BSA SUBMISSION - TRAI CONSULTATION PAPER ON CLOUD COMPUTING

July 25, 2016

Shri A. Robert J. Ravi,
Advisor (QoS)
Telecom Regulatory Authority of India
Mahanahgar Door Sanchar Bhawan
Jawahar Lal Nehru Marg (Old Minto Road)
New Delhi – 110012

Dear Sir,

Subject: Response to the TRAI Consultation Paper on Cloud Computing

This is with reference to the TRAI Consultation Paper on Cloud Computing issued on 10th June, 2016.

In this regard, please find enclosed the following:

1. Submission from BSA | The Software Alliance ("BSA") on the Consultation Paper [Annexure 1]
2. BSA's 2016 Global Cloud Computing Scorecard with the India country report [Annexure 2 and 3]

We hope our submission and our cloud computing report are useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion and stand ready to answer any questions you may have.

Thanking you,

Yours Sincerely,

____
Jared Ragland, Ph.D.
Senior Director, Policy
Asia Pacific

Annexure I

BSA's Submission to the Consultation Paper on Cloud Computing

Introduction

BSA | The Software Alliance ("BSA")[1] is thankful for the opportunity to offer comments on the Consultation Paper on Cloud Computing ("Consultation Paper") released on June 10, 2016.

As the leading advocate for the global software industry, BSA is greatly interested in contributing to initiatives that seek to advance cloud computing. We commend the efforts of the Telecom Regulatory Authority of India (TRAI) to conduct this Consultation.

The software industry is undergoing a dramatic transformation. BSA members increasingly provide a wide array of Internet-enabled services, such as cloud computing services, data analytics, security solutions, and much more. This is in addition to a full range of software solutions that are more often downloaded online or used on remote servers. These technologies collapse distance as never before, allowing companies to operate seamlessly in international markets — interacting with suppliers and serving customers wherever they may be. This is the new, digitally-enabled face of trade.

We believe that a policy environment that enables businesses, consumers and governments to leverage the full benefits of cloud computing is the key to driving the digital economy. We observe that the countries with the most favorable policies for cloud computing are those which prioritize free movement of data across borders, respect for international standards, protection of privacy and intellectual property, and robust enforcement and deterrence of cybercrime. We also find that many countries recognize that coordination of national cloud computing policies, both internally and with those of other nations, will facilitate benefits for all countries participating in the global economy.

Cloud computing remains in a relatively early stage of development. In some areas, limited government regulations are appropriate, for example to establish data privacy frameworks or provide for consumer protection. In such cases, it is important for the Government of India to keep such regulations in line with emerging international trends and best practices. For many of the issues raised in this Consultation Paper, an overly-regulated approach is likely to inhibit development, deployment and growth of cloud computing services, to the detriment of Indian businesses and other entities.

Despite cloud computing's early stage of growth, various standards bodies have, over the past decade, made significant efforts and progress in developing industry standards and best practices. Therefore, as the Government of India seeks to establish an enabling policy environment to promote cloud

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

computing, we urge TRAI and other relevant agencies to work together and, where possible, look to industry best practices rather than formal regulations.

Procurement is a related and extremely relevant aspect for the development of cloud computing. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing. Quick and flexible procurement processes that are not hampered by burdensome terms and conditions will allow users to fully leverage the vast array of benefits offered by cloud computing technologies.

As the Government of India develops and implements policies to foster the adoption of cloud computing, it is paramount that TRAI and other Indian government agencies take a coordinated approach and provide clear and predictable indications to the market on the policies to be adopted and the objectives such policies seek to achieve. As TRAI has done with this Consultation Paper, it is also critical that the Government of India continue to seek the input of interested and relevant private sector stakeholders to inform policy making in this area. This will allow investors to plan and execute long term strategies and investments in the Indian market and will help ensure that India is positioned to become a global leader in developing an effective, trusted, transparent and restrained regulatory environment, that works well with emerging international practices, and allows Indian businesses and consumers to fully benefit from existing and future opportunities presented by cloud computing and related services.

