Regulatory landscape around cloud computing

Introduction

A precise description of cloud computing key characteristics has been still under development. From the perspective of an end user looking at the cloud, it shifts functions that used to be performed by computers located at the network's edge (such as hosting software and data) into data centers residing in the network's core. From the perspective of service providers, the focus is on the ability to coordinate and integrate applications of individual cloud computing elements to interact with other cloud computing elements. The main challenge facing cloud computing to grow is securing the quality of experience including both service and access, and the primary advantages are the result from Capex saving and the benefits of aggregating demand. This document offers cloud deployment strategies, observations on the impact of cloud computing on the networks structure, as well as its implications for regulation.

Deployment Strategies

There are at least three different deployment models of cloud computing. In the case of private clouds, all of cloud computing services are deployed through a privately owned data center used exclusively by the organization that builds it for its customer base. These private clouds may deploy proprietary technologies inaccessible to others.

In contrast, public clouds are provided by third parties offering their services to a wide range of interested customers. Public clouds typically offer a wider range of quality of service and pricing than traditional public websites and data centers.

Hybrid clouds, which focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

The scalability of cloud computing also makes it well suited to provide overflow capacity to provide insurance against unanticipated demand.

Networks Implications

As an initial matter, cloud computing will place considerably more onerous demands on the access networks through which end users will gain access to the cloud. The access networks' ability to meet these demands will go a long way in determining cloud computing's attractiveness as an option.

Also the advent of cloud computing will change the nature of demand placed on data centers and cloud computing is increasing demands on the links that connect data centers to one another.

Given the current common regulatory regimes, rationally a standalone cloud computing provider has a multiple data centers as in the case of over the top service providers (ex. iGoogle and icloud) which are outsourcing the their own data center interconnections services because they don't prefer to commit themselves to telecom regulatory regimes and continue enjoying the deregulated Internet world.

Many telecom operators try to differentiate themselves around the world as total telecom providers and launch their own private cloud to serve their customers and ask the NRAs to lighter regulations in order to compete with the deregulated over the top service providers.

Obviously, convergence between the IT industry and telecom industry will be driven by cloud computing and the network ownership is expected to transfer partially (the core element) to over the top service providers (soft networks), and the competition in the customer ownership between both industry players is expected to keep on until discovering a clear business model to share revenues between over the top service providers and a broadband connection provider.

Regulations

The development of the cloud computing industry is also being constrained by the fact that cloud computing providers face considerable regulatory uncertainty.

In the meantime, the regulatory authorities should take steps to ensure that all industry participants have the tools and the opportunity to explore cloud computing's full potential considering the following subjects.

QoS:

Cloud computing assumes that providers will provide guaranteed levels of quality of service and offer different levels of reliability and that people will pay for these services.

In order to deliver these services, network providers will have to establish redundant connections and use sophisticated network management techniques to guarantee that the network can satisfy the demands of cloud computing users.

Market Regulations:

To the extent that customers' needs vary, some customers are expected to pay a premium for higher levels of reliability and network service. Such pricing differentials for prioritized service implicate the debate over network neutrality that has dominated telecommunications policy for the past years. Advocates of net neutrality and associated rules have raised concerns about no restrictions by internet service providers or governments on consumers' access to networks that participate in the Internet.

Commonly, regulation is best suited when the product being regulated is relatively standardized, which is the case of primary network elements that have already been deployed, and technologies and market shares that are stable. In an environment like cloud computing, in which the product varies widely, investment incentives play a critical role, and in which the underlying technology and market positions are in a state of dynamic change, the ex-anti regulation is not appropriate.

Data portability:

The fact that the cloud computing application programming interfaces (APIs) are largely proprietary limits customers' ability to switch to a different provider should they become dissatisfied with their current provider. Standardizing APIs would facilitate data portability and would allow greater reliability by allowing the same functions to be performed by multiple cloud computing providers.

Security and Privacy:

Perhaps the greatest challenge facing cloud computing is with respect to security and privacy. In addition to the business concerns raised by these issues, privacy and security related mandates vary widely across authorities and laws. End users are likely to insist on being able to verify where their data has been hosted after the fact and may well insist on a degree of ex-ante control over where their data is hosted.