Annexure I

AmCham's Response to TRAI Consultation Paper dated 10th June 2016 on Cloud Computing

Introduction

Cloud Computing is a disruptive technology and is completely changing the way mankind did computing thus far. Cloud is making computing ubiquitous, affordable and accessible, thereby ushering in an era of "Ambient Intelligence and Ubiquitous Computing". The easily availability of this enormous computing power on tap is expected to dramatically impact every aspect of life.

For a country like India, cloud computing has a special significance. India is a fast growing developing economy, and traditional ways of IT enablement would have put an enormous additional burden on its resources. This burden will now become light, thanks to cloud. Looking back to the age of traditional telecommunications, given the high cost and time required for laying telephone lines, it was once deemed financially impossible for the tele density of India to ever match the tele density of the West. However mobile telephony changed this all. Just as mobile telephony enabled India to leapfrog across two generations of telecommunication technology making telephony accessible to all, cloud computing will enable India to bridge the digital divide and become truly IT enabled. India currently lags way behind in the global e-governance index, and by adopting cloud technology, India can bring the benefits of IT to the masses. The Prime Minister's Mission of Digital India has the potential to soon become a reality.

We believe by having a proper regulatory framework, India can attract global investment into cloud infrastructure and services, Indian startups and ISV ecosystem can flourish using the cloud and grow to serve India and global customers from India. India stands at the cusp of an enormous opportunity. Millions of legacy apps have to be made cloud ready and India's software power can leverage this opportunity. Just as Y2K ushered in the first software revolution for Indian IT, BPOs ushered in the second IT revolution, Cloud, Mobility and the Internet of Things can usher in the third IT revolution.

In order for this to happen, Government of India needs to create a pragmatic, light touch regulatory framework. TRAI therefore has a huge responsibility on its hands, and having a consultation process with various stakeholders is the right approach to evolve a proper framework. India however cannot take things for granted. Technology and innovation migrate to the most favorable locale. If there is a less than optimal enabling framework, the opportunity will migrate elsewhere. India therefore stands at the cross roads of a historic opportunity with TRAI acting as the guide.

While we commend the TRAI on initiating this consultation, we also believe it to be worth setting some context. Soliciting input from the private sector to inform the regulatory and policy structures under consideration is sensible and, when handled constructively and in a well-coordinated approach, stands to be widely beneficial. Particularly when undertaken while keeping the government's overall objectives in mind. As such we suggest some overarching considerations that have guided our overall submission:

Clarity and Predictability

For the private sector to be able to make large-scale investments confidently, there needs to be clarity in the rule-setting environment and predictability in market development. It is this that enables business to make forward-looking investment. In this sense, TRAI's involvement as the oversight agency for the telecommunications and networking industries is understandable. We note also that the Ministry of Electronics and Information Technology (MeitY) has been taking an active role in setting policy agendas for many aspects of cloud computing and we hope the two agencies will take a coordinated approach to developing the cloud computing market in India and providing clear signals to the market on how the government would like to see the market develop.

Developing the Cloud market

Cloud computing is still at a relatively early stage of development with the potential therefore for extremely rapid growth. Nurturing, enabling and accelerating this growth will be good not only for India's ICT industry, but as numerous studies are beginning to demonstrate, it is good for national economic growth, business agility, and wider social development, including through promoting greater inclusiveness and government-citizen interactions. Frameworks set up to enable and promote broad-based development and growth should therefore be championed, and it is in this context and this spirit that we have provided our detailed responses to the consultation paper.

Regulation

Given the relatively early stage of cloud computing development we strongly caution against taking an overtly regulated approach to structuring the cloud computing industry in India. At this stage of the sector's development in India, we believe that a heavy-handed regulatory approach will likely inhibit growth. And while cloud is still at a relatively early stage in its growth, it is worth bearing in mind that much work has been done over the last decade in various industry standards bodies, and by the industry as well in establishing best practices. This is not to say that there is no place for regulation. In some areas, such as ensuring network equipment is safe, establishing data privacy frameworks or providing for consumer protection there may be cause for limited regulation. But we would encourage the Indian government and TRAI to look where possible to industry best practices, and we have made mention of this and provided examples in our specific responses.

Procurement

A related area to be considered is procurement of cloud services. Buying cloud services is unlike most traditional technology purchases. Customers are accustomed to buying IT infrastructure using procurement rules designed for traditional purchases such as data center hardware or software; however, such traditional purchasing approaches include procurement practices and contract terms that may inhibit adopting the scalability, lower costs and innovative nature of cloud technology. The industry would like to see an environment that allows for a fast and flexible acquisition process without onerous terms and conditions that enables organizations to extract the full scale and flexibility of the cloud.

Innovation

We would also like to emphasize the potential for local innovation to become squeezed in the event of over regulation. One of the biggest beneficiaries of cloud computing are the Micro, Small and Medium Enterprise (MSME) market, as they are suddenly able to access enterprise grade ICT tools affordably and effectively. Utilizing cloud computing, SMEs are able to scale rapidly and, in many cases, are born as multinational export operations. At the vanguard of this in many markets is the e-commerce sector. Overtly regulating cloud computing tends to disproportionately impact SMEs as their costs, including for licensing, for compliance, and related issues, go up rendering the cost benefit analysis unattractive. India's e-commerce market is growing vibrantly and the innovation in the marketplace is rich, varied, and startling.

India as a Cloud leader

India stands to be an enormous market in cloud computing and to be an enormous global presence in the developments coming forth from the cloud computing sector. In the process of building Digital India, we see all of these issues coming together and cloud computing playing a key role in accelerating the outcomes sought by the Government in its Digital India vision. We therefore recommend TRAI to also provide

leadership and restraint in helping to create a transparent and trusted regulatory environment for India's cloud products and services.

1. Cloud computing is a holistic term encompassing ICT infrastructure, processing, storage, networks, operating systems and applications that are available *on demand* in variable quantities. Cloud computing fundamentally transforms the economics of ICT usage by transferring the focus of ICT consumption away from capital expenditure to operational expenditure. A cloud-based business model enables stronger budget control and greater agility in financing requirements and therefore growing a business.

2. Cloud computing encourages customers to develop a *Development and Operations* culture – an organizational culture characterized by continual exploration and development of new services and operations that can automate, enhance or otherwise improve service delivery. With *elastic computing* provided by the cloud, system operators and engineers at any company at any time have access to the tools needed to explore new solutions on a continual basis without the need for purchasing and provisioning expensive, in-house servers and computers.

3. The agility enabled by the cloud computing model allows businesses to be able to profit from highly variable demand. It is this that is fundamental to the cloud business model and it is what is fuelling the rapid expansion of new services and enabling a new wave of innovation.

4. Customers will choose cloud service providers based on their ability to enable growth (the time it takes to scale up access to services or provide the necessary support), on service reliability (including risk management and technical assurance), and on cost control. None of these are areas that respond well to regulation or government mandate. Because customers will also often need agility in terms of support for different operating systems, programming languages, and so on, this is leading to different approaches by cloud service providers in developing the market, with the result being a rich and varied market environment.

5. When data and computer systems are moved to the cloud, responsibilities become shared between the customer and the CSP. The level of responsibility on both parties depends on the cloud deployment model type, and customers should be clear as to their responsibilities in each model. Typically the CSP will be responsible for securing the underlying infrastructure that supports the cloud, and the customer will remain responsible for the data that is put into the cloud. This shared responsibility model reduces operational burdens in many ways, but it also means that, as the data owner, the customer retains control and ownership over their data.

6. Where government regulation has a role to play is in providing a clear regulatory environment for data privacy such as a data privacy act. With adequate personal data protection provided for in law, there should be no need for additional provisions mandating data control on the cloud. Cloud services should be considered a business without further need of licensing, as this may have the impact of slowing cloud development and adoption if overly-onerous requirements are introduced.

7. Almost even if not necessarily all the ICT services would be on or in the cloud in the days to come. Indian government has already adopted ‘Cloud First, Mobile First’ dictum for e-governance and cloud would definitely be a great enabler in realizing the ambitious ‘Digital India’ program.

8. In fact, online authentication using India’s national biometric ID ‘Aadhaar’ initiative is already the world’s largest such endeavor.

9. Cloud Computing is a disruptive technology and is completely changing the way mankind did computing thus far. More than a particular technology *per se*, cloud is more about a new paradigm in terms of business model.

