Telecom Regulatory Authority of India

Recommendations
On
Cloud Services

16th August, 2017

Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan
JawaharLal Nehru Marg
New Delhi – 110002

Table of Contents

Chapter-1 Introduction

1.1 The growth of "cloud computing" (CC) services in the last decade has transformed the way governments, enterprises, and consumers store and process their data and manage their resources. The term CC is commonly used to describe a range of delivery models that offer users an elastic pool of shareable computing resources. As per the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the following are the key characteristics of cloud computing:[1]

- **Broad network access:** This offers an increased level of convenience in that users can access physical and virtual resources from any location and using any device that offers access to the network;
- **Measured service:** Usage can be monitored, controlled, reported, and billed allowing users to pay only for the resources that they use.
- **Multi-tenancy:** Physical or virtual resources are allocated in a way that multiple tenants and their computations and data are isolated from and inaccessible to one another.
- **Rapid elasticity and on-demand self-service:** Resources can be rapidly and elastically adjusted as per requirements. Moreover, such computing capabilities can be provisioned automatically or with minimal interaction with the cloud service provider (CSP).
- **Resource pooling:** The provider's resources can be aggregated in order to serve one or more cloud service customers.

1.2 The delivery of cloud services may involve a range of providers and intermediaries starting from the owner and controller of the cloud facility; intermediaries that connect such persons with cloud users; and aggregators that package and integrate several cloud services into a composite offering for cloud users. In each case it is important to understand the inter-relationship between these entities and their interactions with the end users of cloud services. In India, the concept of CC was acknowledged in the National Telecom Policy, 2012, which identified the following strategies:

i. *"To recognise that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions.*

ii. *To take new policy initiatives to ensure rapid expansion of new services and technologies at globally competitive prices by addressing the concerns of cloud*

[1] ISO/IEC 17788, Information technology — Cloud computing — Overview and vocabulary, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip.

users and other stakeholders including specific steps that need to be taken for lowering the cost of service delivery.

iii. To identify areas where existing regulations may impose unnecessary burden and take consequential remedial steps in line with international best practices for propelling [the] nation to emerge as a global leader in the development and provision of cloud services to benefit enterprises, consumers and Central and State Governments."[2]

1.3 While the benefits and growth trajectory for CC services are widely acknowledged, the rapid evolution and adoption of cloud technology also poses an interesting set of legal and policy challenges. For instance, the Australian Communications and Media Authority (ACMA) has pointed out that under the current Australian regulatory framework, content-streaming and sharing services available on CC may not be subject to the same obligations regarding classification of information as television and radio provide similar content. This can result in differential regulatory treatment and confusion for cloud customers.[3]

1.4 Other studies have also acknowledged the potential for certain market failures and power asymmetries in this sector. For instance, in surveys conducted by Bain and Company, critical issues such as data portability, software incompatibility and vendor lock-ins were highlighted by IT managers.[4] This points to concerns of market power that may arise if segments of the cloud industry were to be dominated by one among a few large providers. Similarly, there is also scope for information asymmetry between large CSPs and their customers in terms of quality of service (QoS) standards, billing and metering of CC services, data protection, data security, etc. This raises the need to identify and address any concerns regarding protection of consumers of cloud services, especially smaller users like retail customers and Micro, Small and Medium Enterprises *(*MSMEs). In this regard, the Department of Telecommunications (DoT) vide its letter dated 31.12.2012, referred as Annexure-I, sought recommendations from the Telecom Regulatory Authority of India (TRAI) on various licensing and regulatory issues arising from Cloud services. TRAI sought clarifications from DoT, vide letter no. 305-3/2011-QoS(Vol.II) dated 23rd June 2014 addressed to Member (Technology) on whether TRAI recommendations should include implementation strategies of Cloud Services in Government (Central & State/ UTs) Organizations as these are already being dealt by DeitY, (refer Annexure-II). Clarification were communicated by DoT to TRAI vide

---

[2]National Telecom Policy, 2012 available at http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final_0.pdf.

[3]The cloud: services, computing and digital data, emerging issues in media and communications, Occasional paper 3 (2013) available at http://www.acma.gov.au/theAC*MA/About/The-ACMA-story/Connected-regulation/emerging-issues-cloud-computing*.

[4]The Changing Faces of the Cloud", Bain and Company, 2017 available athttp://www.bain.com/Images/BAIN_BRIEF_The_Changing_Faces_of_the_Cloud.pdf

letter no. 4-4/Cloud Services/NT-2012 dated 22 June 2015(refer Annexure-III) where DoT intimated that the recommendations on Cloud Services may be given by TRAI on the broad categories mentioned in the earlier letter dated 31st December 2012 **without being too specific on its implementation strategies in the Government sector**.

1.5 TRAI issued a consultation paper in June 2016 following DOT clarifications. These recommendations follow from the Consultation Paper on CC issued by TRAI. The recommendations are divided into four parts:

i. State of CC and potential market failures in this sector.

ii. Summary of stakeholder views and present legal framework applicable to cloud services in India.

iii. Analysis of the issues raised in the consultation paper and the recommendations arising from it.

iv. Summary of the recommendations made by the Authority.

