



---

## IAMAI Submission on Cloud Computing

---

July, 2016

## CONTENTS

<b>Proposals for Regulation of Cloud</b> .....	<b>Error! Bookmark not defined.</b>
<b>I. Introduction</b> .....	<b>3</b>
<b>II. A critique on Key Policy Issues and Suggestions</b> .....	<b>3</b>
<b>IV. Answer to TRAI Questions</b> .....	<b>6</b>
<b>Annexure</b> .....	<b>13</b>
<b>Laws and Regulations around the world</b> .....	<b>13</b>

IAMAI

## **I. INTRODUCTION**

TRAI's consultation paper on 'Cloud Computing' is a comprehensive paper that seeks to address issues viz., growth of cloud services in India, interoperability of data among various cloud platforms, quality of service, security of data on the cloud, government initiatives to promote implementation of cloud services and most importantly the legal and regulatory framework for cloud services in India. The paper also illustrates the concerns that have been identified with cloud computing services worldwide.

The Internet & Mobile Association of India welcomes this 'CP' on Cloud computing which acknowledges the relevance of Cloud as the most adopted business decision in the field of technology in India. However, some of the matters that have been discussed in the paper under the technical and security conditions will pose several challenges to the Cloud Computing ecosystem in India. An approach such as this, if adopted, will affect GOI's Digital India, Make in India, Smart Cities Initiative and also hamper ease of doing business in India.

Parameters covered in the paper include areas of regulation which are contrary to the paper's objective of providing stable growth to the Cloud Industry.

## **II. A CRITIQUE ON KEY POLICY ISSUES AND SUGGESTIONS**

*This section highlights some of the key policy and regulatory issues that India faces in Cloud Computing and Answers to the Questions sought by TRAI have been provided.*

### **A. Licensing Regime will be Deterrent to the Growth of Cloud Services in India**

The paper suggests a licensing regime for cloud computing services. This tantamounts to over-regulation and will throttle the growth of Cloud Services in India. The legislative intent is to cover services that provide a network used for communications and transmitting data. Cloud services themselves do not create a network that facilitates communication and transmission of data but rather only provide services for remotely storing and processing data. In fact, cloud services themselves use services that fall under the definition of "telegraph" or "telecommunication service" to perform their function. In this respect, cloud services are no different from any OSP that harnesses the existing telecommunication networks to connect to their users. In light of this, since cloud services do not fall under the definition of either "telegraph" or "telecommunication service", Creating another set of regulations with authority to a different body will only lead to multiplicity of jurisdictions, regulations and eventually conflicts and contradictions.

The public cloud services market is at a very nascent stage in India at present at \$1.2 Billion. It is projected to reach \$4 Billion by 2020.<sup>1</sup> Digital India project provides potential opportunities for cloud adoption at a \$19 billion

---

<sup>1</sup> <http://www.gartner.com/newsroom/id/3308117>

between 2014-2018.<sup>2</sup> This growth will be throttled if there are regulations around licensing regime that will impede the establishment of cloud services in *India*

Cloud services are same as any other internet service which is rendered through a platform provided by the telecom infrastructure and Internet service providers, who are already regulated. Hence any additional licensing requirements would be counter productive and may well keep CSPs away from India

- **IAMAI Suggestion:** Licensing of cloud service providers (CSPs) will severely impede the growth of the cloud ecosystem. Existing regulations such as the Information Technology Act already apply to cloud service providers. Any licensing regime will discourage global companies to set up datacenters in India. Instead, the government should focus on creating policies and infrastructure that will attract CSPs to establish data centers in India. The association recommends that, in general, cloud platforms must be left to free market mechanism. The government may regulate the Government Cloud platforms in providing e-governance and in storing critical government data and citizen data such as the Aadhaar Database.

## B. Rules on Security over Cloud Already Exist:

Security over cloud is not unique to Cloud Services but any form of digital data over internet whether it is data at rest, data in use or data in transit.

