cloud service providers has an impact beyond the interests of cloud users themselves. Two recommendations are made:

    - **Breach notification** – Providers should be obliged to notify relevant national regulators (whether sectoral or horizontal) and, in certain circumstances, cloud users when significant breaches of security occur that may impact, directly or indirectly, on the security of cloud user data.

    - **Standards, Certification and Audit** - Compliance with security standards requires external review and oversight not generally feasible on a per user basis. National, regional and international audit criteria and certification systems should be encouraged and endorsed.

- **Cloud transparency:** Cloud service providers should be obliged to notify users of the chain of providers that underpin the provision of the service to the cloud user.

- **Cloud contracts and service level agreements:** In a rapidly developing and diversifying marketplace, the terms under which cloud services are provided should generally be left to the parties involved. In the consumer space, however, consideration could be given to the drafting of model provisions addressing key issues of concern to users, such as quality of service, data portability and information ownership.

- **Consultative decision-making process:** National regulators need to consult with cloud service providers and other market stakeholders about the appropriate regulatory treatment and characterization of certain cloud services, with a view to issuing guidance providing legal certainty for market entrants and cloud users.

- **Regulatory co-operation:** Cloud services impact on a range of regulatory areas, both within jurisdictions and across multiple jurisdictions. Regulators should establish formal and information procedures to co-operate and co-ordinate regulatory decision-making that is targeted at cloud service providers, as well as be cognizant of the potential collateral impact that non-targeted regulations may have on the cloud market.

[1] E.g. NIST, 'The NIST Definition of Cloud Computing', No. 800-145, September 2011.

[2] ITU-T FG Cloud Technical Report Part 1, *Introduction to the cloud ecosystem* (02/2012).

[3] See further Bradshaw, S., C. Millard and I. Walden, "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services" *International Journal of Law and Information Technology*, vol. 19, no. 3, 2011: pp. 187-223

[4] In telecommunications, the shift from circuit-switched to packet-switched network architectures represented a similar step-change in the efficient use of transmission resources.

[5] Francis Cairncross, *The Death of Distance*, Texere Publishing, 1997.

[6] Sun Microsystems White Paper, 'Introduction to Cloud Computing Architecture', June 2009, at 9. See also NIST, *Cloud Computing Synopsis and Recommendations*, No. 800-146, May 2012.

[7] See generally ITU-T FG Cloud Technical Report Part 7, *Cloud computing benefits from telecommunications and ICT perspectives* (02/2012).

[8] 'The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010', http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[9] Vivian Reding, European Commissioner, July 2009.

[10] GSR 2012 Discussion Paper, *The Cloud: Data Protection and Privacy – Whose cloud is it anyway?*.

[11] E.g. HP refer to the cloud offering 'Everything as a Service', see http://www.hp.com/hpinfo/initiatives/eaas/index.html

[12] The ITU-T FG Cloud Technical Report Part 1 (02/2012) distinguishes three types of actor in the cloud ecosystem: the cloud service user, the cloud service provider and the cloud service partner (at 2.1.3).

[13] For the purpose of this paper, 'infrastructure' refers to any component of the cloud service, not an IaaS.

[14] GSR 2012 Discussion Paper, *The Cloud: Data Protection and Privacy – Whose cloud is it anyway?* See also ITU-T Technology Watch, *Privacy in Cloud Computing*, March 2012.

[15] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (OJ L 108/33, 24.4.2002).

[16] Ibid., at arts. 2(a) and (c) respectively.

[17] Public Branch eXchange. E.g. Interactive Intelligence, White Paper: 'A new approach to Communications as a Service (CaaS).

[18] See, for example, Walden, I., "The regulatory implications of Internet telephony", pp.226-231, *Computer and Telecommunications Law Review*, vol. 2, no. 6, 1996.

[19] ITU WTPF 2001, *Report of the Secretary-General on IP Telephony*, 31 January 2001.

[20] E.g. European Regulators Group, 'Common position on VoIP', ERG (07) 56rev2, December 2007. Available at http://erg.eu.int/doc/publications/erg_07_56rev2_cp_voip_final.pdf

[21] See generally the *Telecommunications Regulation Handbook* (10th ed.), IBRD, World Bank, *info*Dev and ITU, 2011.