Chapter-2 Background

A. DoT letter and TRAI's consultation process

2.1 After the release of the National Telecom Policy2012, DoT vide its letter dated 31.12.2012 sought recommendations from TRAI on CC based services pertaining to the following broad aspects:

- Regulatory framework for CC
- Security over the cloud
- Cost benefit Analysis
- Quality of Service of the Cloud Services
- Interoperability amongst the cloud players
- Incentivisation for conceptualization and implementation of India based Cloud Services
- Legal framework for multiple Jurisdictions/Areas of operation
- Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organizations and other strategic networks.

2.2 Pursuant to the reference by the DoT, TRAI issued a consultation paper discussing emerging issues in CC regulation on 10.06.2016. In this consultation paper, stakeholders were asked to give their detailed and reasoned inputs on various issues detailed in Annexure-IV.

B. Stakeholders responses

2.3 The Authority received comments and counter comments from stakeholders. These were placed on the TRAI website www.trai.gov.in. An Open House Discussion (OHD) with stakeholders was organized on April 3rd, 2017. This section sets out the responses received from stakeholders on the following key issues relating to cloud services regulatory framework.

▪ *Regulatory framework for CC*

2.4 **Scope of Cloud Services in law**: Most of the stakeholders have submitted that the TRAI should adopt a light-touch regulatory approach that minimizes regulatory burdens, provides policy clarity and certainty, creates a climate that maximizes infrastructure investment, and recognizes the global nature of the cloud technology. They have highlighted that the current regulatory framework consisting of Information Technology Act ("IT Act"), the IT Act (Reasonable Security Practices and Procedures) Rules or Intermediary Guidelines, etc. are sufficient. Further, CSPs will also be under purview of

regulation from data controller/data processor perspective if the Parliament chooses to enact a comprehensive data protection/privacy law.

2.5 Several stakeholders have pointed out that various other legislations such as Income Tax Act, 1961, Consumer Protection Act, 1986, Payment and Settlement Systems Act, 2007, Indian Copyright Act, 1957, Central Excise Act etc. must also necessarily be complied with by the CSPs. Few stakeholders have suggested that a regulatory body (similar to TRAI or Real Estate Regulatory Authority) must be set up to oversee the activities of CSPs in India and a legislative framework should be set out delineating aspect such as data ownership, data transfer, data retention, data deletion, security and backups, right to access/information requests and enforcement mechanisms.

2.6 Some stakeholders have supported the regulatory guidelines and best practices approach as the cloud market is presently driven contractually and many extant laws already govern the CSPs.

2.7 **On licensing/registration of CSPs**: Most stakeholders were of the opinion that licensing/registration of CSPs is not required at this stage. Many stakeholders suggested an alternate light touch regulatory approach to be the better approach. Stakeholders reasoned that since cloud services are provided over telecom infrastructure which is already licensed and regulated, CSPs need not be licensed/regulated separately.

2.8 **Data protection:** In relation to data protection during migration, most stakeholders argued that existing laws and policies are sufficient to ensure the same. However, some of them suggested that the government should embed code of practices such as ISO 27018[5] within the proposed Right to Privacy Bill. Alternatively, amendments could be introduced to the IT Act. Two stakeholders have supported the need for a comprehensive privacy legislation governing all categories of personal information and with horizontal applicability to government and businesses alike. However, some stakeholders have stated that contractual provisions are the appropriate mechanism even for regulating the data protection rights and obligations of end-users and CSPs in cloud environment.

2.9 **Location of storage of data storage:** Some stakeholders believed that primary location for the data storage should be encouraged to be in India. Alternatively, data should be allowed to be taken outside India, only to such countries that provide full, absolute and immediate legal access to it, under multilateral or bilateral agreements, specifically while dealing with sensitive personal data. Few stakeholders suggested that data storage outside the country should only be allowed for maintaining backups and for disaster recovery purpose. This choice should, however, be entirely that of the customer using cloud services.

2.10 **Data security:** Many stakeholders have recommended that data security during migration should be maintained by CSPs by implementing international security

[5]ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

standards and encryption policies such as ISO 27001[6], Service Organization Controls Report (SOC) 1 and 2, Payment Card Industry Data Security Standard etc. About security during migration, a majority of the stakeholders have stated that rather than attempting to "prescribe a secure migration path", governments should encourage the adoption of voluntary disclosures and transparently developed, industry-led international standards, while reducing conflicting legal obligations on CSPs.

- *Legal framework for CSPs operating in multiple jurisdictions*

2.11 **Secure transfer of data between jurisdictions:** Most of the stakeholders have pointed that country level agreements can facilitate secure cross border transfer of data through internationally binding laws like the "Privacy Shield" that has been executed between EU and USA. Further, there should be transparent disclosure of location of data and prior permission before transferring it offshore. Some stakeholders have also advocated for an appropriate methodology to lodge complaints in home country in case the data is misused.

2.12 **Lawful interception of data:** Many stakeholders have opined that regulations should encourage the practice of hosting data within India. Alternatively, data should only be allowed to be transferred to such countries that provide full, absolute and immediate legal access, under multilateral or bilateral agreements.