There is no need bring laws to govern the Cloud service providers as various laws like Information Technology Act and Companies Act 1956 are applicable to Cloud service providers and also the customers of the Cloud service which require various disclosures, filing and record keeping obligations to be fulfilled. In addition, different sectoral regulators such as the RBI have implemented frameworks which regulate the use of cloud by banks and other regulated entities (for e.g. RBI Circular on Sharing of IT resources by banks). Similar frameworks exist under SEBI and IRDA for the securities and insurance markets. Therefore, the sector is adequately regulated.

All CSPs are governed by the norms prescribed by the DOT/TEC/DEITY and all data which enters and leaves India is within the oversight of the existing surveillance and blocking regulations [IT Act]. IT (Amendment) Act 2008 has specified “reasonable security practices and procedures” to protect “sensitive personal data or information” (SPDI). It is mandatory to identify the SPDI processed or stored by the CSP and ensure all the processes are compliant with IT (Amendment) Act 2008. . TRAI had acknowledged this factor for the MVAS industry and exempted MVAS services from licensing

**IAMAI Suggestion:** Many nations have adopted robust cyber security and data protection laws to hold a significant stand in the cloud readiness index. [Please refer to the annexure]. It should be noted that any unreasonable interference creates legal uncertainties and commercial risks for businesses operating in India. This has a direct impact on the attractiveness of India as an investment destination for locating servers in the country.

Any form of over regulation, unsystematic approach, heavy handed bureaucracy, will be deterrent to the growth of Cloud services in India. The regulators must revisit the high and practical standards set by most policies around the world and stress upon international cooperation on these areas.

---

<sup>2</sup> IAMAI Report on Encryption

### C. Promoting Free Flow of Data is Imperative

India needs to improve its cloud readiness and encourage trans-border data flow [TBDF] to reap the economic and strategic benefits. Removing barriers to TBDF and driving domestic data flows would be the key to encouraging public/private enterprise as well as providing economies of scale and penetration to the NeGP for citizen-centric services in India.

Geographic restrictions on data and other limits on the outsourcing of work or data lead to overly restrictive legal restrictions that require data to be stored within the country or place limit on the trans-boundary transfer of data create an overly restrictive legal environment that is not conducive to generating economic activity within a country[data center]

Ensuring the harmonization of international rules is essential for the smooth flow of data around the world and between different cloud providers to promote openness. National privacy regimes should avoid unnecessarily burdensome restrictions on cloud service providers such as registration requirements for data controllers & processors and cross-border data transfers such as the case with EU and some other countries<sup>3</sup>.

**IAMAI Suggestion:** The association strongly opposes **mandatory data or server localization** which would reduce competitiveness and would have a deterring impact on the GDP of the economy and drive away India's extensive ability to attract data centre investments. The government should only impose such restrictions for critical government data or government cloud.

Negative impact of mandating Data or server localisation:

- IAMAI report 'Make In India- Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure'-suggests that mandatory localization would reduce competitiveness and would have a deterring impact on the GDP of the economy. It would contract the national GDP by 0.1% to 0.8% and negatively impact the investment climate, bringing down net investment into the country by nearly 2%. This would also reduce the monthly income of the average Indian worker by 11%.<sup>4</sup>
- It will create virtual borders within the internet by creating restrictions to the movement of data across borders.
- Localization requirements would prevent Indian businesses from competing globally, by restricting the flow of information that is necessary for global commerce and innovation
- Security agencies can, with the use of malicious software, access data stored anywhere in the world, so localization requirements would not avoid data interception.
- Mandatory data localization requirements substantially increase costs for companies, which might be imposed on consumers. Higher cost barriers might also discourage SMEs to innovate and operate in those countries.