[22] See, for example, Carr, *The Big Switch: Rewiring the World, from Edison to Google* (Norton: New York 2008).

[23] E.g. ITU-D, Regulatory and Market Environment, *Cloud Computing in Africa: Situation and Perspectives*, April 2012; European Parliament study, *Cloud Computing,* European Commission, DG for Internal Policies, IP/A/IMCO/ST/2011-18, May 2012.

[24] ASA Adjudication on UK2 Group, 29 February 2012. Available from www.asa.org.uk

[25] ASA Adjudication on WEBHOSTUK Ltd., 11 July 2012.

[26] See Facebook 'Statement of Rights and Responsibilities' (version dated June 8, 2012), at 16.1.

[27] Cour d'Appel de Pau, 1ère Chambre, Dossier 11/03921, *Sébastian R v Société Facebook Inc*, 23 March 2012.

[28] I.e. Directive 2002/22/EC (OJ L 108/7, 24.4.2002), art. 30.

[29] Facebook is an example of a cloud computing provider that does not allow its users are to move their data to competing providers. On the other hand, Google's Data Liberation Front is an initiative which intends to facilitate data portability to and from Google's products, http://www.dataliberation.org/.

[30] Commission proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11/4 draft, 25 January 2012.

[31] Ibid., at article 18.

[32] Ibid., at article 18(3).

[33] See generally Bornico, L., and Walden, I. "Ensuring competition in the Clouds: The role of Competition law?", *ERA Forum* (2011) 12, pp. 265-285 (8,453 words).

[34] Brockmeier, J., "Amazon APIs: Cloud Standard or Zombie Apocalypse?", 12 April 2012, available at http://www.readwriteweb.com/cloud/2012/04/amazon-apis-industry-standard.php

[35] See "EUROPA - Press Releases - Antitrust: Statement on Apple's iPhone policy changes," September 25, 2010.

[36] "EUROPA - Press Releases - Antitrust: Commission initiates formal investigations against IBM in two cases of suspected abuse of dominant market position," 26 July 2010.

[37] See Ibid.

[38] Ibid.

[39] See *Google Inc. and Onix Networking Corporation v. The United States and Softchoice Corporation* (United States Court of Federal Claims 2011).

[40] See Ibid.

[41] Ibid., para 25.

[42] See generally Walden, I. (ed.), *Telecommunications Law and Regulation*, 4th ed., OUP, 2012.

[43] See GSR 2011 Discussion Paper, *Open Access Regulation in the Digital Economy*, 2011.

[44] E.g. Body of European Regulators for Electronic Communications, 'Report on best practices to facilitate consumer switching', BoR (10) 34 Rev1, October 2010.

[45] MusicTank, 'The Dark Side of the Tune: The Hidden Energy Cost of Digital Music Consumption', 2012, available at http://www.musictank.co.uk/resources/reports/energy-report

[46] Available at http://ec.europa.eu/information_society/activities/sustainable_growth/docs/datacenter_code-conduct.pdf

[47] See http://www.google.com/patents/US7525207

[48] E.g. In Germany.

[49] As provided under European Union law.

[50] See, for example, http://gcloud.civilservice.gov.uk/

[51] E.g. Australia Government, *Cloud Computing Strategic Direction Paper*, April 2011.

[52] N Kroes, (2011) "The Role of Public Authorities in Cloud Computing", Aspen Institute IDEA Project Plenary, *Brussels, 24 March,* <www.aspeninstitute.org.> accessed 27 April 2012.

[53] BSA/Galexia, 'Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity', 2012, available at http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf

[54] E.g. SAT-3 in Southern Africa, EASSy in East Africa and WACS in West Africa.

[55] Laverty, A., 'The Cloud and Africa – Indicators for Growth of Cloud Computing', available at http://theafricanfile.com/ict/the-cloud-and-africa-indicators-for-growth-of-cloud-computing/

[56] Asia Cloud Computing Association, *Asia's first 'Cloud Readiness Index'*, 7 September 2011, available at http://www.asiacloud.org/index.php/products/cloud-readiness-index/162

[57] ITU-D, Regulatory and Market Environment, *Cloud Computing in Africa: Situation and Perspectives*, April 2012

[58] Bradshaw, at 6.