2.13 About extraterritorial requests for lawful interception, most of the stakeholders are of the opinion that the scope of bilateral agreements may be widened for sharing information between nations. To enhance lawful access to information, the government of India should enter into Mutual Legal Assistance Treaties (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 including negotiating e-MLATs. Some stakeholders have also stated that India could consider joining the Council of Europe's Budapest Convention on Cybercrime that inter alia contains provisions on remote search and seizure and mutual legal assistance. Further, some stakeholders have also recommended setting up of a single agency to coordinate processes of obtaining orders for disclosure of data from CSPs. They also suggested that CSPs should identify a point of contact who will be responsible for receiving and responding to all orders issued against them.

2.14 **Interoperability:** Most of the stakeholders agreed that interoperability in Cloud services is an important concern for the users.

2.15 However, some stakeholders were of the view that technical standards for interoperability are domain of the CC industry and any regulatory intervention should be avoided on this issue. Another view that emerged from the stakeholders is that interoperability clause should be under a mutually agreed, contractual agreement

[6]ISO/IEC 27000 family - Information security management systems

between the CSPs and the customers; interoperability in CC should not be under any regulatory framework. However, if a need is felt for regulation on this issue then it should be `light touch' in nature.

2.16 Some stakeholders suggested that the best way to ensure interoperability in CC services is to follow industry best practices and international standards like the ones prescribed by ISO, etc. 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.

2.17 Further, it was suggested that the government may establish interoperability test beds which can help assess the level of interoperability between CC services provided by various CSPs.

- *Cost benefit analysis*

2.18 Most of the stakeholders agree that the benefits of cloud deployment far outweigh its costs. CC offers several advantages over the traditional IT setup. Some of the advantages are low capex requirements, scalability, multi-tenancy and low maintenance cost.

2.19 Stakeholders highlight that cloud computing offers distinct advantages for social networking and e-commerce websites where internet traffic can be highly unpredictable and demand for computing and storage can rapidly increase. In such scenarios, cloud computing enables instant scaling up of the resources. In addition, with cloud computing, businesses and government agencies can focus on strategizing and delivery of their services as the requirements of building, owning and maintaining the IT resources are reduced.

2.20 In terms of factors that businesses consider while selecting the type of cloud service deployment, stakeholders highlight that cost of deployment is one of the most critical factor. Cost of cloud services is particularly crucial factor for small and medium enterprises. Pay as you go model of cloud pricing works particularly well for MSMEs. However, few stakeholders pointed out that large organisations give a higher priority to data security and compliance over cost of deployment. For large organisations, security and operational efficiency of the cloud services seems to be the critical factors and thus they often opt for private clouds with fixed pricing models. Other factors that businesses consider for selecting a cloud service are reporting of overall QoS, Service Level Agreement (SLA) fulfilment, flexibility & elasticity of cloud service access.

C. The present legal framework for cloud services in India

2.21 In India, provisions pertaining to privacy, intermediary liability etc. under the Information Technology Act, 2000 (IT Act) are also applicable to CSPs. Section 43A of the IT Act requires any body corporate that is possessing, dealing or handling any sensitive personal data or information to ensure adequate protection of such information.

It provides for the payment of compensation in case of any negligence in this regard. The term "body corporate" refers to any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities, which would include a CSP incorporated outside India. However, the scope of this provision is limited to the protection of "sensitive personal data or information", which has been defined in the rules in this regard by the Government.

2.22 Section 69 of the IT Act empowers the Central Government, State Government or any officers who are specially authorised to issue orders, to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource.[7] The direction to disclose and gain access to such a resource can be issued to "any person in-charge of the computer resource". There are certain substantive and procedural safeguards built into Section 69. As such, the interception of communications under Section 69 must be carried out in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, or public order , or for preventing incitement to the commission of any cognizable offense relating to the above.

2.23 Further, Section 69B of the IT Act permits authorised entities to monitor and collect traffic data for the purpose of cyber security. Besides Sections 69 and 69B, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ('the 2009 Rules') stipulate further procedural safeguards.

2.24 Furthermore, Section 72A provides for punishment for disclosure of information in breach of lawful contract. It provides that any person, including an intermediary, who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

[7]Section 2 (1) (k) of the IT Act states that a computer resource includes a computer system, computer network, database as well as software.

Chapter-3 Analysis and Recommendations

A. Is there a market failure?

3.1 Over the last decade, CC services have seen an exceptional growth in their usage. From 2012 to 2015, demand of cloud computing accounted for 70% growth of related IT market.[8] Global cloud IT market revenue is predicted to increase from $180 billion in 2015 to $390 billion in 2020, attaining a Compound Annual Growth Rate (CAGR) of 17%.[9] The growth of CC in India is equally promising. An analysis by Gartner Inc. suggests that the market for public cloud services in India is projected to increase to $1.81 billion in 2017 from $1.31 billion in 2016 depicting a growth of around 27%.[10]

3.2 Even though the CC market seems to be functioning well in terms of increasing adoption and growing competition among players, the design and mode of delivery of cloud services gives rise to certain potential concerns, which need to be discussed further. The cloud market suffers from a problem of information asymmetry as customers whose data is collected and stored in the cloud do not know what systems are in place to protect that data. Any misuse of data or security breach at the end of CSPs can lead to massive financial and reputational losses for cloud customers and create negative externalities for third parties who might be affected by the breach. Further, there is also a need to understand if the market has the tendency of being dominated by a few large players as some may argue that the inherent design of the cloud business is conducive for large players with significant resources. In addition, as noted above, issues like data portability, software compatibility and vendor lock-ins have also been highlighted by IT managers in surveys relating to cloud service.[11]

3.3 The existence of information asymmetry in terms of data protection, QoS, billing and metering of CC services is particularly relevant for the smaller users like retail customers and MSMEs. For example, if an MSME does not get the promised QoS or is billed inaccurately for the availed services, it may not have the capability or capacity to raise and resolve these issues against a large CSP. Presently, there are no forums available for

---

[8]"The Changing Faces of the Cloud", Bain and Company, 2017, Available at http://www.bain.com/Images/BAIN_BRIEF_The_Changing_Faces_of_the_Cloud.pdf

[9]Ibid.