---

<sup>3</sup> <http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf>- Global Data Privacy Directory 2014

<sup>4</sup> Make in India –Data Center Incentivisation Report 2016

- Regulatory restrictions requiring localization of data will disrupt the economies of scale which cloud provides. Such restrictions will negatively impact the competitiveness of the companies especially the SMEs and startups who are increasingly relying on cloud services to reduce their IT costs.
- Very importantly, if similar policies are adopted by other countries it will severely impact the Indian IT-ITeS companies that heavily rely on offshoring of data from around the world to India. As a matter of fact, India as part of the India-EU Free Trade Agreement (FTA) negotiations has demanded that the EU relaxes the restrictions on movement of personal data of European citizens to India. The policy direction requiring data localization (if taken) will be contrary to the position taken by India in these negotiations.
- The argument that data security is better ensured through data localization is a fallacy. Security is independent of geographical location of data, but rather depends on the security practices followed by the CSPs.

### III. Conclusion

India needs government initiatives to drive cloud adoption, business friendly policy framework, and a good international collaboration strategy to govern cyberspace. The cloud policy needs to take into cognizance that there is enough competition in cloud market to address issues such as security and interoperability. Regulation of cloud services is highly undesirable. Instead, the government should focus on creating policies and infrastructure that will attract CSPs to establish data centers in India.

### IV. ANSWER TO TRAI QUESTIONS

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

**IAMAI response:**

**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.
- 

**b. Promotion of social networking, participative governance and e-commerce:**

- Cloud technologies help in easy deployment of various collaboration tools and are available to users quickly.
- Start ups and e-commerce companies can leverage cloud to develop and deploy the applications
- cloud model enables them to scale up or down the infrastructure as needed.

**c. Expansion of new services:**

- With deployment of PaaS cloud model it is easy to develop new services and deploy them in the cloud environment, thereby enhancing business agility.
- PaaS augmented with IaaS can provide both development and deployment environment that can be leveraged to develop new applications
-

**d. Any other items or technologies. Please support your views with relevant data.**

**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?**

**IAMAI response:**

Moving from traditional IT Infrastructure to cloud computing is due to the economics of Cloud Computing also known as cloudonomics. The main reasons how the cloud computing will help cost reduction in the IT budget of an organisation are:

- By lowering the opportunity cost of running technology
- By allowing for a shift from capital expenditure to operating expenditure
- By lowering the total cost of ownership of technology
- By enhancing organisation's ability to focus on core activities

**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?**

**IAMAI response:**

There are various types of Cloud Deployment models viz., Public, Private, Hybrid and Community Cloud. The businesses will choose the model best suited to their needs for deploying as per their business and size..

**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?**

**IAMAI response:**

Such migration would be governed by the contractual arrangements between CSP and customer. There are industry standards and technology solutions available in the market to enable secure migration.

**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?**

**IAMAI response:**

There is no need for any regulatory provisions as contractual arrangements will take care of this requirement. Competition, industry standards and technology advancements will drive the cloud ecosystem to address the data portability issues.

**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?**

**IAMAI response:**

Various Standards Development Organizations (SDOs) globally are working on defining standards to address the issue of interoperability in the cloud - e.g. ISO/IEC 19941 standard on 'cloud computing - interoperability and portability'. The market forces should be allowed to address this problem, instead of bringing regulations in place especially given that the cloud industry is still at a nascent stage. These issues can be addressed as part of the contractual arrangement between CSP and customer and do not necessitate regulatory intervention.

**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.**

**IAMAI response:**

The relationship between a CSP and its consumer, quality of services, interoperability standards between CSPs should be left to the industry and free market mechanisms.

**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?**

**IAMAI response:**

This is a B2B issue and should be left to the industry and free market mechanisms.

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

**IAMAI response:**

Complaint and grievance redressal would be addressed as part of the contractual arrangements and does not require any regulatory intervention.

**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.**

**IAMAI response:**



- Security concerns over cloud can be best addressed through voluntary adoption of cyber security standards and best practices by CSPs and customers. The cyber threat landscape is ever evolving and regulatory prescriptions will only drive companies towards compliance instead of addressing such evolving threats.
- Competition and brand reputation are significant drivers for CSPs to invest in security. In many cases, the CSPs are able to deploy stronger security measures than their customers (esp. SMEs & startups).
- Regulations must not restrict CSPs to deploy state-of-the-art technologies (e.g. limits on encryption), else there is a risk of weakening security

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

**IAMAI response:**

As iterated earlier, this gets addressed through contractual arrangements. Standards are constantly evolving to address such issues.

