



## **Paper: Regulatory Framework for Cloud Computing**

**Sachin Dev Duggal**

Chairman Computing Chamber – Associate Chamber of Commerce  
President and CEO, nivio.com

**Edition – Final**

**For the Telecoms Regulatory Authority of India – 5<sup>th</sup> July 2011**

---

**the power of the “few” in the cloud**

---



always turned on!™

[blog.nivio.com](http://blog.nivio.com)  
[www.nivio.com](http://www.nivio.com)

**nivio Technologies India PVT. LTD**  
562 Udyog Vihar, Phase V, Gurgaon - 122016, Haryana, India



## Interlude

The “**power of few**” is quite simply the main reason why governments around the world need to look at this phenomena, new industry and paradigm shift known as the “cloud” with a new set of eyes and a new set of values. It is here, it is changing and it will continue to re-shape economies from yesterday to tomorrow.

The power of the few outlines the change – movement from millions of individual units (computers) that are not necessarily linked nor controlled to the cloud where all of them are grouped and huddled... and controlled by a handful of companies. When a nation’s economic agility is thus controlled by a “few” they have power that needs regulation but one that does not cripple innovation or stifle growth.



## What is the Cloud exactly?

Before contemplating the challenges or the need for regulation it makes sense to define what exactly we mean by the “cloud” as some of it has existed in different manifestations (and acronyms) for the last decade or two; ever since the Larry Ellison’s notion of the Networked Computer.

“Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.” [University of California Berkeley].

In a somewhat crude simplification the notion of Cloud Computing simply makes what we today have as a “generator” either under our desks or in our private datacenters and changes everything from the hardware, platform and software (and even the desktop) into a service that is “consumed” and not “owned”.

The representation of the cloud can translate into many types of implementations – for the purposes of completeness these are briefly highlighted below but the real significance of this paper is based on the Public Cloud.

**Public cloud** – sold to the public, mega-scale infrastructure (e.g. Amazon, Google, Salesforce, Azure, etc.)

**Hybrid cloud** – composition of two or more clouds where you can abstract applications or services through a combination of in-house infrastructure or reach out to multiple Clouds

**Community cloud** – a shared infrastructure for specific community (e.g. health care)

Hereafter – the key discussion will be around the Public Cloud with additional references to others if appropriate.

## What is the hierarchy of the cloud? Everything as a Service {EaaS}

The levels of the cloud (we often believe it is all just one thing but in truth it is wider than the definition of “computing”) are critical to understanding the true complexities in being able to “police” / “regularize” and “mediate” in the cloud – which is the true essence of this paper.

### Infrastructure as a Service: {IaaS}–

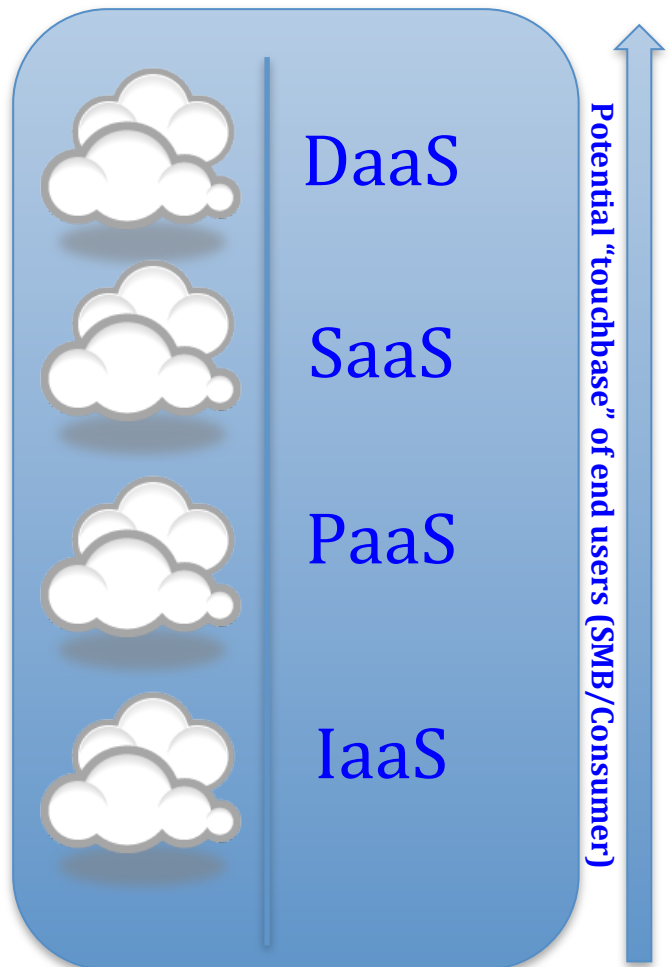
At the bottom of the pyramid of the cloud is the notion that you do not need to spend money buying hardware but instead rent it on a unit (per hour, per GB, per mbps). Amazon, Rackspace are examples of this. *Typical Buyer is the CIO/Techie/Engineering team – the people that know about tech.*