[10]"Gartner Says Public Cloud Services in India Forecast to Reach $1.8 Billion in 2017", Available at http://www.gartner.com/newsroom/id/3592917.

[11]The Changing Faces of the Cloud", Bain and Company, 2017 available at http://www.bain.com/Images/BAIN_BRIEF_The_Changing_Faces_of_the_Cloud.pdf.

the resolution of such issues.

3.4 The fast-paced development in the cloud market coupled with issues of concern has led regulatory authorities and governments across the world to discuss need for standards governing the functioning of certain aspects of cloud services, such as data protection, data security, interoperability, portability, and jurisdiction issues. Saudi Arabia, which is one of the few countries that is considering a specific law on CC, offers the following reasons to consider regulating this area:

- Providing clarity and regulatory certainty on the rights and obligations of the providers and users of CC services.
- Establishing a clear regulatory framework to manage potential security risks connected with the use of cloud services.
- Encouraging improved quality of cloud services.
- Encouraging investment in a local cloud industry

3.5 At the same time, given the efficiencies and cost advantages associated with CC, there is an increasingly strong push towards making existing legal and regulatory regimes more "cloud-ready" and "cloud-friendly" to tap into these benefits. For instance, a study undertaken for the European Commission (EC) estimated that the public cloud would generate €250 billion in GDP in 2020 with cloud-friendly policies in place against €88 billion in the "no intervention" scenario, leading to extra cumulative impacts from 2015 to 2020 of €600 billion.[12]

3.6 Against this background, this section sets out the Authority's recommendations on the proposed regulatory framework for cloud services in India. These recommendations have been framed with a view towards striking an appropriate balance between the innovation, business needs of this rapidly evolving sector and the protection of interests of consumers of cloud services.

B. Legal and regulatory framework for Cloud Based Services

3.7 A study of regulatory frameworks in jurisdictions such as EU, U.S., Saudi Arabia, South Korea and New Zealand reveals that different regulatory frameworks ranging from comprehensive legislations to self-regulations have been adopted by different jurisdictions based on the present status of cloud services and present concern of the stakeholders. Some of the important strategies adopted by few leading jurisdictions to regulate CSPs have been discussed below. Apart from regulatory framework, many countries, including India, have specific guidelines and accreditation norms that apply specifically in the context of provision of cloud services to government agencies:

[12]European Commission, Unleashing the Potential of Cloud Computing in Europe, Brussels, 27.9.2012, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

i. **Regulation through a comprehensive legislation:** South Korea has already passed a legislation governing the development of CC services and the protection of its users. Under this law, the Minister of Science, ICT and Future Planning has been entrusted with the power to prescribe the usage of certain standard agreement forms by CSPs, and to notify standards for the quality of service and data protection and security, among others.[13]Countries such as Saudi Arabia[14] and China[15] have also proposed to impose government regulation on CSPs. Both countries have tabled draft regulations to address the issues in cloud services. The proposed regulations tabled by Saudi Arabia seek to implement a license regime for all CSPs who wish to provide cloud services to cloud users having a residence or user address anywhere in the territory of the kingdom. Similarly, the proposed Chinese regulations also require an operator of a cloud service to obtain a license to operate such business in China.[16]

ii. **Self-regulation:** New Zealand, on the other hand, has a voluntary code of practice (the CloudCode) for CSPs. This CloudCode is developed and operated by an independent professional body of the IT industry.[17] This is a disclosure based framework that requires signatories to make specific disclosures to their clients during and after the sales process on issues such as their ownership, security measures in place, location where data is stored, etc. It provides for a mechanism through which any person can made a complaint to the CloudCode Registry if it is noted that any signatory to the code has made an inaccurate disclosure. While the CloudCode does not impose any legal obligations on the signatories, a complaint can result in a requirement for a CSP to update its disclosures or even lead to the removal of a signatory. Non-compliance with the code can also attract liability under general law (for example for misleading and deceptive conduct). In the US, consumer advocacy groups such as the Cloud Standards Customer Council, a body with over 650 member organizations led by a steering committee, works on laying down standards, security, and interoperability issues surrounding the transition to

---

[13]Republic of South Korea, Act on the Development of Cloud Computing And Protection of its Users, available at https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=35630&type=part&key=43.

[14]Public Consultation Document on the Proposed Regulation for Cloud Computing, available at http://www.citc.gov.sa/en/new/publicConsultation/Documents/143703_en.pdf.