10. Cloud services need not be brought under any additional licensing and regulatory regime:

a. Almost everything on the Internet (and, increasingly on mobile) is already a manifestation of 'Cloud' and if not, it would very soon be.
b. All cloud services are accessed over the network infrastructure services of telecom licensees. Hence, licensing or even registration of cloud service providers is neither pragmatic nor desirable.

11. Issues related to cyber security, encryption, privacy and data breaches, etc. are indeed important. However, these issues are already covered under the Information Technology Act and the extant rules thereunder. In any case, all these issues including challenges to law enforcement and cross-border jurisdictional issues are generic to the whole of Internet itself. Hence, it would be best if TRAI stays away from those issues to avoid unnecessary regulatory overlap. All the same, TRAI can and should recommend some baseline security and privacy especially for IoT and critical information infrastructure even as it should recommend to the government to allow choice of encryption to the users and ensure consistency across the different sectors within the country. These could include 'security by design', 'privacy by design', 'default encryption', 'strong passwords', etc.

12. It is appreciated that certain government data (identified as sensitive) may need to be stored and processed within the country in the interest of national security, for other government services & functions and definitely for all the private sector and the individuals there should be total freedom of choice. Government has already established dedicated cloud for government agencies.

13. In fact, in several scenarios, free cross-border flow of data is a pre-requisite for ensuring resiliency and enhancing cyber security.
    a. For example, business continuity and disaster recovery can be significantly improved through locating BCP/DR sites in different countries or regions around the globe.
    b. Likewise, cybersecurity can be enhanced by using the approach of 'Follow The Sun' and providing critical support and solutions via security operations and response centers located in different countries for users in India.

14. India should also be cautious about what it does on this front as creating unnecessary barriers would not only increase costs but also pose grave threats to India's largest exports, viz. the IT outsourcing business that fetches over USD 100 billion of annual revenues and is slated to cross USD 300 billion by 2025, according to NASSCOM.

15. Quality of Service (QoS) of cloud services depends on a variety of factors including the architecture, scale, network topology and use by other users and tenants, etc. Hence, this is best left to the market forces.

16. TRAI should instead focus on making suitable recommendations so as the investment into data centers in India is incentivized and usage of cloud picks up both by the government and the private sector.

In light of the above, we now provide our response to the issues raised in the paper in-seriatum.

Comments on Questions contained in the TRAI consultation paper on Cloud Computing

Question 1. What are the paradigms of cost benefit analysis especially in terms of:

a. accelerating the design and roll out of services
b. Promotion of social networking, participative governance and e-commerce.
c. Expansion of new services.
d. Any other items or technologies. Please support your views with relevant data.

Response

There are a range of different factors to consider in evaluating cloud computing technologies. The consultation paper highlights capital expenditure cost savings as a primary benefit, and describes security, reliability, interoperability and vendor lock-in as threats from using cloud services. The paper also highlights that cloud computing offers greater efficiency, scalability, dynamism, reliability and availability that would yield better security, more innovation and lower barrier of entries for SMEs.
There is an inherent contradiction in such views expressed in the consultation. For benefits to emerge in the use of cloud computing, India should focus on creating a competitive market for cloud computing services. This will include avoiding unnecessary regulatory burdens, promoting innovation and adhering to internationally recognized standards. India should not adopt policies that are intended to create advantages for Indian cloud providers operating in India as they only seek to make such Indian providers less competitive in the global market that their cloud services can serve.

a. accelerating the design and roll out of services
   - Enable improved IT efficiency and economies to reduce IT costs.
   - Shifts from fixed cost to variable cost.
   - Allow pay per use. Enable faster delivery of services.
   - Help improve the agility and dexterity of government services.
   - Scalability to meet demand peaks. • Replacement for lost skills

b. Promotion of social networking, participative governance and e-commerce.
   Cloud technologies helps in deployment of various collaboration tools and be available for the users quickly. Start up and e-commerce companies can leverage cloud to quickly develop and deploy the applications and cloud model enables them to scale up or down the infrastructure as needed.

c. Expansion of new services.
   With deployment of PaaS cloud model one can quickly develop new services and deploy them in the cloud environment quickly thus enhancing business agility. PaaS augmented with IaaS can provide both development and deployment environment that can be leveraged to develop new applications quickly.

c. Any other items or technologies. Please support your views with relevant data.
   As the technology shift is moving towards automation, machine learning, artificial intelligence and going forward business decisions will be driven by cognition, Cloud technologies become enabler for such new technologies to enhance business agility.

One of the key reasons for cost reduction in using cloud is" optimization" or pay-per-use where applications needing variable compute at different time can deliver significant cost savings on cloud. Regardless of which deployment or service model is implemented, cloud computing can enable governments to increase the agility and efficiency of their operations and lower overhead costs of ICT. In addition, new computing resources are just a click away, whereas traditional ICT solutions could take weeks or even months to stand

up. Because resources are elastically provisioned, they can quickly scale, and users only pay for computing resources when they consume them. This can be particularly helpful for government services, such as e-government tax filings and returns, which experience a predictable spike in usage and capacity. Cloud computing also supports more rapid and fluid innovation, creating shared services, promoting iterative development, providing built-in analytics that take advantage of big data, and enabling employees to access resources from their own devices to collaborate on a global platform.

Most importantly, cloud computing can increase the security and resilience of an organization's ICT infrastructure. In part, security improves because moving data and services to the cloud can act as a forcing function for robust data governance. As a result, organizations become not only more aware of the data that they retain but also more purposeful about how they treat it. A move to cloud services may also improve security because it transfers some responsibility for managing ICT onto the cloud service provider (CSP). Depending on the cloud service model, cloud providers may not only manage datacenter security but also network controls, identity and access controls, and patching. Large CSPs also have visibility into and the ability to quickly protect their entire environments.

Cloud can also deliver significant security benefits for new and emerging technologies – a process that would be near impossible in a traditional on premise environment.

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

Response

India's focus should not be simply capital expenditure cost reduction. Instead, a longer term view should be taken to seek the benefits of cloud to Indian companies aiming to be competitive in the global marketplace. That said, economies of scale are the driving force of cloud but whether the use of cloud results in cost reduction would depend on the IT requirements of the business. Some workloads or applications that are growing at the same rate as the business might be cost effective to remain in on-premise Data Centers, especially if the latest infrastructure models are already being used.

Increase volume output or productivity with fewer people. Cost per unit, project, or product plummets. This enables businesses to better streamline processes. As most of the service requests in cloud environment are automated and with minimum human intervention, services like Infra, platform and SW are available for users to consume very quickly. Also the consumer (end user) gets billed based on consumption and only when needed, there is no need to have the IT infrastructure purchased well in advance. As usually observed in a typical scenario there is big gap between planned utilization and actual utilization that helps in IT budget optimization.

Acquiring capital for large purchases is difficult, for all sizes of organization. This is especially true for smaller organizations for which finance companies apply rigorous debt to equity ratios and thus the amount of capital they can acquire. For this reason it has historically been difficult for organizations to sufficiently justify capital expenditure to get approval for many projects. Moving to an OpEx model removes this limitation and allows small scale projects to be undertaken, unconstrained by capital considerations. Cloud enables faster delivery of services and can help improve the agility and dexterity of government services. In addition, its scalability allows agencies to respond to peaks in demand for services.

The emergence of cloud services is fundamentally shifting the economics of IT. Cloud technology standardizes and pools IT resources and automates many of the maintenance tasks done manually today. Cloud architectures facilitate elastic consumption, self-service, and pay-as-you-go pricing. Many IT leaders today are faced with the problem that 80% of the budget is spent on keeping the lights on, maintaining existing services and infrastructure. This leaves few resources available for innovation or addressing the never-ending queue of new business and user requests. Cloud computing can free up significant resources

that can be redirected to innovation. Cloud also allows core IT infrastructure to be brought into large data centers that take advantage of significant economies of scale in three areas:

- Supply-side savings. Large-scale data centers lower costs per server.
- Demand-side aggregation. Aggregating demand for computing smooths overall variability, allowing server utilization rates to increase.
- Multi-tenancy efficiency. When changing to a multitenant application model, increasing the number of tenants (i.e., customers or users) lowers the application management and server cost per tenant.

The size of the savings is however difficult to measure and will depend on the type - private vs. public cloud - and usage of a particular cloud service, as well as on how the environment is adapted. Just as engineers had to fundamentally rethink design in the early days of the car, so too will developers have to rethink design of applications. Multi-tenancy and demand-side aggregation is often difficult for developers or even sophisticated IT departments to implement on their own. If not done correctly, it could end up either significantly raising the costs of developing applications (thus at least partially nullifying the increased budget room for new app development); or capturing only a small subset of the savings previously described.