Indeed, the stakes are very high for India given the large and increasingly cloud dependent domestic information technology (IT) and business processing management (BPM) industries. According to the industry group NASSCOM, the Indian IT-BPM market in 2016 is over USD $143 billion, with exports exceeding USD $100 billion.[2] Any measures adopted that slow the growth of cloud computing globally and within India could put at risk the growth of this important industry in addition to the many other costs to the Indian economy.

BSA and its members have extensive experience working with governments and other stakeholders around the world on policies that promote cloud computing. We share these views hoping to assist TRAI in its efforts to map out the necessary policies that will help promote increased development, deployment and adoption of cloud computing in India.

BSA Global Cloud Computing Scorecard

BSA, and our research partner Galexia, have been conducting a survey of major cloud computing markets since our first Global Cloud Computing Scorecard was released in 2012.[3] We recently published our third and the most recent and updated study, the 2016 Global Cloud Computing Scorecard,[4] earlier this year in April. In these studies, BSA ranks the countries surveyed according to their cloud computing readiness.

[2] NASSCOM IT-BPM Snapshot at http://www.nasscom.in/indian-itbpo-industry.

[3] The 2012 and 2013 BSA Global Cloud Computing Scorecards and accompanying country reports can be found at http://cloudscorecard.bsa.org/2012/ and http://cloudscorecard.bsa.org/2013/ respectively.

[4] 2016 BSA Global Cloud Computing Scorecard and accompanying country reports at http://cloudscorecard.bsa.org/2016/.

Each country is graded on its strengths and weaknesses in seven key policy areas, encompassing the laws, regulations and IT infrastructure necessary for the support and growth of digital technology and cloud computing. These areas are: 1) data privacy; 2) security; 3) cybercrime; 4) intellectual property rights; 5) standards that enable data portability and international harmonization of rules; 6) promotion of free trade; and 7) IT readiness and broadband deployment.

India's relative ranking within this group of 24 countries has remained relatively stable over the last 5 years, coming in 19th (2012), 17th (2013), and 18th (2016) out of 24 countries surveyed even though India's absolute score has steadily climbed, from 50/100 (2012) to 53.1/100 (2013) to 56.1/100 (2016), indicating improvements in cloud computing readiness over time. That said, given that some other countries have progressed even faster, India risks falling farther behind in its global competitiveness. India can and must foster a conducive policy and regulatory regime for cloud services to flourish and avoid imposing onerous and burdensome obligations that can impede the adoption and provision of cloud computing.

For more information, the BSA 2016 Cloud Computing Scorecard and accompanying India Country Report are attached to this submission as Annexures II and III, respectively.

BSA's Response to Questions in the Consultation Paper

Because BSA is an industry association representing many of the leading global cloud computing service providers (CSPs), we have attempted to focus our responses on those questions amenable to industry wide input. We have chosen not to answer all of the questions in the consultation, especially where we felt questions were specific to individual company practices or experiences and not suitable to an industry wide response.

Financial & Operational Benefits

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.

A range of factors must be considered to conduct a cost-benefit analysis and evaluate various 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.

It also emphasizes how cloud computing offers greater efficiency, scalability, dynamism, reliability and availability that would yield better security, more innovation and lower barriers of entry for small- and medium-sized enterprises (SMEs).

Companies and government agencies should consider how cloud computing services can ***accelerate the design and roll out of services*** by enhancing IT system efficiencies and the savings of reduced on-premises IT costs. Such entities must adapt to variable cost procurement models that incorporate pay-per-use approaches that allow for faster and more tailored services, and move away from fixed capital expenditure procurement models. Cloud services, by their nature, can offer real-time scaling which will improve the agility and dexterity of enterprises and agencies to meet evolving consumer and constituent demands.

The advantages of cloud computing for ***promoting social networking, participative government, and e-commerce*** are both obvious and untapped. Start-ups, e-commerce companies, and government agencies can use the flexibility of cloud computing to quickly provide products and services to customers, to create mechanisms for real-time feedback from customers and constituents, and tailor IT needs to meet rapidly evolving demands and expectations.

Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) models allow enterprises and agencies to ***expand new services*** quickly by creating a rapidly adjustable development and deployment environment for new services.