[15]Available at https://www.cov.com/-/media/files/corporate/publications/file_repository/alert_insert_cyber_security_review_measures_english_translation.pdf

[16]China's Ministry of Industry and Information Technology, a draft "Notice on Regulating CC Service Market Business Activities" (Draft Notice), available at http://www.nortonrosefulbright.com/knowledge/publications/145031/cloud-computing-in-china-new-rules-will-increase-regulatory-oversighthttp://www.nortonrosefulbright.com/knowledge/publications/145031/cloud-computing-in-china-new-rules-will-increase-regulatory-oversight.

[17]Cloudcode, New Zealand cloud computing code of practice, available at https://cloudcode.nz/upload/files/NZCloudCode.pdf.

the cloud.

In Singapore, the Infocomm Development Authority of Singapore has issued the Cloud Outage Incident Response (COIR) Guidelines, which offers a voluntary framework for CSPs and cloud users to deal with outages in the cloud. The guidelines provide a tiered framework for transparency in CSPs' outage response for cloud users allowing users to choose the appropriate tier of outage protection to complement their requirements. It is proposed that a Working Group will further enhance the COIR Guidelines into a Singapore Standard under the auspice of Singapore IT Standard Committee.[18]

iii. **Sectoral regulations:** Many jurisdictions have chosen to adopt a functional regulatory approach pursuant to which they regulate certain functions performed by cloud providers (primarily the collection and storage of data) through various laws, rather than regulating CSPs as such. For instance, in UK, the Data Protection Act, 1998 (DPA) is also applicable to personal data that is processed or stored by CSPs. The information commissioner's office has released a data protection guidance for organisations that use CSPs to enable them to comply with the DPA.[19] Similarly, in the US data protection obligations arising from sectoral laws such as the Health Insurance Portability and Accountability Act of 1996 and the Financial Services Modernization Act of 1999 are applicable to CSPs. Further, certain states in the U.S such as Maryland, Nevada and Massachusetts also have laws pertaining to data protection and data security which are applicable to CSPs.[20]

In Australia, while all CSPs are not covered by the licensing requirement under the Telecommunications Act, there may be instances wherein the nature of services provided by the CSP will be categorised as "carriage services" under the legislation. For instance, if a CSP only provides the service of data storage, it may not be characterised as a "carriage service", whereas a webmail service that enables customers to communicate with each other may be characterised as a "carriage service". Accordingly, a CSP providing a webmail service will be subject to the licensing requirement under the Telecommunications Act.[21]

iv. **Engagement between Government and the industry:** In Europe, the Cloud

---

[18]Infocomm Development Authority of Singapore, Cloud Outage Incident Response Guidelines, available at https://www.imda.gov.sg/industry-development/infrastructure/ict-standards-and-frameworks/cloud-outage-incident-response-guidelines.

[19]Information Commissioner's Office, Guidance on the use of cloud computing, available at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf.

[20]Jared HarshBarger, Cloud computing providers and data security law: Building trust with United States Companies 16 J. Tech. L. &Pol'y 229 2011.

[21]Australian Government, Department of Communications, Cloud Computing Regulatory Stock Take (2014), available at https://www.communications.gov.au/publications/cloud-computing-regulatory-stock-take-report.

Security Industry Groups (C-SIG) established by the European Commission (EC) Directorate General for Communications Networks, Content and Technology (DG CONNECT) play a key role in providing independent validation and advice on CC related proposals. The C-SIGs comprise of representatives from major European and multinational companies and organizations with significant involvement in cloud computing[22] The DG CONNECT has convened several sub-groups such as the C-SIG on code of conduct, C-SIG on service level agreements (SLA) and C-SIG on certification schemes to engage stakeholders and implement the EC's European Cloud Strategy. It should be noted that EC bodies generally chair the C-SIG sub-groups.[23]

The following are some of the activities that have been carried out by the C-SIG sub-groups:

- Voluntary certification scheme developed by C-SIG Certification subgroup and the European Union Agency for Network and Information Security (ENISA).
- Voluntary code of conduct on Data Protection for Cloud Service Providers developed by the C-SIG subgroup on codes of conduct.
- SLA standardisation guidelines developed by the C-SIG subgroup on SLAs.

3.8 **Proposed regulatory framework for Cloud Services in India**: As discussed earlier, Cloud service providers are still at nascent stage in the country. While stakeholders have raised the concerns relating to implementation of Quality of service standards, prescription and enforcement of SLA, transparent billing and metering of Cloud Services (CS), data protection, security, and well-defined framework for redressal of the grievances of the CS users, most of the stakeholders have opined that licensing/ registration of CSPs is not required at this stage as it may be counterproductive and restrict inventions. Further they emphasised that adoption of light touch regulations with minimum regulatory burden will on one hand address the concerns of CS users. It will also provide policy clarity and certainty and create a climate of maximum investment in infrastructure and push the growth. Therefore, there is a need to have fine balance to address the concerns of the consumers while providing complete flexibility to the CS industry to grow and adopt business models that are most appropriate to meet customer demand. After analysing the various approaches adopted by different countries and considering the status and growth of Cloud Services market in India, the Authority is of the view that light touch regulatory approach should be adopted to regulate Cloud Services at present. Various available options have been explored. It is felt that

[22], Cloud Select Industry Groups, available at https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups.