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Response

While business of all size benefit from the efficiencies of cloud services, the most impactful dimension of cloud services in cost reduction is actually the benefit to small businesses, where cloud services can spare these businesses the upfront cost of building an IT infrastructure and enable them to use standard applications off the cloud.

What, when, how, how much and why a customer would use cloud, would depend on respective organizations' own perspective in terms of perceived benefits and risks with respect to their own needs, budgets, technical and financial resources, critical functions, requisite scale, flexibility and seasonality of the operations, extant regulations and physical infrastructure. Businesses should assess what data assets and what computing processes they have, categorise them between those that can/can't or should/shouldn't go into the cloud and the choice of cloud model such as public, private or hybrid. Neither all the data nor all the processes need be in the cloud, at least not in any random or uncontrolled cloud. However, this decision is best left to the customers' choice rather than a matter of regulatory enquiry and determination.

The type of cloud service deployment model by business enterprises are driven by whether the organization can deploy workloads onto public cloud or is it a regulated organization that doesn't allow data/workloads to be deployed onto public cloud. There are scenarios where customer build their own private cloud more from security perspective and augment that with some of the non-critical workloads deployed onto public cloud environment. In that scenario there might be possibility of workloads running on private and public cloud interact with each other and share data/services between them which results in a typical Hybrid scenario. In case of SME's which typically are not regulated leverage public cloud deployment more as that deployment enables them to achieve business agility and scaling up/down features.
Various cloud computing deployment options are possible and selection of which type or model of cloud computing depends on the needs and requirements of each individual customer. Those decisions are not necessarily size dependent, as cloud computing can enable relative small business to scale their services across the globe with minimal capital investment and staff.

The key influencing factors for the selection of deployment model are:

- Existing Infrastructure and application landscape – if an organization has already invested substantially in the IT infra, they typically start with a Hybrid approach to cloud, leveraging their existing investment and also getting benefits of new age solutions on Cloud.
- Application landscape – while most of the applications are rapidly moving to cloud, businesses using legacy applications are looking at IaaS as opposed to newer businesses which are effectively using PaaS and SaaS to build their entire IT environment. This helps them reduce the cost and time to market.

Cloud environments can be public, private, or hybrid, and the drawbacks and benefits vary with each model. For instance, the actual costs of public cloud are relatively low because the public cloud environment benefits from economies of scale, meaning that providers' physical and virtual computing resources are pooled and then assigned and reassigned to serve multiple consumers. As a result, customers sharing distributed resources achieve a lower variable cost than they could access on their own. A private cloud shares many of the characteristics of public cloud computing, including self-service, elasticity, and pay-by-use, in addition to dedicated resources that provide additional control and customization. The hybrid cloud merges the best of both worlds, allowing customers to move between public cloud, private cloud, and traditional on-premises environments.

In addition to various deployment models, there are also numerous cloud services options, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). As with the cloud deployment models, the cloud services options have differing benefits and drawbacks. Whereas IaaS solutions allow for optimum flexibility, providing computing power to support various software programs, SaaS solutions offer ready-made but less flexible programs. SaaS solutions are the easiest to manage, requiring that cloud providers take on a greater degree of responsibility over the implementation of various security controls, and IaaS solutions require cloud customers to continue to manage more security implementations. In both instances, PaaS offers a middle ground, providing a platform and tools to ease the creation and management of organization-specific software.

Enterprises of any size have to manage risks associated with the use of IT. One approach is to use vendors who may be more capable of managing those risks than the enterprise itself. Cloud services often offer SMEs that have limited expertise with the ability to more effectively manage not only cost, but also security and even regulatory compliance, along with benefits of agility. For larger enterprises, key considerations are security and performance.

Enterprises, big and small, need to understand who is responsible for managing what risks, as well as where an external vendor is responsible and how capable it is of doing so effectively. Security is a journey rather than a destination, it requires an ongoing conversation about how risk is being managed. Security requires an understanding of where the "compliance boundaries" are, i.e. some risks are properly the responsibility of the cloud vendor, while some are retained by the customer.

Question 4. How may a secure migration path be prescribed so that migration and deployment from one cloud service to another is facilitated without any glitches?

Response

Cloud service providers tend to facilitate migration and portability in creative and innovative ways without regulatory intervention, because every cloud vendor has a business interest to attract customers from their competitors and will make available tools to facilitate migration. So long as the incumbent provider does not "lock in" the data by technical means which defeat or block the competitor's migration tools, portability is generally not an issue. In addition, for some SaaS services where no data stays to reside with the cloud service provider (e.g. blocking spam), migration is as easy as rerouting email traffic from one gateway to another.

Ultimately, migration path will depend on the needs of each specific case. However, what matters is that the cloud provider gives appropriate security assurances and commits to predefined service levels that will be relevant and sufficient to safeguard the integrity, confidentiality and availability of everything, depending on the type and volume of data and processes to migrate.

A prescriptive approach is not conducive to the growth in cloud computing and will inhibit innovation. Instead, the cloud providers should have the flexibility to offer different approaches to migration for their customers, and the government should allow market forces and user choices to shape the industry direction. Where appropriate, contractual requirements cloud be used by the customer to ensure the continuity of operations. But mandated prescribed standards for cloud providers to handle data, processes and virtual machines developed on other platforms will hurt innovation.

Additionally based on our experience, Migration and deployment are driven by following 4 phases:

- Phase 1 is the 'Workload / Network Compliance Discovery'. To be able to define the perfect migration path it is important to gather key data on the existing customer server & workload environment: servers, workloads, operating systems, application, data, dependencies between applications to name just a few examples. After collection all data has to be analyzed and assessed – and sorted by certain criteria. We then move into the second step which is the planning.
- Phase 2 is the 'Macro Design / Analysis / Micro Design / Wave Planning' phase. For those applications that are a fit for being moved to the cloud, we provide an application assessment report and architecture for the target deployment and furthermore a recommendation for how the appropriate migration strategy will be scheduled. In this phase the different workload characteristics and the categorization mentioned earlier in this webcast comes into play. Of course, in this step not only technical and architectural data get analyzed – a second key input is the financial validity of the transformation and migration: which are the best candidates from a TCO perspective, what migration plan is financially the best.
- Phase 3 is the first 'Migration' phase where standardization and registration are being performed – the phase in the process where we virtualize, the target test environment gets provisioned, all necessary modernizations of OS and MW take place and the workloads get configured for testing and production using analytics, tools and automation.
- Phase 4 is the second 'Migration' phase and the last phase of the process – 'Remediation, Testing and Workload Cutover'. The migrated image, now boarded in the cloud environment goes through some first smoke tests and additional more extensive testing and – if successful – gets handed over to the customer. metering and billing systems etc.

When an enterprise is thinking about migrating to the cloud, it's similar to moving to a new house -IT must plan and organize as well as consider the costs and benefits. This is the same whether the organization is looking to switch between providers or move to the cloud from the on-premise environment.

The question of viability has many parallels with what organizations have dealt with for years in vendor outsourcing agreements. The core issues of financial stability, capital investment, basic service guarantees, and avenues of recourse if the service agreement is breached are all relevant to cloud services.

However, the cloud scenario introduces other issues relating to multi-tenancy and switching providers:

- The customer organization should obtain guarantees about bandwidth and availability in multi-tenant environments. The cloud service provider should set clear expectations about scalability and protections against service disruptions due to scaling of activities by other customers.
- The customer organization should find out whether it can switch providers if the cloud service provider fails to meet expectations, and what the switching costs would be.
- Other issues related to switching providers include:
    - Retaining ownership of domain names.
    - Data portability.
    - Application portability, particularly in a PaaS scenario, and associated costs.

- The cost of data migration to a different service, especially one with very different facilities for hosting important databases.
- Portability of identity and access controls and associated costs. Many cloud service providers expect the customer to use the cloud service provider's identity and access control system. If the organization wants to move to a different provider, it might be forced to re-provision all those user accounts.

In addition to the issues outlined above, we would recommend organizations to seek in their service level agreements and contracts confirmations that their cloud service provider should takes the threat of malicious attacks seriously, that it will make reasonable efforts to protect data entrusted to them from thieves and hackers, and that it will minimize potential attack surfaces. Organizations must also be confident that the cloud service provider should abide by known, unambiguous rules governing how customers' and employees' information is processed, used, stored, and possibly distributed to and shared with third parties.