[59] E.g. EU, Directive 02/22/EC on universal service and users' rights, art. 20.

[60] E.g. Nigerian Communications Act 2003, s. 104.

[61] E.g. Australia, Telecommunications (Consumer Protection and Service Standards) Act 1999, Part 5.

[62] Bradshaw.

[63] See Hon, W., C. Millard and I. Walden, "Negotiating Cloud Contracts – Looking at Clouds from both sides now", forthcoming in the *Stanford Technology Law Review*, currently available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199

[64] Ibid., at p.42.

[65] CIO, 'Creating effective cloud computing contracts for the federal government', 24 February, 2012; available at https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

[66] See generally ITU-T FG Cloud Technical Report Part 5, *Cloud security* (02/2012).

[67] Kamara, S., and K. Lauter, "Cryptographic Cloud Storage", in Sion, R. and others (eds), *FC'10 Proceedings of the 14th International Conference on Financial Cryptography and Data Security* (Springer-Verlag Berlin, Heidelberg 2010), 136.

[68] See ITU-D report *Understanding Cybercrime: A Guide for Developing Countries*, March 2012, at section 6.3.11.

[69] However, public campaigning may sometimes result in changes to company terms. For example, as a result of previous controversies, Facebook recently put its proposed revisions to its 'Data Use Policy' and 'Statement of Rights and Responsibilities' to a vote of its users. See http://www.insidefacebook.com/2012/06/01/facebook-puts-proposed-policy-changes-up-to-a-vote-following-activist-campaign/

[70] See generally Reed, C., 'Information "Ownership" in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No 45/2010: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461

[71] E.g. Rwanda, Law N° 44/2001 of 30 November 2001 governing telecommunications, art. 24.

[72] See Irion, K., "Government cloud computing and the policies of data sovereignty (September 30, 2011). Available at SSRN: http://ssrn.com/abstract=1935859 .

[73] E.g. Vienna Convention on Diplomatic Relations (1961), *UN Treaty Series*, vol. 500, p.95.

[74] See http://www.wisekey.com/en/solutions/DataSovereignty/Pages/default.aspx

[75] Bradshaw, at 203.

[76] Ibid. E.g. BS EN 15713:2009 'Secure destruction of confidential material'.

[77] http://www.iso.org/iso/catalogue_detail?csnumber=42103

[78] American Institute of Certified Public Accountants, *Statement on Auditing Standards (SAS) No 70, Service Organizations*. It was replaced in June 2011 by *Statement on Standards for Attestation*

Engagements (SSAE) No 16.

[79] https://cloudsecurityalliance.org/

[80] https://cloudsecurityalliance.org/research/ctp/

[81] See http://www.itu.int/ITU-T/studygroups/com17/index.asp

[82] E.g. the UK HM Government has issued 'G-Cloud Information Assurance Requirements and Guidance', 10 May 2012.

[83] IDC, 'IT Cloud Decision Economics: 10 Best Practices for Public IT Cloud Service Selection and Management', July 2011.

[84] E.g. NIST, 'Guidelines on Security and Privacy in Public Cloud Computing', December 2011.

[85] ENISA, 'Procure Secure: A guide to monitoring of security service levels in cloud contracts', 2012.

[86] The full title is: 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001', Pub.L. 107-56.

[87] See the 'Top 100 Cloud Service Providers, 2012 Edition, available at http://www.talkincloud.com/tc100/.

[88] E.g. International Chamber of Commerce, Policy Statement 'Cross-border law enforcement access to company data – current issues under data protection and privacy law', Document No. 373/507 (7 February 2012).

[89] Sherman, M., "At Dropbox, even we can't see your dat- er, nevermind" (19 April 2011), available at http://www.bnet.com/blog/technology-business/-8220at-dropbox-even-we-cant-see-your-dat-8211-er-nevermind-8221-update/10077

[90] ETSI Draft Technical Report 101 567, April 2012.

[91] CETS No. 185, entered in force 1 July 2004 ('the Convention').

[92] E.g. Apple's the privacy policy for its iCloud service, states that it will disclose personal information if necessary "by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence", as well as where Apple "determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate." (www.apple.com/privacy).

[93] See further the discussion paper on the privacy aspects of cloud computing.