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

**IAMAI response:**

This gets addressed through contractual arrangements

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

**IAMAI response:**

Cloud standards which define the roles of responsibilities of CSPs and users already exist. In addition to such standards, terms and conditions already laid down in various existing laws like Information Technology Act, Companies Act 1956, and Copy Right Act will be applicable to Cloud service providers and also the customers of the Cloud service. There are also various laws which require various disclosures, filing and record keeping obligations to be fulfilled. The Reserve Bank of India has also issued guidelines for banks to follow a code of conduct where banks outsource their financial services to a third party.<sup>5</sup>

**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?**

---

<sup>5</sup> . <http://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.pdf>

**IAMAI response:**

There is no need to define new disclosure guidelines. Contractual arrangements and existing laws of the land are sufficient for governing any such scenario.

**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?**

**IAMAI response:**

The arrangements between a CSP and customer would incorporate the respective responsibilities to comply with the applicable legal and regulatory requirements. In such scenarios, there is no need to bring in new regulations to govern CSPs separately. It is also important to recognize the existing mechanisms for international co-operation between countries for enforcement of domestic laws, such as Mutual Legal Assistance Treaties (MLATs) and for governments to keep discussing opportunities to improve these processes and enhance mutual cooperation.

**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.**

**IAMAI response:**

The association suggests that the private and Public Cloud platforms must not be brought under any licensing regime and must be left to free market mechanism. The government may regulate the Government Cloud platforms in providing e-governance and in storing critical government data and citizen data such as the Aadhaar Database.

**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?**

**IAMAI response:**

It is important to recognize well-established principles and mechanisms of international law govern international co-operation between countries for enforcement of domestic laws, such as Mutual Legal Assistance Treaties (MLATs) and for concerned agencies to keep discussing opportunities to improve these processes and enhance mutual cooperation.

**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.**

**IAMAI response:**

Promoting establishment of data centres in India is about developing a regulatory regime that incentivizes private companies to make these investments. If the regime is not reformed, then India will forgo a valuable growth opportunity. The data centre industry's needs are unique from other, more general industrial policies currently in place. So, a conducive regulatory and policy ecosystem that comprehensively addresses such needs with transparency, certainty and assurances is necessary. At present, an investor in the data centre market will not be in a position to invest with certainty or to avail of governmental incentives or schemes as the applicability requirements are subject to bureaucratic and regulatory approval.

The policy requirements for India should begin with developing a comprehensive and systemic framework for data centres. The motivation should be to create an enabling environment for private players to enter the data centre market and to meet the growing needs of data management in India. Most importantly, it should be kept in mind that the data centre market is capital and technology-intensive, which will result in technology and capital from capable players entering into the market. Positive impact on the Indian economy is highly likely as a result.

**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?**

**IAMAI response:**

Meghraj policy for government adoption of cloud already addressed these aspects. Critical govt data, citizen information/services etc. Private/public cloud may be left free to develop on its own without stringent regulations.

**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?**

**IAMAI response:**

India at present does not have sufficient infrastructure to support data center infrastructure in India as per IAMAI Report on Data Center 2016<sup>6</sup>. Due to complicated regulatory mechanisms and bureaucracy, India stands at 179 out of 189 countries in starting a business. Additional challenges are related to data centers requiring huge space capacity as well as power and cooling provisions.

---

<sup>6</sup> Make in India: Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure in India May 2016

Cost is one of the primary challenges to data centre development in India, and energy makes up the lions share of that cost. Energy costs consist 75% of the costs of operating a data centre, hence, power requirements for the sector continue to rise. It is also burdensome for a business to apply and get electricity connection. On average it takes 67 days on an average and go through seven different procedures, as against 3 in Japan. The green data centers need to be brought in place.

Beyond energy needs, data centres require an enormous volume of water to cool high-density server farms, which is making water management a growing priority for data center operators. A 159 megawatt data center can use up to 360,000 gallons of water a day and as the scale increases data center operators have to depend heavily on water supply.