To ensure a trusted relationship, the cloud service provider must provide reasonable disclosure of those mechanisms; the standards, principles, and industry best practices they are based on; and how their effectiveness is verified. To gain these assurances, organizations should ask the cloud service provider for evidence that it maintains a comprehensive and properly documented information privacy and security program—one that is kept updated and provides safeguards appropriate to the organization's needs.[11]

Organizations should also ask the cloud service provider about its policies and practices that affect the ownership, use, and retention of data (or related aggregated data and metadata) that is stored with the cloud service provider. In addition to that, when thinking about compliance obligations related to data stored and processed in the cloud, organizations should consider two issues. First, should the data in question actually be placed in the cloud, and what conditions would have to be met to do this? Second, what assistance can the cloud service provider provide to help the organization meet the applicable compliance obligations? To answer these questions, the organization must first understand what its own regulatory and internal policy requirements are.

Finally, once an organization establishes the viability of storing and processing data in the cloud, it can address how to meet its regulatory compliance obligations as well as data privacy and security-related commitments it has made to customers, shareholders, employees, and other stakeholders. Just as important is the question of how it will show proof of compliance. The cloud service provider should clarify the processes and escalation paths it will follow in exceptional circumstances, such as notifying the organization in case of a data breach. The terms of agreement should therefore include a list of compliance-related documents that will be provided by the cloud service provider, including certifications, plans, and escalation paths.

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Response

The Authority must appreciate and take into account subtle yet extremely crucial distinction between the two types of data when it comes to personal data.

Firstly, there is data created or stored by the customer into the cloud and for this, the customer should have the right to control and recover, and obtain its erasure from the cloud. However, there could be second type of customer data as well, created, collated or derived by the cloud provider in the course of the customers' use of the cloud service; this should be left with the cloud provider without any right of the customer per se. Of course, such data may need to be anonymized/de-identified from the respective customer at the source of its generation, but the cloud provider should have the right to keep the data and to exploit it even after the customer has left or migrated. For example, a search engine should be able to keep the archives of searches; a cyber security company should be able to retain the data that goes into its threat intelligence; a manmade by different search history with a search engine or the threat intelligence developed and generated

through detection telemetry collected from customers' devices. In such cases, there is no need to go into the respective databases and erase every artefact captured from a particular customer even if or after that customer chooses to stop using that product or service. It would neither be feasible nor in fact is desirable to do so. In fact, it would be highly counterproductive from a security perspective as well.

Admittedly, the discussions have ensued in the context of even in the non-privacy space (e.g. Internet of Things) around whether, for example, geo-location data of cars should belong to the car manufacturers or to the supplier of the navigation systems in the cars. However, any regulatory intervention in this space is unwarranted at this stage, considering that these developments are in very early stages of maturing, and there is for now no compelling evidence of gross market failure or other problems that could only be addressed through regulatory intervention.

We do not believe the customer loses control on its data while availing cloud services. The customer can chose various kinds of cloud services offerings - Public, private and hybrid depending on the nature of data and the industry in which the customer operates. There are multiple regulations already in place for various industries like banking, insurance and telecom which provide for industry specific regulations around management and security standards to be followed for data. Accordingly, these rules will be applicable irrespective of whether the data is getting processed over a cloud platform or as part of traditional IT services. Additionally, a specific rule around Cloud could also lead to conflicting interpretations with the existing industry specific rules. Hence our view is that there need not be any additional regulations to this effect and the customer who is the owner of the data should choose the suitable cloud service offerings depending on the specific industry they belong to and applicable regulations there to.

When dealing with cloud providers, government organizations must be sure that they own their data in order to maintain data and content privacy. That means organizations should explicitly be allowed to access any of their own data - including text, sound, video, or image files and software - for any reason at virtually any time.

We would also suggest the Indian government considers relying on code of practices such as ISO 27018 rather than developing a new regulatory framework to cover this concern.

Data protection and privacy laws and regulations are designed to provide protection over personal data. Non-personal data owned by the user that is stored in the cloud are also protected through contractual provisions between the user and the provider for the use of the cloud service. Government mandated provisions inhibit growth and innovation in cloud computing services and should be avoided. Instead, model contractual terms may be offered as a best practice for cloud providers to adopt.

The Indian government should seek to align data protection regimes with internationally accepted models so that it will ensure continued global data flows with other countries or regions such as the EU. The government should promote policies that advance the goal of transparency so purchasers of cloud-based services can make intelligent decisions regarding the risk of lock-in.

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Response

Standards and interoperability are key to the growth of the ICT industry, including cloud computing. Standard setting should be driven by industry using current standards development organizations with the aim of setting a global framework. A variety of standard setting organizations may be involved in different aspects of cloud computing. The role of government should be to encourage the development and adoption of open standards relating to cloud computing, and to foster interoperability through open and transparent processes. But the government should avoid "picking winners" from among different standards. The

government should participate in standards setting activities as a convener, as a trusted expert, and as a major purchaser of technology and implementer of standards. The government should rely on voluntary, consensus based standards versus technical requirements set by the government.

Firstly, the authority must remain not only technology neutral but also business-model neutral. Both open source and proprietary technologies have their respective advantages and disadvantages. Businesses and users should have total freedom of choice when it comes to open source or proprietary or any combination thereof, unfettered by any regulatory fiat. Some users appreciate a closed proprietary system and will accept less flexibility in exchange for higher security for instance (choice between the iOS and Android is a good example of that), which others will on the contrary choose the higher flexibility, taking the risk of lower security. Again, development is still in such an early stage that the market needs time to mature and authoritative intervention could do more harm than good by disrupting the natural evolution of business practices.

In any case, where technological standardization is considered, for the cloud of all areas it is crucial that standardization efforts be market-led, transparent, open and inclusive, always technology-neutral, outcome oriented and globally compatible (because the cloud by nature works across borders, and anything that would be local would defeat the whole idea and ruin the economies of scale that are achievable). Moreover, there is a lot of work already underway at global level and it'd be best for Indian government, businesses and experts to participate and contribute therein rather than undertaking isolated and disjointed in-country endeavors.

In particular from IaaS perspective conforming to OpenStack standards and from PaaS perspective conforming to Cloud Foundry should be maintained that would enable interoperability between workloads deployed in different cloud environments.

We suggest leveraging already established global standards for Information Security Management like ISO 27001 / ISO 27018 and Cloud Security Alliance framework to be the base for ensuring standardization across different cloud service providers.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? Essential versus desirable parameters and their respective benchmarks may be suggested.

Response

The TRAI should avoid any mandated service quality levels for cloud services as such mandates could limit the development and usage in India of innovative cloud services, applications and devices. These services are different services from traditional telephone services, relying on fundamentally different technology and featuring myriad different service attributes and configurations, with different capabilities and limitations and raising different policy considerations. Amcham believes that service quality is an area in which the TRAI should apply the light-handed regulation followed by many regulators with respect to cloud services and should avoid imposing strict requirements.

For cloud services, examples of QOS parameters that can distinguish providers from others in the market place are: security, resiliency, scalability, flexibility, interoperability and cost. Given these myriad options, a light-handed regulatory approach to Quality of Service will best promote innovation in a competitive market.

Neither there can nor there should be uniform and common metrics for all cloud services, since all of them serve different purposes in different ways, using different media and based on different business models. For example, the performance indicators which will make sense in the service level agreement (SLA) of a cloud-based email security service will have nothing in common with those for a cloud-based backup

service, and neither of the two will be comparable in any way to the relevant performance indicators of IaaS or PaaS service.

SLA's for VM availability apart from 100% Network availability and HVAC (uptime of Cloud DC) should be mandated. Managed IaaS can be also added to include SLAs upto operating system level.

Strength of the cloud is choice to customer. All cloud service providers offer a bouquet of services to the customers based on features, performance and cost. These service parameters are changed based on market requirements, innovation and are left to the choice of customer. Given the diversity of cloud services offers across different models, it is recommended that the regulator should provide the service availability guideline but not the feature or QoS.

Our availability commitments are made through our contractual commitments with our customers. A good thing about cloud services is that customers can actually get these contractual commitments around performance criteria for the length of their use of the service, whereas it may be less common to get contractually binding performance commitments in perpetuity for boxed products. Hence we recommend regulator to provide guidance on Availability and let the performance / QoS for different cloud services to be determined by market and delivered using contractual commitments.

