TRAI CONSULTATION PAPER ON CLOUD COMPUTING

MICROSOFT RESPONSE

Microsoft Corporation India Private Limited (MCIPL) welcomes the opportunity to present before Telecom Regulatory Authority of India, its views on Cloud Computing.

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.

Microsoft has a long and abiding commitment to India lasting over 25 years and has partnered with central and state governments in various e-governance projects. Microsoft has established development centers in India where thousands of Indian engineers are working on developing State of the Art software. Microsoft was the first MNC to establish cloud datacenters in India to offer cloud services from local datacenter to the Government and private sectors in India. Microsoft currently has three hyper scale data centers in India offering a wide array of cloud services ranging from IAAS to SAAS. Various Government and private organizations are already leveraging the power of this cloud infrastructure to dramatically enhance their productivity at a fraction of the cost.

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.

Chapter#1: Introduction

No comments

Chapter#2: Introduction

- Benefits of cloud computing should also include brining innovation to SMEs – through first party and third party services readily available on cloud platforms.

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.**

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. For instance, Microsoft detonates email attachments blocked by our advanced threat protection service, and if malware is found in the attachment, then we can search our entire cloud environment for that attachment and protect all of our customers from that malware. Alternatively, if a government agency detects a new piece of malware in its environment, then to protect other agencies, it must share that malware, and other agencies must look for it—a much more tedious process.

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. For example, the Microsoft Azure IoT Suite secures devices while they are out in the field by providing a unique identity key for each device, which can be used by the IoT infrastructure to communicate with the device while it is in operation. Azure IoT Hub

access control policies in the cloud enable activation and disabling any device identity, providing a way to disassociate a device from an IoT deployment when required. This association and disassociation of devices is based on each device identity.

Additional device security features include the following:

- Devices do not accept unsolicited network connections. They establish all connections and routes in an outbound-only fashion. For a device to receive a command from the backend, the device must initiate a connection to check for any pending commands to process. Once a connection between the device and IoT Hub is securely established, messaging from the cloud to the device and device to the cloud can be sent transparently.
- Devices only connect to or establish routes to well-known services with which they are peered, such as an Azure IoT Hub.
- System-level authorization and authentication use per-device identities, making access credentials and permissions near-instantly revocable

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

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.

Research Microsoft conducted, based on customer data, indicated that cloud impacts all areas of spending - the infrastructure costs, costs of supporting and maintaining existing applications, and new application development costs. The supply-side and demand-side savings impact mostly the infrastructure portion, which comprises over half of spending. Elasticity in particular is a game-changer because, as described before, renting 1 machine for 1,000 hours will be nearly equivalent to renting 1,000 machines for 1 hour in the cloud. This will enable users and organizations to rapidly accomplish complex tasks that were previously prohibited by cost or time constraints.

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?

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.

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

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. Microsoft believes that this is best addressed through a set of best practices and contractual arrangements rather than prescribed requirements. The practices that found work well both in our experience and through working with customers and governments around the world span considerations around cloud service provider viability, transparency, control and compliance.

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.[1]

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. Microsoft recommends that organizations develop a data classification policy and a set of —harmonized compliance requirements - a list that summarizes the organization's regulatory and internal policy obligations and that can, in turn, be used to define the requirements the organization has for the cloud service provider.[2]

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?

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

[1] For real-life examples of such documentation, see —Microsoft's Compliance Framework for Online Services|| and —Securing Microsoft's Cloud Infrastructure|| at www.globalfoundationservices.com/security/index.html. See also www.microsoft.com/downloads/details.aspx?FamilyID=5736aaac-994c-4410-b7ce-bdea505a3413&displaylang=en

[2] See the discussion of the Process core capability area of the DGPC framework in —A Guide to Data Governance for Privacy, Confidentiality, and Compliance: Part 2: People and Process|| at www.microsoft.com/datagovernance.

at virtually any time. For leading cloud services, data ownership is certified by ISO/IEC 27018. We would recommend the Indian government considers relying on a code of practices such as ISO 27018 rather than developing a new regulatory framework to cover this concern. To be concrete, ISO 27018 requires that cloud service providers operate under six key principles:

1. Consent: CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer.
2. Control: Customers have explicit control of how their personal data is used
3. Transparency: CSPs must inform customers where their personal data resides and make clear commitments as to how that data is handled
4. Accountability: ISO/IEC 27018 asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of personal data
5. Communication: In case of a breach, CSPs should notify customers, and keep clear records of the incident and the response to it
6. Independent and yearly audit: A successful third-party audit of a CSP's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, a CSP must subject itself to yearly third-party reviews.

For further information please go to the link below:

(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498).

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?

We recommend leveraging already established global standards for Information Security Management 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? The parameters essential and desirable and their respective benchmarks may be suggested.

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?

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.

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.

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.

Microsoft partners with governments around the world in development of cloud security frameworks, as well as a cloud provider. Based on our own experience, as well as building on the efforts of others, we have developed a series of best practices and principles that we believe would support governments as they develop and implement policies and programs to migrate their data and systems to cloud services. They also build on commitments that Microsoft puts at the heart of our trusted cloud: security of operation, data protection ad privacy, compliance with local requirements and transparency in how we do business. We encourage our government partners to consider those in developing a risk-based, agile cloud procurement environment.

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

Consider relying on contract law here. The right to terminate for breach or the right to terminate at will can both be leveraged here to protect the customer.

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

Microsoft believes that this is best addressed through a set of best practices and contractual arrangements rather than prescribed requirements.

This talks about how we migrate securely https://msdn.microsoft.com/en-us/library/mt403322.aspx

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

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, or Microsoft Office, 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?

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.

In addition, see answer to Question#5 above.

Question 15. W**hat polices, 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?**

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.

Microsoft believes that 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.

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?

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 Department of Electronics and Information Technology (Deity).

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?

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).

Microsoft has been at the forefront of safeguarding customer security and privacy and also at the same time cooperating with Law Enforcement Agencies. Microsoft has also been at the forefront of conducting an international dialogue through which Nation States can quickly share data relating to crime and terrorism.

Microsoft works with Government of India agencies like Cert-In and National Security Council Secretariat to share information pertaining to malware and botnets to fight cybercrime and to help keep Indian cyberspace and critical information infrastructure safe.

Microsoft had challenged the US Government's authority to force it to part with data of a customer which was lying in Ireland. Microsoft's contention was that the US Government ought to approach the Government of Ireland for this data and not Microsoft. Microsoft on 14.7.2016 won this case against the US Government. The Court has ruled that US Law Enforcement Agencies cannot force Microsoft to reveal data lying in another country.

There are undoubtedly some challenges in MLAT mechanism and the speed with which customer data is shared between countries. This is however a problem for Nation States to resolve and not for Microsoft or similarly placed companies. Microsoft on its part is at the forefront of a global dialogue to help Nation States evolve a quicker mechanism to do this. Microsoft is also helping evolve global norms of conduct in cyber space so that countries do not target each other's civilian infrastructure during cyber warfare.

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 centers in India.

(c) encouraging business and private organizations utilize cloud services

(d) to boost Digital India and Smart Cities incentive using 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?

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."[3]

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, like Microsoft, 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.

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

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.[4] 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 datacentres in India? What should be the protocol for information sharing between states and between state and central?

No Comments.

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 datacentres and cloud services platforms in India?

Refer to Question#18 above.

[4] Microsoft Azure and O365 enable their customers to choose where they data resides, https://azure.microsoft.com/en-us/support/trust-center/; https://products.office.com/en-us/business/office-365-trust-center-welcome.