**Platform as a Service: {PaaS}** – is the “solution stack” as a service, PaaS sits on top of an IaaS layer and is about providing a development and launch platform that provides facilities that support the complete life cycle of building and delivering web applications and services entirely available from the internet over the web.

Facebook, Salesforce and Amazon (S3) are examples of this. *Typical Buyer is the CIO/Techie/Engineering team – the people that know about tech.*

**Software as a Service: {SaaS}** – this is the third level of the stack is more for the end consumption by businesses and consumers – it is the applications themselves usually “Line of Business” or “Consumer Web Applications” that are in this space. Examples of this include Salesforce (which also exists in the PaaS space), xero.com, Hotmail, office365 etc. *The Typical buyer is the SMB or consumer – not many large corporates use the “cloud” SaaS model.*

**Desktop as a Service: {DaaS}** – right at the top of the “touchbase” barometer lies Desktop as a Service where the notion of having a PC is eradicated and as such you simply consumer it through a device (could be a PC/Mac or even a tablet/Phone/TV). Examples of this service include nivio.com, hosted citrix etc. *Typical buyers are small to medium business and consumers.*





## **The need for mediation, mentoring and frameworks (open standards)**

**Cloud computing offers the potential for efficiency, cost savings and innovation gains to businesses, governments and individual users alike. To realize these benefits, a more robust regulatory framework could give users the confidence needed to embrace cloud computing. Regulatory potential covering the relationship, between consumers of cloud services and the providers or between providers themselves, could include service level agreements, interoperability and transparent business practices.**

Managing the cloud ecosystem is a challenge for any government – there is a fine balance between killing innovation and losing implicit control (one could argue that explicit control has gone by virtue of the open internet).

It is worth mentioning that no government in the world has today really adopted a policy to the cloud – many are still grappling with its wide intent.

### **Promote Service transparency – “unmasking the masked”**

The most important part of the cloud is the low bootstrapping cost for small companies to provide products- at the same time the ability for end users (SMB or consumer) to know what is going to stick around is a little like walking into a casino and betting on a roulette number – you really don’t know who is going to be around in six months or one year.

What is even more important is that the web world often masks the size of the provider and as such a three-man shop and a one hundred-man shop could be competing for the same customer albeit with far less clarity on who is “actually” bigger. The key here, as with most of this paper, is the fine balance between stopping young companies from growing but also for looking at the safeguards for the end customer.

Thus, the lack of clarity around the “potential longevity” of the provider, the quality of service and easy access to “comparable” data makes it very hard for customers to assess the solutions. In addition, improved transparency addresses some of the other attributes we are going to discuss in this paper - about the cloud in terms of confidentiality, ultimate ownership and liability (plus reliability). The transparency paradigm also addresses the ability of aggregated supply (something which the “openness” of the cloud propagates – imagine an ERP solution that is actually 4-5 vendors).



### **Specific Considerations for this section:**

- Service operators in each area should be promoted to outline key facts including service reliability data to a neutral Government Platform in order to get “Certified by the Government of India”.
- Clear need for security procedures that are required as part of this “Certification” stamp.
- Voluntary certification via approved third party rating agencies, and effective third party auditing will help mature the market and reduce the need for centralized regulation.
- A number of existing frameworks and initiatives are already being explored (such as such as the Accountability Model, Privacy-by-design, and Binding Corporate rules. These could help clarify accountability concepts- but require more industry involvement and government understanding.