**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?**

**IAMAI response:**

Data centres incur one-time and recurring taxes that have a significant impact on long-term costs for any data centre. The capital-intensive nature of a data centre triggers relatively high sales taxes and property taxes. Further, electricity tariff, stamp duty charges, import duties on equipment sourced from outside India and multi-jurisdiction tax implications further impact data centre costing.

It is suggested that India adopt data centre-specific tax and duty incentives that will encourage investors to operate here. Where to locate the assets and the people associated with delivering global data content and services is a defining tax consideration — in terms of both direct corporate tax rates and indirect sales taxes. Friendly tax jurisdictions play a big factor in choosing a place for establishing a data centre and complex tax jurisdictions do just the opposite.

## ANNEXURE

### LAWS AND REGULATIONS AROUND THE WORLD

Many small countries have quickly advanced by incorporating appropriate legal and regulatory changes required to take the full advantage of the digital economy. Developed nations like US, Japan and EU countries have adopted various strategies by analysing the overall policy, regulatory and technology landscapes in their countries. Several countries in Europe have had a wide consultation with stakeholders to identify ways to maximise the potential of the cloud with minimum reugaltion. Their specific cloud policy represents a political commitment of the government in implementing these strategies for faster proliferation of cloud.

- ◇ **Singapore:** Adopted a new privacy law that balances user protections and continued innovation<sup>7</sup>
- ◇ **Malaysia:** Made the biggest gains due to a range of changes in cybercrime, intellectual property laws and improvements in efforts to improve digital trade. Malaysia crossed the mark to come under the more developed economies under the “cloud readiness “Index<sup>8</sup>.
- ◇ **Central and South American countries:** Peru, Uruguay, Costa Rica and Mexico have inculcated data privacy laws in the past few years to further open trade businesses or cross border data flows.
- ◇ **Canada and Russia:** Made a range of improvements to their Intellectual property protections in line with key international agreements.
- ◇ **European Union:** The EU is in the process of revisiting its privacy rules and implementing changes to it’s data protection rules with an aim to facilitate the free flow of personal data and reduce administrative burden for companies.
- ◇ **United States:** The US government has consciously and systematically improved and clarified its approach to surveillance in the last few years, offering increased and better oversight to US and non-US citizens. Examples of this include the outlawing of domestic telephone data collection, the implementation of the Presidential Policy Directive 28, the Judicial Redress Act and recommendations by the Privacy and Civil Liberties Board.
- ◇ **Australia:** Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came in to force on 12 March 2014. The amendments have significantly strengthened the powers in investigations (including own motion investigations). And for the first time, the country introduced fines for a serious breach or repeated breaches of the privacy principles.
- ◇ **Australia, Canada, Japan and Korea:** Have comprehensive privacy regimes without any onerous registration requirements for cross border trade. The Personal Information Protection Act (PIPA) of Korea, which came into force on 30 September 2011, is one of the strictest data protection regimes in the world.
- ◇ **Mexico:** The Mexican economy is one of the most open economies in the world which has signed the highest number of double taxation agreements (27) necessary for e-commerce growth.

The Asia Cloud Computing Association (ACCA), on the mission to accelerate the growth and development of cloud computing in Asia Pacific, in 2010 placed India in the second bottom out of 14 nations in its latest Cloud Readiness Index<sup>9</sup>.

---

<sup>7</sup> <https://www.pdpc.gov.sg/legislation-and-guidelines>

<sup>8</sup> [http://www.asiacloudcomputing.org/images/research/ACCA\\_CRI2014\\_ExecSummary.pdf](http://www.asiacloudcomputing.org/images/research/ACCA_CRI2014_ExecSummary.pdf)

<sup>9</sup> [http://www.asiacloudcomputing.org/images/research/ACCA\\_CRI2014\\_ExecSummary.pdf](http://www.asiacloudcomputing.org/images/research/ACCA_CRI2014_ExecSummary.pdf)