Competitive Market for CSPs

By their very nature, cloud technologies operate across national boundaries. The cloud's ability to promote economic growth depends on a global market that transcends barriers to international trade and data transfers, such as preferences for particular products or providers and data or hardware localization requirements.

In order for the benefits of adopting cloud computing to emerge, the Government of 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.

The Government of India should not adopt policies that are intended to create advantages for Indian cloud providers operating in India to the detriment of foreign providers. Rules that protect providers that operate in India, shielding them from healthy international competition, will tend to freeze innovation, raise production costs, and make Indian CSPs less competitive in the global market that their cloud services can serve.

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?

Advantages of Cloud Computing

Cloud computing is a term that includes IT infrastructure, processing, storage, networks, operating systems, and applications that are available on demand in variable quantities. A cloud-based business model enables companies to have stronger budget control and greater agility in accessing the technology they need.

Service requests in the cloud environment are highly automated, allowing consumers to acquire, utilize and adjust services rapidly with little cost to the enterprise or agency. The end-user of cloud service is only billed for the services utilized, which allows more efficient use of limited resources, and to adapt to changes in expected IT usage.

The gap between expected and actual usage combined with large up front capital expenditures, can be a large burden, especially on smaller enterprises and agencies. Small companies may have difficulty raising the necessary capital to invest in technology. Moving from a CapEx to OpEx model removes such limitations by allowing smaller projects to be undertaken without incurring large sunk costs from unnecessary capital investments.

The move to the cloud and capitalization on its benefits across the board is hardly inevitable, and an urgent task lies ahead for governments. In order for societies to obtain the benefits of the cloud, policymakers must provide a legal and regulatory framework that will promote innovation, provide incentives to build the infrastructure to support it, and promote confidence that using the cloud will bring the anticipated benefits without sacrificing expectations of privacy, security, and safety.

We believe that there are significant economic benefits to be gained from a move to cloud computing accruing directly through reduced costs and indirectly by allowing for increased focus on core business functions. Many organizations still operate networks that are decades old. Gradually, these networks have been enhanced to support new services, but their basic architecture has not changed. These dated networks are costly, prone to failure and difficult to manage. As just one pertinent example, a large, dated on-premises IT system costs significantly more in electricity and maintenance as a function of capability than newer cloud-enabling data centers. Overall, cloud computing gives organizations the ability to add business value through renewed focus on core activities.

Cloud computing is also very beneficial when organizations need to deploy capacity to handle their peak demands. Since a CSP can reallocate resources across many enterprises with different peak periods, the CSP needs to deploy less total capacity to handle the same amount of business operations and services. Average unit costs are reduced by distributing fixed costs over more units of output. Larger cloud providers can therefore achieve significant economies of scale.

Among the biggest beneficiaries of cloud computing are SMEs. Cloud computing allows SMEs to leverage enterprise grade IT tools to which they would not otherwise have affordable access. Utilizing cloud computing, SMEs are able to scale IT use rapidly. Excessive regulation tends to disproportionately impact SMEs as costs, including for licensing, compliance, and related issues, go up and the cost-benefit ratio is undermined. India should, therefore, avoid over-regulation that could negatively impact the development of cloud computing.

In addition to the cost-benefits highlighted above, cloud computing services offer significant security benefits. CSPs can provide a level of protection for their customers' digital assets that exceeds what most individual companies are capable of providing on their own. This is particularly important for SMEs. The security benefits provided by the use of cloud services include but are not limited to: 1) increased physical security, as access to cloud servers is restricted to authorized personnel only, constantly monitored, and protected through technologies such as multifactor authentication; 2) regular security audits and assessments to detect and deter security incidents; and 3) data loss mitigation in the event of natural disaster or power outage though the use of backups located in various geographic locations.

Cloud Service Models

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?