[23]For instance, the sub-group on code of conduct is jointly chaired by DG CONNECT and DG Justice, available at https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers .

regulation of the CSPs through their industry body is most appropriate framework as it will create an environment to speed-up investments and growth and it would also have capability to effectively control restrictive and anti-consumer practices simultaneously ensuring a code of conduct in the sector. A well-shaped and well nurtured growth of CSPs will not only be good to meet consumer demands but will also catalyse digitisation drive in the country. This approach would be with minimum intervention and such a framework will also protect the interests of the users of cloud services while ensuring that the technological and business advancements in the cloud sector are not hindered by any form of strict regulation.

3.9 Accordingly, the Authority recommends that DOT may prescribe a framework for registration of CSPs industry bod(y)(ies). The terms and condition of registration of Industry led body, Eligibility, entry fee, period of registration, and governance structure etc. would be recommended by TRAI once the recommendations are accepted by the Government in principle. Under this approach, CSPs operating in India would collaborate to form "industry body for Cloud Services in India"[24]. No restrictions on number of such industry body is being imposed to ensure that there is freedom on functioning of such industry body and such body should not become monopoly of few big entities. Further, the Government including TRAI may reserve the right to seek any information from such industry body, investigate the conduct to ensure transparency and fair treatment to all its members, issue directions or orders or guide lines, as and when needed.

3.10 All CSPs above a threshold value to be notified by the Government from time to time in previous financial year have to become member of one of the registered Industry led body for cloud services and accept the code of conduct prescribed by such body. The threshold may be based on either volume of business, revenue, number of customers, etc. or combination of all these. This industry-led body for Cloud Services would prescribe the code of conduct of their functioning which would include the following:

i. **Adopt a constitution** that is fair and non-discriminatory towards its members. The constitution should have provision to adopt the directions, orders or guidelines issued by the Government from time to time. Constitution should also facilitate provision of sharing information with the Government or TRAI when asked by them from time to time. It should also facilitate investigation of the conduct of such industry body by the Government or TRAI to ensure transparency and fair treatment to all its members.

ii. **Membership**: Membership shall be open to any CSPs operating in India, with an equal opportunity without any discrimination. Each member shall be bound to

[24]As an example of this approach, the MIB (Ministry of Information and Broadcasting) notified creation of BARC (Broadcast Audience Research Council) to design, commission, supervise and own an accurate, reliable and timely television audience measurement system for India.

follow the code of conduct prescribed by the Industry body. The procedure followed by the industry body and its various sub-groups while formulating codes of conduct and other guidelines shall be fair, transparent and non-discriminatory.

iii. **Creation of working groups:** Industry body shall be free to create various working groups to conduct the business including but not limited to for prescribing codes of conduct, to deal with standardisation and technical issues, to deal with consumer grievance redressal etc..

iv. **Mandatory codes of conduct, standards or guidelines:** setting out the The codes of conduct, current best practices[25], standards or guidelines formulated by the industry regulatory body for cloud computing may specifically include the following:

a. **Definitions:** The code should set out definitions of entities and activities that are sought to be regulated.[25] While the Authority endorses the following widely-accepted definition of CC from ISO/IEC 17788:20143, it would be advisable for the industry body to further deliberate upon this issue and develop definitions that are most suitable for the Indian cloud context:

"Cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand."

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.[26]

The Authority also endorses the following definition of a CSP laid down by the International Telecommunications Union (ITU) wherein a CSP is defined as a *"party which makes cloud services available" and* "cloud service" has been defined as *"One or more capabilities offered via cloud computing invoked using a defined Interface."*

ITU also separately defines other CSP related terms like cloud service broker, cloud service partner etc. The industry body should consider and adopt relevant definitions for this sector in Indian scenario.

b. **QoS parameters**: The code should delineate QoS parameters to be complied with by CSPs for different segments of customers and publish them on their website. The code should also set out a requirement to publish, on a regular basis, the QoS metrics achieved by CSPs in order to promote transparency in

[25]The Office of Privacy Commissioner in Hong Kong has defined CC as "a pool of on-demand, shared and configurable computing resources that can be rapidly provided to customers with minimal management efforts or service provider interaction. The cost model is usually based on usage and rental, without any capital investment".

[26]ISO/IEC 17788, Information technology — Cloud computing — Overview and vocabulary, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip.

the sector. This should include QoS metrics achieved at network level and in different customer segments, or deployment models.

c. **Billing models:** The code should lay down various credible billing models that can be followed by member CSPs and publish them on its website.

d. **Data security:** The code should set out the recommended "reasonable" cloud security standard(s) to be followed by its members, pertaining to issues such as encryption of sensitive data, backup options, and disaster management strategy to protect information held by CSPs from misuse, interference, unauthorised access, and loss. All such standard information should be published on their website for the purpose of transparency. For instance, in Australia the Office of the Information Commissioner has issued a detailed guidance as to what would constitute "reasonable steps" pertaining to data security.[27]

e. **Dispute resolution framework:** The code should set out a model framework for handling of complaints, including complaints pertaining to billing, metering and QoS, that should be resolved by CSPs independently. The code may also require CSPs to publish periodic reports on their website of the complaints handled and resolved by them. Procedures may also be prescribed for handling of those grievances which have not been resolved at CSPs level.