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Response

Since there is no universal singular business model of cloud services, it is neither realistic nor desirable to expect or even accept a common set of metrics. Metrics for service level and performance are a matter of mutual contract between the cloud provider and its customers and the normal dispute resolution mechanism should be used as and when needed. Yes, greater awareness may need to enhanced transparency, efficiency and predictability in such arrangements.

Client of cloud services should have a view of estimated monthly billing based on services being used. The same view should be available as part of self-service portal provided by CSP for the client to service the requests. Apart from estimated billing details clients should also get a view of the services provisioned by the client and also status of tickets raised for any issues. For any ambiguity of the billing there needs to be as part of governance model, client should submit the disputed billing details to CSP who in turn should validate the billing by providing the services provisioned and duration to the client to remove any discrepancy in billing, if any.

Since cloud services are pay-per-use, customers have complete visibility and control of the resources that they are using on cloud. We provide dashboard and analytics of existing utilization and forecast for future utilization. This helps customers re-verify and plan their billing, themselves.

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

Response

There needs to be 24X7 telephonic, chat and web support provided by cloud service providers to raise the complaints/tickets for support. There need to be published governance mechanism which covers escalation matrix to raise the complaints.

Also Cloud services are delivered through commercial contract between customer and provider like other IT services and are governed by the legal framework, jurisdiction and arbitration applicable in the contract.

Globally, while there are different regulations around cloud services, we have not come across sector specific grievance redressal mechanism. It is typically handled by the provider and the legal provisions in the contract.

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Response

There are different approaches to deploy cloud services in a public, private or hybrid model. The consultation document appears to make the assumption that data and processes on the cloud are "online" while data and processes on-premise are "offline". However, an on-premise system that is networked and connected to the Internet can be at as much risk as data or processes stored in the cloud. In fact, security may be more effectively managed by a sophisticated and experienced cloud provider than by a consumer of the IT department of an SME. Keeping data and processes offline can exacerbate availability and reliability concerns.

Using cloud services does not necessarily imply the use of a public and multi-tenanted cloud. The customer's evaluation of risks determines whether data and processes should be stored in a public or private cloud. These risks are for the customer to understand, and it is not practical for a cloud provider to know what is best for the customer. Responsibilities regarding the managing of risks between the customer and the cloud provider will vary depending on the cloud delivery model (e.g. end users have less control over risks in a SaaS model compared to an IaaS model – in the latter, the user may be responsible for ensuring that the operating system is patched for security vulnerabilities, while in the former, the operating system is not exposed to the end user). It is not reasonable nor realistic for the government to effectively mandate outcomes across these various models given that they vary widely. Contractual responsibilities and compliance boundaries will vary equally.

The consultation document over-simplifies and over-generalizes the considerations regarding security. For instance, the assumption made at paragraph 4.6 about data streams being visible to the cloud provider in an unencrypted form is not true in all instances. There are implementations of cloud where storage and transmission of data are protected in a way that only the customer and not the cloud provider or other vendor have access to the keys. Whether the government can gain lawful access to such data will also depend on a range of circumstances on how the data is protected.

The consultation document also reflects a misunderstanding of the role of NIST. NIST does set the security requirements for the United States government. However, it has **no** role in defining requirements for the private except in the form of voluntary guidance, or through requirements that flow down through contractual arrangements to companies selling to the government. Under US law, the United States government must always use voluntary consensus-based standards whenever feasible instead of developing its own standards.

Security is indeed a very important consideration when it comes to cloud services. CSPs can actually play a role in not just ensuring and improving safety and security of the services they provide but also offer Security As a Service. Kindly allow us to elaborate;

1. Cloud providers themselves would need to ensure that their services are safe and secure, meaning resilient, with adequate confidentiality, integrity and availability. This could be achieved notably (as in the European model) through:

    a. An obligation to take technical and organizational measures to manage cyber risk to the cloud service at all times

b. An obligation to detect and report cyber incidents impacting the resilience, integrity, confidentiality or availability of the cloud infrastructure / service / platform. Where an incident only affect one or a few specific cloud users only, reporting could be confidential and to those customers only.

c. An ability to transparently demonstrate compliance to those provisions by way of proofs of compliance, audits, relevant certifications and other forms of cooperation with supervisory agencies.

2. On the other hand, cloud providers should also be encouraged to make security as a service available to their customers in a way that can be adapted and tailored to the different needs of each. These could include things like:

a. A requirement to ensure adequate authentication mechanisms to ensure that only authorized users of the customer can access the cloud resource.

b. A requirement to make available to the customer metrics on the security posture and cyber risk profile of the cloud infrastructure / platform / service in real time. Metrics for the same should be defined in consultation with relevant stakeholders including but not limited to the cyber security vendors, be transparent and auditable.

c. A possibility (not necessarily a requirement but a lawful option) to provide security as a value added service as part (or on top of) the main underlying cloud service.

Information assurance has been a long-standing practice since the traditional boxed product and on-premises systems era. Many governments today have established IT security programs that address risk-based processes (such as data classification schemes, lifecycle management, etc.), policies, and governance models. Many of these can be re-used and adapted for a cloud environment, whereas others (e.g. physical asset management) may need to be reapplied or deprecated. Because cloud moves much faster than traditional IT products, cloud assurance programs must be calibrated to match the pace of technology while still meeting the established security bar.

Achieving that goal requires a rethink and active risk-based decision making at every step of a government's process of developing and implementing a cloud assurance program, as well as a clear understanding of the different roles and responsibilities involved. Having an effective governance model can clarify the roles and responsibilities for government and third party stakeholders alike – these are necessary to consider risk and efficiency and to determine whether new technologies are able to be consumed. In addition, determining data and system sensitivity and criticality requires a government to weigh the relative risks related to the confidentiality, integrity, and availability of different data sets and systems. Leveraging global standards enables governments to achieve a high level of security with maximum agility and efficiency, and assessing and managing unique risk scenarios not mitigated by global standards solidifies a risk-based approach. Governments that establish ongoing authorization processes also ensure that highest priority risks are regularly evaluated. Ultimately, a risk-based approach must also be instilled through continuous improvement, a process during which governments evaluate how effectively risks are being managed and how risk priorities might be shifting.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Response

In our view, termination or exit provisions are independent commercial provisions in a contract agreed between the parties and are not linked to security of data. Security of data would be governed by the standards and obligations agreed to between the parties with respect to storing and processing of data in a cloud environment. The customer can chose various kinds of cloud services offerings - Public, private and

hybrid depending on the nature of data and the industry in which the customer operates; thereby ensuring that security standards applicable on the nature of the data are met.

Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Response

Migration from one cloud service provider to another is feasible if the cloud service providers comply to open standards which would make them interoperable. Migration of workloads becomes complex due to proprietary underlying technologies used by CSP's and availability of same platform in the target cloud service provider. Even before migration is planned one need to assess the feasibility of the same first. Migration has to be phased/step process which would include classification of workload, compliance, data security needed, design and actual migration.

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?

Response

Offering / Responsibility		Bare Metal Cloud	Private Cloud (Virtual, Single Tenant)	Public Cloud (Virtual, Multi-Tenant)
Data Center Management		CSP	CSP	CSP
Provisioning	Server	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform
	Operating System	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform
Management	Hypervisor	N/A	CSP Automation – Monitor, Inform, Request, Perform	CSP Automation – Monitor, Inform, Request, Perform
	Hardware	CSP Automation – Monitor Customer – Monitor (optional) CSP Automation – Inform Customer – Request CSP Manual – Perform CSP Automation – Perform Customer - Perform	CSP Automation – Monitor CSP Automation - Inform CSP Automation – Request CSP Automation - Perform CSP Manual – Perform	CSP Automation – Monitor CSP Automation - Inform CSP Automation – Request CSP Automation - Perform CSP Manual – Perform
	Operating Systems	Customer	Customer	Customer
	Applications	Customer	Customer	Customer

CSP – IaaS Cloud Service provider
Monitor – collect statistics on performance and health
Inform – Provide notification of status
Request – Using API or Web Portal, create request for action/task
Perform – Complete requested task/action

Additionally, as ministries and agencies determine which data, systems, and services they want to migrate to the cloud and how they will manage risks, they should also consider which cloud service and deployment models are most fitting for their needs. In each of the cloud service models, the responsibility for various security functions is divided between the cloud service provider and the ministry or agency customer. As a reminder, there are three major types of cloud services models: IaaS, PaaS, and SaaS.