There are many factors that enterprises and agencies should consider when selecting the type of cloud service deployment model. All enterprises should be concerned with the effectiveness and security of the service, and the trustworthiness of the provider. Smaller organizations are likely to be drawn to public cloud offerings because of ease of use and cost considerations. Larger organizations may look to CSPs that provide multi-tenant or public cloud deployments that meet larger organizations' regulatory needs and exceed their operational requirements and security considerations. Many CSPs are able to demonstrate security and privacy commitments sufficient to demonstrate their compliance with numerous regulatory regimes and other industry and government established assessment tools. CSPs can offer operational flexibility in IaaS and PaaS solutions, relatively low maintenance in SaaS solutions, and security at scale, including as a result of their visibility into malware and their ability to retain best-in-class security professionals.

A major advantage of adopting cloud solutions for enterprises and agencies of all sizes is that leading CSPs are often much more capable of providing high quality IT services, 24/7 support, and risk management solutions than in-house IT resources. This is especially true for SMEs that have limited expertise with the ability to effectively manage IT costs, security and regulatory compliance.

Cloud Security in relation to Data Migration

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?

CSPs 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. In addition, for some SaaS services where no data resides with the cloud service provider, migration is as easy as rerouting traffic from one gateway to another.

Rather than attempting to "prescribe a secure migration path", governments should encourage the adoption of voluntary, transparently developed, industry-led international standards, while also working to minimize conflicting legal obligations on CSPs.

The specific mechanisms for transferring data from legacy systems to CSPs and from one CSP to another will depend heavily on the specifics of each organization and their existing data structures. BSA members offering cloud computing services have developed a variety of solutions that can be tailored to their customer for secure transfer of data from one system to another. In some cases, this may be rather straightforward. In others, it may be more difficult, such as when the data is tightly associated with particular applications and is not easily convertible to alternative systems.

As CSPs continue to evolve, it is likely additional voluntary international standards will emerge, and governments should support industry-led efforts to promote data portability. However, a prescriptive regulatory approach to address cloud migration is likely to be counter-productive and would likely limit the services available in the market place without improving data migration capabilities.

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?

As cloud computing solutions evolve and mature, industry standards are developing for security, interoperability, and data portability. Because the ease or difficulty of migrating data from on-premises systems to CSPs, or one CSP to another, varies greatly depending on the kinds of data and data uses involved, it is critical that governments avoid prescriptive, one-size-fits-all requirements.

Governments should remain technology neutral and avoid imposing any limitations on, or preferences for, particular business models and licensing models. Open source and proprietary technologies are increasingly integrated into the same services and software solutions and each model has its respective advantages and disadvantages. The Government of India should establish policies that ensure that business, government agencies and consumers have the freedom of choice to determine and select which combinations of products and services will provide the best value for money given the particular enterprise needs. The role of government should be to encourage the use and adoption of standards that are global, voluntary, and developed through industry-led multi-stakeholder processes which reduce costs, promote innovation, and facilitate interoperability through open and transparent processes.

Internationally, much work has been done in various industry bodies to set standards or processes for promoting interoperability. Since cloud computing, by its nature, works across international borders to achieve economies of scale, enhanced reliability and security, the best way to ensure interoperability is, therefore, to adhere to the work already done by following industry best practices and, where they have been widely adopted, international standards.

BSA members adopt and comply with a variety of standards, and governments 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. Finally, the government should rely on voluntary, consensus based, industry driven standards instead of setting technical requirements themselves.

We recommend the Government of India: (1) support IT industry organizations developing international standards that will ensure optimal portability and interoperability; (2) accept and utilize widely adopted international standards and certifications; and (3) refrain from requiring use of local standards and certifications.

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

As stated before, we urge against a prescriptive regulatory approach for data portability. The provisions necessary will vary and depend on the kinds of data and enterprises involved. Some BSA members have established protocols, including strong encryption of data in transit, to ensure secure data transfers and to minimize security risks. Some of our members also offer ready solutions for data exportation into various standard data formats for users that wish to migrate their data to alternative IT systems or CSPs. The details will be determined by the nature of the service provided, the needs of the end-user, the kinds of data involved and their various uses, as well as many other factors. The specific terms of data exportation should be clearly laid out in the contract between the end-user and the CSP and not through regulation.