### **Whose data is that really? Who can see it? Where is it stored?**

The question of Data is the most talked, debated and yet probably the least understood phenomena in the world of the cloud.

The data debate has a many fold dimensions that need to be included – the details below are by no means exhaustive but at a principal level that could expand the research further.

#### **Who really owns the data?**

As the title of this subsection elucidates –there is a real problem that is clearly visible when you look at the “cloud pyramid”; who really owns a user’s data.

Take this example: a young start-up company builds on top of a PaaS provider that is using a 3<sup>rd</sup> Party IaaS (we are trying to make this overly complicated).

- What happens when the PaaS player stops paying their IaaS Bill?
- What happens when the young-ISV is switched off due to bankruptcy?
- What happens if the ISV accidentally deletes your data?

As you move from the disk (IaaS) to the Blocks of Data (PaaS) to their contextual meaning (SaaS / ISV) (contextual meaning refers to the actual understandable format of the data) the data means something completely different – in some cases the underlying storage methods mean the data is really not logically collated together (see systems such as Hadoop that allow data to be stored in multiple locations on the principle of chunks).

There is no simple way to manage this conundrum – some of the ideas that currently float in this vacuum are:

- Tie the IaaS/PaaS/SaaS providers into a tri-partite contract with the customer such that there is insurance that the “SaaS” player or the “Contextual representor”



continues to exist for 30 days in “escrow”. This additional “tax” is the “insurance” that participants in the ecosystem have to pay.

- Make the customer contract with the IaaS provider and then permission PaaS / IaaS providers to access their data.

## Who can see my data?

The privacy battle continues with more and more going to the cloud; the questions of privacy are many-fold but specifically center of third parties to see the “contextual representation” (after-all no-one is so fussed if the people can only see ones and zeros) and also center on the ability of law-enforcement agencies to “be-able-to-see” a user’s data – this we will deal with under a separate subsection.

When data is stored in the cloud, the end users always forget about where it is, what jurisdiction and privacy policy exists to manage it. Therefore, the issue of data privacy is very much to the forefront of everybody’s mind, with many television commercials advertising products and news programs describing another data breach. Any organization has a legal obligation to ensure that the privacy of their employees and clients is protected. Laws prohibit some of this data to be used for secondary purposes other than for what it was collected. An organization cannot surreptitiously collect data on say, the health of employees, and then use this to charge smokers with higher insurance premiums. In addition, it cannot share this data with third parties. In the world of cloud computing, this becomes much harder as you now have a third party operating and managing their infrastructure, and hence by inference will have access to the organization’s data.

Often, privacy notices specify that individuals can have access to their data and to have this data deleted or modified. If this data is in a cloud provider’s environment, privacy requirements still apply and the enterprise must ensure that this is allowed within a similar timeframe as if the data were held within a traditional IT implementation. This sometimes becomes impossible especially in Public Cloud Deployments as they have a unified approach to dealing with customers and often are unable to segregate the data (most cloud applications are “multi-tenancy”).

There are a number of cloud provider companies that specialize in distinct markets and tailor their services to those markets. This is likely to become more prevalent in the upcoming years and there will also likely be niche cloud providers. For instance, cloud providers that offer services in the health care market- place would be bound by the relevant regulations for that market (HIPAA in this case)—and we would expect them to charge for the special handling and controls that are needed.



## Where is it stored?

The location of the data adds a perplexing dimension to the entire storage and data conundrum – not only are companies that are “Indian” now required to follow Laws of India but also of foreign companies – the situation gets far more complex when you have to consider the potential that most cloud providers are currently out of India – so you could have a situation that means an Indian ISV with data in foreign lands is providing services to Indian customers.