- IaaS pools hardware resources for compute, storage, and connectivity capabilities, over which a customer can deploy and run operating systems and applications (i.e., PaaS and SaaS).
- PaaS delivers application execution services and often an operating system, enabling customers to create and deploy their own applications (i.e., SaaS) with greater agility.
- SaaS, also referred to as "on-demand software," delivers ready-to-use applications, such as e-mail, customer relations and management systems, on scalable cloud infrastructure.

In any service model, the cloud service provider manages the underlying cloud infrastructure—the datacenters that power the cloud service. However, responsibility for various security controls otherwise varies. As a result, risk scenarios related to customer control requirements may respond most noticeably to architecture decisions that alter these responsibilities and corresponding levels of control. Systems and data sets over which governments want to retain greater structural control, for instance, may be more suitable for IaaS or PaaS solutions, within which governments have more flexibility regarding security implementations. Alternatively, for SaaS solutions, cloud service providers take on a great degree of responsibility for the implementation of security controls, reducing the breadth of customer responsibility compared to IaaS or PaaS solutions.

In any service model, coordination between cloud service providers and ministry or agency customers is key. Therefore, in addition to assessing cloud service providers, governments should also carefully assess ministry or agency implementation of security controls; cloud environments result in shared security responsibilities between cloud service providers and customers. In each service model, government customers and cloud service providers may have full or shared responsibility for certain security controls.

For instance, SaaS providers are responsible for managing service-level capabilities, which include employing security best practices such as penetration testing and defense-in-depth to protect against cyber threats. SaaS providers are also responsible for physical and data security in the form of employee access controls, encryption of data in transit, and enabling strong authentication. However, customer responsibilities include user identity and access controls, device management, and data management (e.g. rights management services, data loss protection), which are unique activities that the customer must implement. These security activities, which are under the customer's purview, empower the customer to control, access, and protect its own data.

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Response

The success of the cloud computing industry depends on the global interoperability of services and the free movement of data across borders, as well as robust protections for the privacy and security of customers' data. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it and they rightly expect that the information they entrust to cloud service providers will be highly secure and that cloud service providers will be respectful of their privacy. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues.

The legal constraints on the user should not be binding on the cloud provider, and rightly so. The cloud provider may not know what kind of data the user is putting in the cloud, and what restrictions may apply to a particular type of data. Though counter-intuitive, the question actually needs to be reversed.

It is the customer's responsibility to know what they can and cannot do with respect to certain tyoe of data and hence, they must make an informed choice and decision about using the cloud for the same accordingly. For example, if a certain type of data cannot be exported out of the country on account of any regulations, the customer should choose a cloud provider who meets the requisite conditions and ensure that the same are clearly chalked out in the respective contract.

Yes, to enable customers make informed choices, cloud providers should be transparent upfront about data location and the options available to limit migration / transfer of data to foreign data centers, if any, and parties should agree on the prior notice and possible compensation rules that would apply if terms and conditions were to change. For example, in the German network and information security agency's cloud

procurement catalogue, the only additional information required is prior disclosure by the cloud provider of any foreign data access provisions that the cloud provider may be subject to and thereafter, it is the customer's decision what and how to go about choosing the service, if at all.

We encourage trans-border data flows to help grow our developing economy, once a project is in contractual mode, it should be mandated that no data can be transferred outside the country without written concurrence of the end user leveraging cloud services.
We recommend following guidelines for disclosure and for protecting customer's data on cloud:

- Cloud Service provider should transparently let the customers know location of their data
- Cloud Service provider should enable encryption and allow customers to encrypt their data on cloud
- In case of IaaS, where customer has more control, CSP should provide networking capabilities to restrict access to the data using RBAC.

Question 15. What policies, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Response

Firstly, cloud is about achieving efficiencies through consolidation of data centers that are interconnected via resilient telecommunication links.

Notwithstanding the location for storage of data with respect to any particular user, service or use case the existing norms for lawful interception and monitoring under the extant laws within India, viz. the Indian Telegraph Act and the Information Technology Act) are applicable. In that sense, cross-border data communication is similar to the international voice calls in that sense.

Typically CSP's provide data center services centered on the delivery of on-demand server infrastructure. The do not manage the content or applications hosted from our infrastructure as this is the direct responsibility of our customers. CSP should accept subpoenas sent via fax, email, regular mail and hand-delivery. CSP should respond to all valid subpoenas or court orders from entities and courts who have proper subpoena power and jurisdiction over CSP.

The Indian cloud market is quite mature and major players already have their data centers operating in India. Therefore the requirement of hosting data outside India is remote. Only in the case of backups and for disaster recovery data, the data can be stored outside the country. This choice is however entirely that of the customer. In most cases the primary data will reside in India, and the backups will reside either in India or elsewhere. There is also a theoretical possibility of an entity in India choosing to locate its data outside India. In case Law Enforcement requires such data, there already exist time tested frameworks like the Mutual Legal Assistance Treaty between countries to handle such remote contingencies.

Existing legal agreements, such as Mutual Legal Assistance Treaties, need to be modernized to ensure they are fit for the cloud area. These agreements already provide a mechanism for governments, including the Indian government, to obtain digital information stored outside their borders, but there's room for improvement. Ultimately we need an updated set of broadly accepted rules that preserve the rule of law and work effectively across national borders. As new national laws are passed to address these issues they must respect the sovereignty of other countries and the fundamental human rights and online privacy of all users – they cannot be a blunt instrument to seek unilateral and unfettered access to information.

In addition, we would recommend that the Minister appoint a single agency to coordinate all Enforcement Agency processes to obtain orders for disclosure of data from cloud service providers. All Enforcement Agencies will work through this single agency to pursue and enforce all such orders. Cloud service

providers will be expected to appoint, and identify to the minister, a point of contact who will be responsible for receiving and responding to all orders issued against them.

Alternatively, Governments should leverage existing mutual legal assistance treaty (MLAT) arrangements and INTERPOL to address lawful intercept requirements beyond national boundaries. Any obligation to be imposed on a cloud provider to decrypt or provide access to data should apply only if the system architecture enables the decryption to take place (e.g. where the vendor or operator holds the key). It should not be required if the architecture does not allow the vendor or operator to perform such a decryption. Access requests should be backed by proper legal authorization. Encryption used by corporate enterprises intended to create a secure private network for corporate communications should not be subject to requests for access to unencrypted data.

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations thereunder? Please comment with justification.

Response

It is important to recognize that, much as was the case with the Internet's commercial development, the developments in cloud technologies and the global spread of cloud business largely have been achieved in the absence of, not because of, government oversight and intervention. The innovation that has fueled the explosive growth in cloud computing technologies to date has been the result of private sector investment, in a climate of slight, if any, regulatory oversight.

Accordingly, it is vital for the TRAI to set a national policy framework that will support the continued, aggressive investment in the next-generation network infrastructure necessary to power the cloud computing applications and services. Over-regulation of communications networks will slow the deployment of the ubiquitous, next-generation networks over which the emerging cloud services - from software as a service Applications, to hosted VoIP applications, to contact centers, to the Internet of Things - will ride as it develops over the coming years. We encourage TRAI to adopt policies with respect to the cloud computing that will help to support the continuation of this network investment more generally.

Beyond these important issues of infrastructure deployment the policy landscape is growing more complex in other ways. As cloud solutions gain adoption across a greater range of market and industry segments, and at greater scale, many stakeholders in the cloud ecosystem are finding themselves engaged with a broad array of agencies with varied roles, levels of experience, expertise, and confusing and sometimes conflicting regulatory and enforcement authority regarding cloud services. This situation is mirrored both at the national and international level. This creates uncertainty about the regulatory authority's approaches to the issues and about the cloud business opportunities in these sectors.

Given the breadth of cloud services, and their impact across virtually every sector of the economy, the assortment of agencies implicated by the cloud is not surprising. Nevertheless, the great potential for regulatory confusion through duplicative and inconsistent rules and enforcement—and, in turn, for detrimentally affecting innovation and investment in cloud technologies—is a significant cause for concern for industry stakeholders.

The potential for negatively affecting private sector investment in the networks and communications technologies that are essential to the cloud marketplace must be at the forefront of TRAI policies. The TRAI should seek to foster a coordinated framework for that minimizes regulatory burdens, provides policy clarity and certainty, creates a climate that maximizes this enabling network infrastructure investment, and recognizes the global nature of the cloud technology.