Rather than attempting to regulate in this area, or impose prescriptive rules, we urge governments to support emerging international standards to promote security, interoperability and data portability, and to avoid imposing additional country-specific certification requirements that only raise costs for the CSPs and end-users without improving data portability.

Data Ownership

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?

Contractual provisions are the appropriate mechanism for regulating the rights and obligations of end-users and CSPs in the cloud environment. Governments should avoid establishing specific requirements for how consumers control their data, as they are likely to inhibit growth and innovation in cloud computing services and limit consumers' choices of available CSPs. Instead, governments should promote policies that advance the goal of transparency so purchasers of cloud-based services can make informed decisions.

Data protection and privacy laws and regulations are designed to provide protection of personal data. The Government of India should seek to align data protection regimes with internationally accepted models so that they will ensure continued international data transfers, which are the lifeblood of cloud computing services.

Cloud Security

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.

BSA member companies have a deep and long-standing commitment to protecting consumers' data across technologies and business models. Consumers will only take advantage of the benefits of new technologies, such as cloud computing services, if they trust that the data they entrust to a CSP will be secure, protected and not used in unexpected ways. BSA member companies offering cloud services provide enhanced solutions both by adopting, developing and implementing advanced security solutions, and in some cases providing Security-as-a-Service solutions, directly to both end-users and to other CSPs.

It is critical that CSPs are able to adopt and implement cutting-edge cybersecurity solutions that can be adapted and tailored to the different needs of different users and use cases. Governments should avoid imposing any requirements to use particular technologies or services. Instead, national cybersecurity frameworks should be risk-based and prioritized, technology neutral, practicable, flexible and respective of privacy and civil liberties.[5]

When considering the security implications of cloud computing, it is important for the Government of India not to make inaccurate assumptions about the security of cloud services versus traditional, or "on-premises" IT systems. An on-premises system that is networked and connected to the Internet can be at as much risk or more 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 in-house IT

[5] Asia-Pacific Cybersecurity Dashboard at http://cybersecurity.bsa.org/2015/apac/

departments. This is especially true for small organizations and agencies, and SMEs. The alternative of keeping data and processes offline can exacerbate availability and reliability concerns and undermines the real and potential benefits of effectively utilizing IT systems in business operations.

There are a variety of steps that many CSPs take to enhance the security of their systems. These often begin with physical security. Facilities are secured and monitored and access of personnel is controlled. Data can be secured in a variety of ways, including with strong encryption, both at rest and in transit. At the operational level, CSPs may choose to comply with a variety of security-related standards and certifications. Many will submit to third party audits or other validation measures to assure private- and public-sector customers that the security measures in place are effective. Leading global standards related to information security demonstrate a provider's security commitments across the relevant domains. Governments can achieve high security outcomes by either using those standards or mapping their own security requirements to their controls, minimizing the differences or novel requirements as much as possible to ensure efficiency and reduce costs.

Like with interoperability and portability, governments should promote the development and adoption of voluntary, transparently developed, industry-led international standards, and recognize certifications from internationally accredited entities. Unfortunately, the Government of India imposes local security testing requirements in addition to international testing requirements. These requirements increase costs, which can lead to reduced security as end-users may have less access to cutting-edge security solutions available on the global market.

The perpetrators of cyber-attacks are constantly adjusting their methods, targets and technologies. The imposition of highly prescriptive security rules must be avoided as they fail to recognize new and evolving methods and technologies which could, in turn, limit the ability of CSPs and others to anticipate and respond to emerging threats.

Encryption Policy

India lacks a uniform, consistent and effective encryption policy. Most other countries allow the use of strong encryption standards ranging from 128-bit to 256-bit to ensure the security of sensitive information exchanged via the Internet and other networks. In India, however, only 40-bit encryption can be used without additional regulatory approval according to the Department of Telecommunications' Guidelines for the Grant of License for Operating Internet Service (ISP Guidelines).

Encryption standards differ greatly from one regulatory agency to another in India, each having their own specific standards. In September 2015, the Government of India published a Draft National Encryption Policy that was withdrawn shortly after publication. The draft raised a number of concerns including restrictions on the use of commercially available encryption (by restricting key lengths for example) and mandates to disclose proprietary information.