f. **Model SLA:** The code should also formulate a model template of SLAs which sets out model clauses pertaining to technical and legal aspects of CC - such as QoS, customer satisfaction, security, data protection, pricing and action in case of SLA violation - for the protection of the customers. This will ensure that safe and fair terms & conditions of contract are drawn up by big and small market players alike. For instance, the EC also facilitated an industry group, called C-SIG SLA subgroup, which prepared a set of SLA standardisation guidelines for CSPs and professional CC services customers. These guidelines lay down the principles for developing SLA standards for CC services along with objectives to be achieved through these SLAs in terms of performance, security and data protection etc.[28]

g. **Disclosure framework**: The code should set out a disclosure mechanism to promote transparency in Cloud Services. This may include requirements to

---

[27] Office of the Australian Information Commissioner ,Guide to information security (2013) , available at https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf.

[28] C-SIG SLA subgroup, "Cloud Service Level Agreement Standardisation Guidelines", 2014.ISO has also developed a SLA framework which establishes a set of common building blocks - concepts, terms, definitions, contexts - that can be used to create cloud SLAs, available at https://www.iso.org/standard/67545.html.

make disclosures regarding location, migration and outsourcing of cloud data to third parties along with disclosures on security and interoperability. For example, under the New Zealand CloudCode, a signatory CSP is required to disclose critical details regarding their cloud products and services such as- (i) who has ownership of data (ii) how data security is ensured (iii)where data is located (iv) how data can be accessed and used by customers etc. The CloudCode does not impose any legal obligations on the signatories, however non compliance with the code can attract liability under general law.

h. **Compliance to its codes and standards:** Industry body shall monitor adherence to prescribed standards/codes by its members, for which adequate audit mechanisms shall be instituted. The results of the audits shall be displayed on the website of the CSP.

i. **Compliance to guidelines, directions or orders issued by DoT:** Industry body shall ensure compliance by its members to the guidelines, directions or orders issued, from time to time, by DoT/TRAI.

j. **Information by DoT:** Industry body shall ensure compliance by its members to provide **requisite information in stipulated time lines as and when sought by DoT/TRAI**.

3.11 TRAI has recognised the dynamic nature of cloud services being provided. The scope, nature, security requirements, and creation of transparent networks beyond national boundaries will require considerable oversight on cloud service provisioning. Accordingly, a government body will have to be tasked to periodically review the progress of Cloud services and advise the Government regarding various actions required to be taken. In this background, the Authority recommends that the Government shall create an **Cloud Service Advisory Group (CSAG)** to advise itself of the sector's evolving requirements, proper functioning and security challenges. This Advisory Group may consist of:

i. Representatives of Centre/ state IT departments

ii. MSME associations

iii. Consumer advocacy groups

iv. Industry experts

v. Representatives of Law enforcement agencies

3.12 In view of above discussions, Authority recommends-

i. Light touch regulatory approach may be adopted to regulate cloud services;

ii. DOT may prescribe a framework for registration of CSPs industry bod(y)(ies), which are not for profit. The terms and condition of registration of Industry body, Eligibility, entry fee, period of registration, and governance structure etc. would be recommended by TRAI once the recommendations are accepted by the Government in principle.

iii. **All Cloud service providers above a threshold value notified by the Government from time to time in previous financial year have to become member of one of the registered Industry body for cloud services and accept the code of conduct (CoC) prescribed by such body. The threshold may be based on either volume of business, revenue, number of customers, etc. or combination of all these. Registered Industry body, not for profit, may charge fee from its members, which is fair, reasonable and non-discriminatory.**

iv. **Industry body for Cloud Services would prescribe the code of conduct of their functioning. Code of conduct shall include provisions as detailed in para 3.10.**

v. **No restrictions on number of such industry bodies may be imposed to ensure that there is freedom in functioning of such industry body and such body should not become monopoly of few big entities.**

vi. **DoT may issue directions, from time to time, to such industry body as and when needed to perform certain function and procedures to be followed.**

vii. **DoT may also withdraw or cancel registration of industry body, in case it finds the instances of breach or non-compliance of the directions/ orders issued by it, from time to time or non adherence to code of practices notified by it.**

viii. **DoT may keep close watch on the functioning of industry body and investigate functioning of the body to ensure transparency and fair treatment to all its members.**

ix. **A Cloud Service Advisory Group (CSAG) to be created to function as oversight body to periodically review the progress of Cloud services and suggest the Government actions required to be taken. This Advisory Group may consist of**

   a. **Representatives of state IT departments,**
   b. **MSME associations,**
   c. **Consumer advocacy groups,**
   d. **Industry experts and**
   e. **Representatives of Law Enforcement agencies.**

C. An overarching and comprehensive legal framework for data protection

3.13 While Cloud Computing and Cloud Services provides several benefits to both the public and private sector in terms of cost, flexibility, efficiency, security and scalability, the thriving market also gives rise to significant concerns pertaining to the privacy and confidentiality of the data and applications entrusted to CSPs.