Expanding the above; the Internet has become an essential tool for businesses of all sizes. Any business with a Web presence or individuals who post on social networking sites are recording data on one or more servers that could actually be located anywhere. Whether users are posting personal information to Facebook, or updating their business links on LinkedIn, this data will be stored somewhere. As businesses move towards the using and embracing of cloud providers, the location of the data will become more and more important due to data privacy, legal, or regulatory demands.

Global companies need to ensure that any services it deploys to the cloud are used according to laws and regulations that are in place for the employees, foreign subsidiaries, or third parties who need to use it. Laws in one country will be markedly different from that in certain other countries, so even if it is a company’s own employees who are using the service, the company needs to be aware of the laws that pertain to them in their location.

As an example, the data protection laws of the EU member states, as well as other countries, are extremely complex and have a number of definitive requirements. The transfer of personal data outside these countries needs to be handled in very specific ways. For instance, the EU requires that the collector of the data, or data controller, must inform individuals that the data will be sent and processed in a country outside of the EU. The data controller and end processor must also have contracts approved by the Data Protection Authority before this can be undertaken. This will have different levels of difficulty depending on the country that is processing the data. The United States and the EU have a reciprocal agreement and the U.S. recipient only has to self-certify its data procedures by registering with U.S. Department of Commerce.

In putting data onto a third party server, whether a cloud provider or otherwise, data is being entrusted to them and the country where they are located. This means domestic data being “accessible” to foreign countries. These laws may be more onerous if the server is hosted in certain countries, such as China, where the local laws may allow the local government to have unlimited access to the data regardless of its sensitivity. There may be laws that limit (or prohibit) from encrypting the data without ensuring the local authorities can decrypt it when they require.

The cloud provider market is expanding, but there are still only a limited number of players who can offer large scale hosting of applications and data. This may lead companies that subcontract some or all of the hosting to another company, possibly in another country. Some cloud providers will inevitably go bankrupt or cease operating as a cloud provider and



the access to data could become an issue especially if overseas. Depending on where the server resides, this may cause customers to go through another country's jurisdiction to get the data back and it may be subject to completely different access rules to what they are used to.

The where it is stored discussion also opens up the "how can I move it" to another provider discussion which in itself is a whole gambit of issues as every operator runs different formats and some are even proprietary / encrypted. It is essential that users have the ability to move data at their will to other providers or to an "escrow" whilst preserving the contextual relevance of the data. There have been no real discussions on this at a global level as part of the problem is that policy decisions are only now taking place.

## **What about Lawful Intercept?**

Whilst this is an extremely important point – it is probably the shortest one to consider – established and transparent methods for letting Governments protect their boundaries and national security are of key importance. With more and more happening in the cloud – the previous methods of Lawful intercept are no longer valid and as such need new thinking.

### **They are not valid because:**

- Machines and data are no longer physically in a place
- Encryption and security of data are far stronger and of industrial grade
- End companies have to sign deeper and more stringent End User Agreements with customers that previously never covered data (data was local and software manipulated it locally).

At nivio we take this very seriously and have set mechanisms in place to let governments access data that belong to their citizens provided they give proof and due cause. This does not make us an arbitrator but specifically required a process of a court order and not just mindless eavesdropping!

Additional elements of lawful intercept include being able to handle civil matters such as divorce, inheritance.

Careful and mindful operational flows need to be investigated to ensure that basic protections for citizens can be employed. There is a clear need and general acceptance to protect against terrorism and uphold basic civil rights – at the same time there are concerns that by centralizing of data there could be "big brother" policing and this is what needs to be kept at bay.

The additional dimension in this, the Lawful Intercept potential within the cloud, is dealing with foreign jurisdictions and creating equivalent of a Double taxation treaty.



## What about access?

The cloud is somewhat of a moot point if nothing is done about regulating access – whether it is frameworks for the internet exchanges or “operator interoperability” to ensure that networks handover to each other or the basic of simple high-speed connectivity (greater than 2mbps) at an affordable price. It is clear that to become a “cloud-onomy” the need for access and its generic and reliable availability are key. Another dimension is the creation of better and more well-connected datacenters around the country – as India is accelerating in the internet world (today we are fast becoming the largest consumer of the internet) the need for world-class datacenters and regulations that ensure companies follow due measures is an absolute necessity.