We urge the Government of India to fully consult with relevant stakeholders before developing or implementing a National Encryption Policy. The Government of India should adopt a clear policy permitting the use of strong-encryption. The Government of India should also avoid any efforts to require technical access solutions (e.g. backdoors) or encryption-key escrow systems, for any such efforts will only weaken vital data security for all. As we report in a recent publication on encryption,[6] "Cryptographers warn that it is impossible to weaken encryption without strengthening the hands of hackers and foreign adversaries."[7]

Obligations on CSPs

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

In a cloud environment, responsibilities are often shared between the customer and the cloud service provider (CSP) depending on the business model.

The responsibilities for managing risks will vary depending on the cloud delivery model. For example, end-users have less control over risks in SaaS models compared to IaaS models. 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. Given the variety of cloud models and CSP/end-user arrangements, it is neither reasonable nor realistic for the government to effectively mandate outcomes across these various models. Instead, the roles and responsibilities of CSPs and their customers/end-users should be decided between the parties in their agreements.

Cross-Border Data Flows

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?

The ability to transfer data internationally is the lifeblood of cloud computing and the modern digital economy. The success of cloud computing depends on users' trust that their information will be properly protected. At the same time, to maximize the benefits of the cloud, including the resilience that results from dynamic geographical redundancy, CSPs benefit from being able to move data through the cloud in the most efficient way. Cross-border data flows enable international commerce and are also critical for:

<u>Systems Integrity</u>: Global cloud and other Internet-enabled service providers invest in state of the art security and reliability. Limiting cross-border data transfers will reduce the ability of cloud customers from utilizing CPS with the strongest security and reliability features.

<u>Redundancy and Reliability</u>: Cloud and other Internet-enabled service providers often store data in geographically dispersed locations, making it harder for hackers to gain access and ensuring that if natural disasters or other unforeseeable forces damage or disable one data center, customer data is not lost and end-user services are not disrupted.

<u>Efficiency – Data Transmission</u>: Internet-enabled data transfer relies on the efficient transfer of data from one point to another to maximize transmission speed. The nature of the Internet is such that

[6] Encryption: Securing Our Data, Securing Our Lives, found at http://encryption.bsa.org/
[7] http://encryption.bsa.org/downloads/BSA_encryption_primer.pdf - page 10.

often the fastest and most efficient route for data transfer from one location to another is not a straight line but through geographically dispersed connection points and servers.

Efficiency – Data Processing: The cost of processing data often depends on the operational demands on particular servers and data centers. The ability to transfer data to underused equipment, for example during off-peak hours, minimizes the costs of processing.

BSA members invest significant efforts to ensure that their customers' sensitive information is used appropriately and fully protected wherever it is transferred, stored or processed.

As the policies to promote the adoption of cloud computing are further developed, the Government of India should ensure that data protection and cybersecurity frameworks are in place while: 1) avoiding all unnecessary restrictions on cross-border data flows; and 2) recognizing the need for service providers to determine where infrastructure is located to maximize efficiencies of scale and economy and to ensure the most secure and reliable services.

Members of BSA have a deep and long-standing commitment to protecting consumers' data across technologies and business models as they recognize that consumers are only comfortable taking advantage of the benefits of new technologies, including cloud computing, if they trust that their information is protected.

The adoption of an accountability model, as established by the OECD, which requires organizations that collect data to be responsible for its protection no matter where or by whom it is processed would appropriately protect users. This approach requires organizations transferring data to take appropriate steps to ensure that any obligations – in law, guidance or commitments made in privacy policies – will be met.

In sum, governments should avoid all unnecessary mandates regarding the location of data storage and the restriction of international data transfers, as these policies reduce the efficiency and efficacy of cloud services and unnecessarily limit consumer choice.

Lawful Interception

Question 15. What 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?

Governments should leverage existing mutual legal assistance treaty (MLAT) arrangements and coordination via INTERPOL to address lawful interception requirements beyond national boundaries. To enhance lawful access to information, the Government of India should enter into MLATs with more international partners. For countries with which India has already signed an MLAT, it should focus on resolving interpretational differences and enhancing the efficiency of the processes in both directions.