There can be no such thing as a definitive "scope" for cloud computing services. Anything and everything can be or become a cloud service. Trying to define a scope in law would essentially mean chilling innovation and setting the boundaries of cloud irrespective of what technological and business model innovation may evolve. Cloud is not a technology, it is a new paradigm, a new way of doing business to deliver storage and computing services remotely through a novel approach to architectural design.

Hence, any proposal to bring in a licensing or even registration system would be a backward step considering that:

a. Almost everything on the Internet (and, increasingly on mobile) is already a manifestation of 'Cloud' and if not, it would very soon be.
b. All cloud services are accessed over the network infrastructure services of telecom licensees. Hence, licensing or even registration of cloud service providers is neither pragmatic nor desirable. In fact, on July 20, 2006 Indian government had directed ISPs to ensure unfettered access to the Internet except for the specific webpages / URLs specifically directed by the government to be blocked. Effectively, it implies that the customers should have unfettered access to any service, application or information unless it has been blocked / restricted using the due process of law.

The scope of cloud services is very broad and ranges from infrastructure to software which is provided as a service to a customer. Accordingly, we believe that cloud service providers should not be subjected to any additional license or registration for the following reasons:

- Any kind of licensing or registration goes against the basic mandate of the current government i.e., "ease of doing business" and "liberalize"/"deregulate" what ought not to be regulated;
- The services rendered via Cloud are depended on infrastructure owned by private companies. For instance, for successful functioning of Cloud Services the Cloud Service Provider ("**CSP**") is dependent on telecom operators and internet service providers. As is the case, these industries are already regulated. For the same reason there is no reason for any additional licensing requirements so as to regulate the CSP separately.
- There is an urgent need for the creation of a robust IT infrastructure and cloud services will definitely play an integral part in this program. For micro, small and medium enterprises, especially the start-up community, it is extremely important to have access to affordable cloud infrastructure whereby facilitating affordable solutions to the public at large. Hence, such move will impact the scalability of cloud services offerings in India thereby impacting private as well as government projects like Digital India which heavily rely on cloud offerings to make them commercial and technologically viable.

In essence, we are of the opinion that any kind of licensing requirement will be counterproductive and could possibly keep CSPs away from India if the atmosphere is not conducive for business. Instead, our suggestion will be that Government should consider adopting relevant international standards as any law relevant today could become obsolete or redundant tomorrow.

India already has a surfeit of Laws under IT Act, Consumer Protection Act etc. to take care of the various issues which might arise due to proliferation of cloud services. So there is no need for a separate Law or a licensing mechanism for taking care of cloud services. Market forces and customer requirement should be allowed to take care of these. For instance, there is currently no licensing requirement for software development and sale. All the problems which can arise in cloud, like service standards, SLAs, security, privacy, Law Enforcement Access etc. are present in software development and IT services. However these are all handled under the ambit of existing laws. In fact, the absence of regulations has enabled the proliferation of the software industry in India. To quote another example no licensing is required for mobile app development. We feel that similarly for cloud, there is no need for any Licensing or Licensing authority.

In the case of the private sector, the customer will determine the type of cloud service needed and thereafter based on the commercials and the technical specification will select the appropriate cloud provider. Any

disputes can be taken care of by existing legal redress mechanisms. In the case of Government, since the procurement has to be completely transparent and also for compressing the very long and tortuous procurement process, it is important to empanel cloud service providers based on the requisite international standards. Government organizations will then be able to benefit from the agility provided by cloud by incorporating agile procurement. This is being done by Ministry of Electronics and Information Technology (MeitY).

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

Response

Amcham considers that requirements for compliance with interception and monitoring requirements should further the dual objectives of encouraging new market entrants and competition, and at the same time further the important national security and law enforcement requirements of the Indian authorities. Government authorities should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. They should also commit to using existing MLAT processes in order to obtain data that is stored beyond their borders.

Providers with a physical presence in the country should be subject to the law of the country. For those without any physical presence, can appoint a representative in country who would be the contact point and control point through which national jurisdiction is exerted over the cloud provider.

As for the question of "CSPs in possession of data" related to national security breaches, the question to ask is whether the CSP has – or can or should have – any knowledge of the data that the users puts in the cloud. For instance does India want a Cloud Service Provider to inspect the data of all its customers in search of data that may be related to a breach of national security in India? Firstly, how would the CSP know, and secondly, does India really want the CSP to learn about such sensitive data.

Under European e-commerce law, cloud providers who only convey, cache or host user data are not liable for the content of such data, unless they are informed that there is something wrong with the content, in which case they must take action to have it removed. A similar system could be thought of here. However, what is important to bear in mind is that:

- The responsibility to detect information that's relevant to national security should not be delegated to the cloud provider, who has neither the authority, nor the legitimacy, nor is skills, nor more importantly the need to know or determine what relevant to national security.
- At the same time there should be some due diligence in terms of cooperating with competent authorities through due process and under the rule of law to facilitate official investigations.

The existing laws sufficiently addresses the concerns around access to information and that there should not be a separate protocol in this regard. This is so because these issues are not unique to a cloud environment but are applicable to any kind of digitized data. Separately, it is also imperative to note that CSP providers are not the owner of the data shared on a cloud environment but is only the processor. Accordingly, it may be practically impossible for the CSP provider to monitor the veracity of all the data shared on the cloud environment, especially considering the volume of data that is transmitted. It is also estimated that the volume of data would exponentially increase and any general supervision is practically unviable. More importantly, the CSP is not the owner of the data and hence the CSP would not be entitled to access the data as this could potentially raise serious concerns on confidentiality and integrity of data.

All cloud providers operating in India fully operate under the Laws of India. So they fully, willingly and whole heartedly submit to the territorial and legal jurisdiction of India. Currently there are

established legal processes which Law Enforcement agencies in India follow to access data from cloud service providers.

(a) Most cloud customers are enterprise customers. Law Enforcement agencies have the authority to directly approach these enterprises who are custodians of the data to obtain the same.
(b) In the case of individual subscribers availing free services like webmail etc, there are currently established processes through which Law Enforcement agencies obtain data from cloud service providers on a daily basis.
(c) In the case of say, an Indian National residing overseas and availing the services of a cloud service provider, as per the extant international Law, the Law of the country where the person resides will prevail. To obtain data of such individuals, there exist international treaty mechanisms like the Mutual Legal Assistance Treaty (MLAT).

Question 18. What are the steps that can be taken by the government for:
(a) promoting cloud computing in e-governance projects.
(b) promoting establishment of data centres in India.
(c) encouraging business and private organizations utilize cloud services.
(d) to boost Digital India and Smart Cities incentive using cloud.

Response

Indian government has already adopted the dictum of 'Cloud First'. Likewise, there is the "Cloud First Policy" in UK.

On the financial side, public subsidies (direct as in money and indirect as in tax franchise or land allocation, for example) must be compliant with the state aid rules under WTO.

On the legislative side:

a. Creating a policy context that accepts and encourages unhindered international data flows. The underlying point is that locking or restricting Indian data within the Indian jurisdiction would be counter-productive as any such barrier would be reciprocated by other countries and thereby in the long run, undermine the very value proposition of cloud and such other paradigms.

b. And in particular creating a regulatory framework whereby overseas customers (including but not limited to those from places like North America and Europe) will confidently and easily choose to have their data hosted in India, for instance by achieving that India's privacy regime is recognized as "adequate" by the European Commission under the EU privacy law, and by putting in place mutual legal assistance treaty (MLAT) and other cooperation treaties with governments of key international partners so as to facilitate cooperation of law enforcement and national security agencies with respect to data in the cloud.

Key factors that would promote cloud computing in e-governance, Digital India, Smart Cities are:
- Clear mandate for government organization to adopt "Cloud First" policy for all existing and future IT requirements.
- Empaneling private Cloud Service Providers at par with government agency's cloud
- Signing the rate contract with key empaneled CSPs to enable government customers to sign the rate contract
- Creating a working model for government organizations to handle pay-per-use billing models prevalent on Cloud.

Key factors that would promote establishment of data centers in India:
- Acknowledging cloud data centers as Infrastructure sector allowing energy duty exemption and other tax incentives for setting up / growing the cloud datacenters in India.

- Ease of doing business for international organizations, allowing multiple jurisdiction and arbitration locations outside India
- Abolishing physical audit or verification of the cloud datacenter in the guidelines
- No data localization requirements, making sure that cloud providers are not liable for disclosure of data,
- Not saying that enforcement agencies should provide encryption keys or attempt to directly access the data stored
- Reducing the cost of Internet BW
- Increased Internet penetration in India

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

Response

Central government in India has already created 'Meghraj' – the government's own private cloud. Several state governments and other public sector entities are also undertaking similar endeavors. On the financial side public subsidies (direct as in money and indirect as in tax franchise for example) as acceptable under WTO state aid rules.