**Getting online:** the government needs to ensure measures that proliferate wide availability of the internet are employed on an “urgent” basis – use of the Universal Service Offering Fund (which now is running into the low teens of billions of dollars) would be a great tool achieving this – offering discount to fees charged by operators as well as doing the relevant plumbing in the underlying system.

**Improving Connectivity:** the key here is ensuring that routing, Internet exchanges are all managed and operated properly such that users are not facing issues where traffic from New Delhi is routed via Mumbai back to New Delhi (in the event the datacenter is located there). Clear routing policies and transparent monitoring needs to be enabled.

## Cyber Law and ensuring the police online is easy and straightforward

The cloud brings into the fold a new set of policing issues that simply existed at a much smaller scale – take for example the hacking incidents that have happened in the past months – previously they attacked only large corporates but as these corporates are now “the few” the ability for a hacker to affect a nations economic agility is far greater and thus the policing needs to take this into account.

This subsection links into many of the topics discussed as it’s the overall management and “law and order” of the online world. The key items to consider when looking at policing and providing security online are including but not limited to the following:

- Ease of filing a report (or an FIR) – can a “net-citizen” easily complain about the issues they are facing (reports of hacking etc)
- Clear and easy ways to “confiscate” data (or assume ownership) when used for illicit purposes – this could be to a “central data warehouse” with contextual access to the application.
- The ability to identify perpetrators of **online attacks** is one of the most fundamental challenges facing the international law enforcement community today. It is a challenge that will only increase as more data moves to the cloud.



## Licensing and its portability

Current software licensing models require a re-think when looking at the Cloud environment. Traditional end-user agreements or enterprise agreements will need to consider license mobility where a customer that has already purchased licenses, can transfer these over to a cloud service provider so those licenses can be hosted on behalf of the end customer, off premise. This is essentially a move to a 'rent, don't buy' model with all the concomitant issue that the music industry has started to face over the last 5 years.

There needs to be clear homework and then a framework for how licensing can be ported from "desktop" to "cloud" so that customers are not double charged, the notion of a per device license will soon become redundant and as such the move will be to the "per user".

## Empowering the many

We started with the idea of the "power of few", where have we seen evidence of this?

We've looked at public, hybrid and community clouds that seem to be leading us towards consolidation – an area that demands regulation and a rise of concerns about who owns and stewards data about all of us. This concern gets multiplied when we look at stacks of services as well as data – all the way through to individual desktops with the potential for divergence between standards amongst the oligarchy controlling the platforms. Hence mediation and open standards are required.

We moved from review of physical relationships of services and data to conceptual considerations around privacy – turning a stone over to uncover some issues that perhaps have always existed but are now being highlighted in the world of cloud computing. Does this convey even more power to the few and demand further regulatory chokers? The regulatory framework consideration takes in governmental control issues around areas such as lawful intercept – and we already have concerns around the world of jurisdictions that have indeterminate – or at least non-universal – moral codes associated with rights to use of data.

The power of the few can take on a different cloak too – the restrictions of access that come with the territory of economic parity – those that can afford access will have more control than those who cannot – at micro and macro level.

And finally, the issue of licensing is one that is challenged in almost absolute terms – just as the music industry has had to develop new operating models for economic sustainability, the same will be true of software vendors and in fact is already happening.

So is the future one of ever-increasing legislation to deal with the power of the few? It is not the purpose of this paper to challenge the need for robust regulatory frameworks – that need is clear – but the perspective of this Author is that if the few are attaining more power, the many are potentially being armed with the weapons for an exponential shift in economic



sustenance. The cloud, if developed with universality, which looks to be likely, has the potential to empower individuals with access to resources and communications that would otherwise be unheard of. The operating models that come under threat are typically stagnant and ripe for change and the old standards that made the few (5%) with economic power the drivers of growth are being replaced

Regulation is about balancing stewardship with liberation and the jurisdictions that acknowledge that there is no perfect approach but considering this equilibrium carefully will be those that empower the many as a consequence of the power of the few.

\*\*\*