Access requests should only be valid when backed by proper legal authorization. Any obligation imposed on a CSP 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 decryption of the requested data. Encryption used by corporate enterprises intended to create a secure private network for corporate communications and should not be subject to requests for access to unencrypted data.

Licensing & Registration

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.

As mentioned above, cloud computing remains in a relatively early stage of development. What is described as cloud computing today is likely only a small subset of the cloud computing services that will be available in the future. It would be very counterproductive to attempt to define the scope of cloud computing in law, as this could chill innovation and set unnecessary boundaries on the evolution of cloud services.

Therefore, BSA opposes efforts to impose any sort of licensing framework on cloud service providers (CSPs), now or in the future. Cloud services are provided over telecom infrastructure which is already licensed and regulated. Therefore, there is no need for any additional licensing or regulatory oversight by TRAI on cloud services per se.

Any additional compliance requirement like licensing or registration would go against the Administration's spirit of liberalization and "ease of doing business" objectives.

Jurisdictional Issues

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?

This question suggests that TRAI may be considering a separate or additional protocol for CSPs with respect to lawful access. On the contrary, the same framework that applies to existing Internet services should apply to CSPs. The issue of territorial jurisdiction does not differ between cloud data and other forms of digitized information available on the Internet.

Furthermore, CSPs do not necessarily "own" the data. Nor are they necessarily authorized to access the data, or monitor it. CSPs cannot police the content and conduct of users on self-service platforms and should not be held responsible for the content of the information stored on processed on their services.

As discussed above, access requests should only be valid when backed by proper legal authorization.

Government Cloud

Question 18. What are the steps that can be taken by the government for:
a. promoting cloud computing in e-governance projects.

India should consider implementing the Meghraj "Cloud First Policy" more broadly. India should develop a document which sets out general guiding principles for a "cloud first" approach for government ministries and agencies to consider in adopting cloud computing solutions as a primary part of their information technology planning and procurement. All government-led, government-controlled programmes should be mandated to go “cloud first”.

Another way to increase public sector adoption of cloud is for a central government agency to develop shared services for public sector customers, making specific services available to all government agencies. These could also be extended to the private sector such as SMEs to increase their adoption of cloud services.

b. promoting establishment of data centres in India.

The Government of India should establish incentives for investing in data centers in India, but should avoid mandates. Many CSPs that do choose to invest in data centers in India are likely to be interested in serving the regional market place. If countries adopt requirements for locate servers in their markets in order to offer services, such as cloud computing services, this will fundamentally interfere with the economies of scale and rational distribution of infrastructure that underpins the potential of these services to drive productivity and economic growth. There may be a variety of incentive schemes that the Government of India might consider, but a key factor will be to ensure that the basic infrastructure (reliability of power, transportation, internal and international bandwidth) is competitive with other global markets.

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?

There is no necessity for a dedicated cloud for government applications, unless there is a very clear reason for it. In fact, a dedicated cloud for government applications negates a number of cost-benefits of cloud computing’s shared resource model where the cloud service provider owns and maintains the network connected hardware required for their cloud services.

A dedicated cloud need not be considered, unless (1) there are specific security requirements which an outsourced cloud vendor is unable to fulfill, or (2) there are technical requirements which an outsourced cloud provider is unable to fulfill.

A separate government cloud does not increase security, either in a single-tenant or multi-tenant environment. Instead, government agencies should decide what kind of architecture they need in order to meet their needs and achieve their objectives.

Data Centre Infrastructure

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?

According to the 2016 BSA Global Cloud Computing Scorecard, India is struggling with IT readiness and broadband deployment compared to other countries. Much of this relates to demographic and other factors beyond IT policies. That said, it is clear that India should aggressively adopt policies that will provide incentives for private sector investment in broadband deployment and that will promote universal access to broadband connectivity.

Without the basic infrastructure in place, it will remain difficult to distribute the benefits of enhanced cloud computing to the economy as a whole. For example, while progress has been made in the electricity and sustainable power development in India, challenges in this area still remain due to the lack of a cross-country electrical grid.