There is a case to be made that some government applications are best hosted on a government private cloud (as opposed to commercial clouds available in the market). How big that cloud needs to be and what functions it needs to host is the prerogative of the respective governments. Multi-tenancy is a desirable feature because the bigger the resource, the higher the number of tenants, the larger would be the economies of scale.

At the same time, it is worth reflecting on where the boundaries of the government cloud should be set, and how it should be made to federate with commercial clouds, considering that commercial cloud services may be both more agile and economic compared to the government's own cloud.

Last but not the least, the architectural design and the procurement of the government cloud should be technology-neutral and choose best options available rather than choose technologies emanating from a particular business model or philosophy or geo-location. For example, a particular technology should be used if and only if it is best of the breed and not just because it happens to be indigenous. This is particularly true of security, since the government cloud is certainly the crown jewel to defend, so it needs the best security capabilities available.

Therefore there can be dedicated cloud for government applications and the same can be carved out Cloud service provider's public cloud which would be dedicated for Govt. The dedicated private cloud build on CSP's public cloud should be multi-tenant, secure and should be flexible to deploy any of the known hypervisors including Openstack.

Customer decisions about whether to deploy public, private, community, or hybrid cloud platforms are often driven by perceptions of the level of security and customer control. Public cloud models provide distributed resources, resulting in unprecedented efficiencies, cost savings, and resiliency, and the newest features and security techniques are applied to the multi-tenant environment first because of the expansive, world-wide user base that it supports. According to Forrester research firm, there is increasing evidence that more enterprises are adopting public cloud platforms as "best, not only for customer-engagement apps but for analytics and core-business apps as well."2

[2] http://www.itwire.com/business-it-news/cloud/72765-%E2%80%98disruption%E2%80%99-ahead-in-maturing-public-cloud-market-forrester.html

Alternatively, private cloud models enable greater customization. Nevertheless, meeting customers' security objectives may not directly correlate to the need for a private, dedicated infrastructure. Large CSPs, have robust capabilities for managing a shared infrastructure while still providing significant and auditable assurances of the security of customer data, including through logical isolation. In other words, while dedicated private cloud solutions can be more specialized, a multi-tenant public cloud is still subject to the same security controls. In addition, due to the large customer base and demand, multi-tenant public and community clouds are prioritized for certification.

Data hosted in the cloud often moves between different services and devices, and given the global nature of commerce and of cloud services, data may also need to move across borders. Some CSPs offer customers choice in where their data resides, mitigating concerns about data sovereignty.[3] In other contexts, governments may opt for dedicated, private cloud solutions. Requiring all public sector data to be subject to data sovereignty concerns is not consistent with fostering an open, global Internet or with cloud-first principles, and in most circumstances, with effective data classification, governments can ensure that relevant data stays within the confines of a regional selection and travels only between countries with data transfer agreements in place. However, under a very narrow set of circumstances (i.e. top secret data), a data residency requirement may be appropriate. Where local cloud service provisioning is preferable to avoid unique risk scenarios related to extremely sensitive data, service provisioning partnerships between global CSPs and local CSPs or technology companies may be considered.

Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

Response

India is a leader in the information and communications technology sector, and it is important that it continues to set an example by eliminating regulatory barriers to the free flow of data across borders. A successful cloud computing industry depends on global interoperability of services and the free movement of data across borders. We recognize the need for legal regimes that respond to evolving technology through fair, uniform procedures that strike a fair balance between privacy and law enforcement. However, these interests must be balanced against the need for cloud service providers and consumers to move data as they see fit. Numerous studies have indicated that the restriction of cross-border data flows by means of local data storage requirements and other policies has a negative impact on the ICT sector and a state's economy as a whole.[4]

According to the World Bank's 2016 World Development Report,

Cross-border data flows are likely to increase with the increasing use of cloud computing, which relies on data flowing back and forth as users retrieve and update information directly on the servers. Barriers to data flows will force firms to relocate tasks and operations, change their information technology (IT) architecture, engage a different supplier, or discontinue services to customers. These barriers disrupt two of the most important business trends facilitated by the internet: the fragmentation of production into global

[4] See, e.g., William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwaechter, *Internet Fragmentation: An Overview*, World Economic Forum (January 2016), available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf ; Business Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World* (2015); International Chamber of Commerce, *Localization Barriers to Trade*, Policy Statement 103/323, available at: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2014/ICC-POLICY-STATEMENT-Localization-Barriers-to-Trade/; Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, The Information Technology and Innovation Foundation (2015), available at: http://www2.itif.org/2015-cross-border-data-flows.pdf.

value chains, and the creation of offshore service hubs like the business-processing operations in India or the Philippines.[5]

TRAI should avoid erecting discriminatory and protectionist barriers and consider specific provisions designed to protect the movement of data, subject to reasonable safeguards like the protection of consumer data when exported. The TRAI should likewise consider that to support the Digital Economy in India, companies should not need to build physical infrastructure and expensive data centers in every country they seek to serve, as this requirement adds unnecessary costs and burdens on providers and customers. TRAI policy likewise should take into account that if some states adopt data localisation mandates, others are likely to follow. This approach would frustrate the capacity of multinational companies to establish call centers, data storage facilities, and other operations in India. Therefore we urge the TRAI to confront these localisation barriers through specific provisions designed to promote access to networks and efficient data processing.

For many services, data would have to perforce traverse across central and state governments. For example, while a student may be provided scholarship by the state government but the identity authentication with Aadhaar would be done by the central government. Hence, it would behove well for the country to deploy central and state data centers efficiently in the spirit of 'cooperative federalism'.

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Response

On the financial side, public subsidies (direct as in money and indirect as in tax franchise or land allocation, for example) must be compliant with the state aid rules under WTO.

On the legislative side:

a. Creating a policy context that accepts and encourages unhindered international data flows. The underlying point is that locking or restricting Indian data within the Indian jurisdiction would be counter-productive as any such barrier would be reciprocated by other countries and thereby in the long run, undermine the very value proposition of cloud and such other paradigms.

b. And in particular creating a regulatory framework whereby overseas customers (including but not limited to those from places like North America and Europe) will confidently and easily choose to have their data hosted in India, for instance by achieving that India's privacy regime is recognized as "adequate" by the European Commission under the EU privacy law, and by putting in place mutual legal assistance treaty (MLAT) and other cooperation treaties with governments of key international partners so as to facilitate cooperation of law enforcement and national security agencies with respect to data in the cloud.

In Summary:

It is critical that TRAI develop a policy framework for cloud services that can help ensure the on-going, robust network deployment necessary to support this technology into the future. TRAI's policies must minimize regulatory burdens, and provide policy certainty that will create the climate to maximize essential infrastructure investment. The key attributes of that framework should include:

- support for the collaborative, self-regulatory initiatives among industry stakeholders that have fueled the growth of the cloud services industry and benefited small and medium enterprises to date;

[5] See http://www.worldbank.org/en/publication/wdr2016 at 300.

- in those limited cases where regulatory action may be justified, use of a light touch, flexible, well-coordinated regime that protects innovation and facilitates rapid cloud market developments;

- clear and transparent rules governing law enforcement access to data and a commitment to follow existing mutual legal assistance procedures; and

- a policy framework for cloud services that facilitates international interoperability and the seamless global deployment of cloud services.

- TRAI should carefully consider if regulation is necessary beyond existing law and, if so, get the right balance between regulatory protection and flexibility for service deployment and use;

- Digital transformation possible only if we embrace innovation with the light touch regulatory approach;

- Regulatory enablement accelerates service delivery & make a meaningful impact on the lives of the citizens;

- Stimulate market development through the promotion of open and competitive markets and adequate consumer protection, wherever possible, through application of existing legal and regulatory frameworks;

- Avoid and, where possible, eliminate barriers to seamless cross border data flows;

- Avoid restrictive data localization requirements that adversely impact investment and innovation;

- **Recognize distinction between services to individual consumers and those sold to businesses to avoid automatically extending consumer protection obligations to the enterprise providers**;

- Consider enabling policy framework that is technology neutral and future proof. When necessary regulations deemed should be a light-touch horizontal regulatory regime that encourages investment and innovation.