3.14 Many jurisdictions across the world such as EU, UK, Hong Kong, South Korea have sought to evolve different regulatory strategies to address these concerns. While the regulatory strategies adopted range from CC services specific data protection, self-

regulatory codes of conduct to application of general data protection frameworks to cloud services, the principles of data protection emerging from these frameworks remain broadly the same. For instance, the E.U. has adopted the General Data Protection Regulation (GDPR) in 2016 to strengthen the data protection regimes across Europe. Apart from the GDPR, a voluntary code of conduct for data protection specifically applicable to CSPs has also been formulated, as detailed later.[29] This code enumerates key data protection norms to be followed by CSPs along the lines of the nine privacy principles enumerated later in this section.

3.15 Similarly, in Hong Kong, under the Personal Data (Privacy) Ordinance, data users are required to protect and prevent the misuse of personal data entrusted to them by data subjects even when it is is outsourced to cloud providers. Further the data users are required to ensure, through contractual or other means, that norms of data retention, purpose and use limitation and data security are honoured by CSPs.[30]

3.16 In United Kingdom, the general Data Protection Act, 1998 (DPA) is also applicable to personal data that is processed or stored by CSPs. The DPA does not prohibit the overseas transfer of personal data, but it does require that such data be protected adequately wherever it is located. This raises compliance issues that organisations using cloud computing services need to address. The information commissioner's office has released a guidance for organisations that use CSPs to enable them to comply with the DPA.[31]

3.17 It is also pertinent to note that the United States does not have an overarching data protection law. However, data protection obligations arising from sectoral laws such as the Health Insurance Portability and Accountability Act of 1996 and the Financial Services Modernization Act of 1999 are applicable to CSPs.[32]

3.18 India does not have a comprehensive piece of legislation dealing with data privacy or personal data protection, but the collection, transfer and use of personal information are governed under the Information Technology Act, 2000 (IT Act).

3.19 Section 43-A of the Act provides that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable

---

[29]EU Cloud Code of Conduct, Data Protection Code of Conduct for Cloud Service Providers, available at https://eucoc.cloud/en/home/.

[30]Office of Privacy Commissioner for Personal Data, Cloud Computing, available at https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf.

[31]Office of the Information Commissioner, Guidance on the use of cloud computing (2012), available at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[32]Jared HarshBarger, Cloud computing providers and data security law: Building trust with United States Companies 16 J. Tech. L. &Pol'y 229 2011.

security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected".

3.20 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules) framed under Section 43-A, describe reasonable security practices and procedures that companies are required to adopt.

3.21 Further Section 72-A provides for imprisonment and/or fine as punishment for disclosure without the consent of the person or in breach of lawful contract.

3.22 In 2012, Planning Commission's Report of the Group of Experts on Privacy identified the following nine national privacy principles which the government could consider while formulating a privacy legislation:

i. **Notice**: A data controller is required to give notice of its information practices to all individuals before any personal information is collected from them or after a breach.

ii. **Choice and consent:** A data controller is required to give individuals choices (opt-in/opt-out) with regard to providing their personal information. Further, data controller is required to take consent before any personal information is collected, processed, used, or disclosed to third parties.

iii. **Collection limitation**: A data controller can collect personal information only for the purposes identified and informed to the individual.

iv. **Purpose limitation**: A data controller is required to process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. Any change of purpose must be notified to the individual

v. **Access and correction**: This privacy principle grants users the right to access their personal information, held by data controllers, and correct them if necessary.

vi. **Disclosure of information**: A data controller cannot disclose personal information to third parties, without providing notice and asking for consent from the individual.

vii. **Security:** A data controller is required to install "reasonable security safeguards" to prevent from loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure.

viii. **Openness:** A data controller is required to take steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

ix. **Accountability**: The data controller is accountable for complying with measures

that satisfy the privacy principles.[33]

3.23 In the recent past, the need for a law on protection of privacy and data has been highlighted in court cases and the media. The Supreme Court is currently hearing arguments on whether right to privacy is a fundamental right under Part III of the Indian Constitution.[34]Further, during the consultation process for CC, few stakeholders have also supported the need for a comprehensive privacy legislation governing all categories of personal information, with horizontal applicability to the government and businesses alike.

3.24 As far as the ***telecom sector*** is concerned, on the 9th of August 2017 TRAI has released a consultation paper on "Privacy, Security and Ownership of the Data in the Telecom Sector". This consultation with stakeholders is to address the following issues:

i. To identify the scope and definition of Personal data, Ownership and Control of data of users of telecom services.

ii. Understand and Identify the Rights and Responsibilities of Data Controllers.

iii. To assess the adequacy and efficiency of data protection measures currently in place in the telecom sector.

iv. Identify the key issues pertaining to data protection in relation to the delivery of digital services. This includes the provision of telecom and Internet services by telecom and Internet service providers (TSPs) as well the other devices, networks and applications that connect with users through the services offered by TSPs and collect and control user data in that process.

3.25 Furthermore, on 31st of July 2017 the Ministry of Electronics and Information Technology (MeitY), Government of India, has constituted a Committee of Experts under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India and comprising of members from Government, Academia and Industry to study and identify key data protection issues and recommend methods for addressing them. The committee will also suggest a draft Data Protection Bill.

3.26 After due consideration of all aspects, in addition to the framework as discussed above, the Authority recommends an overarching and comprehensive data protection law covering all sectors, including a legal framework to protect the data being collected, stored and processed in the cloud. This data protection framework may incorporate the following:

i. **Enhanced protection to sensitive personal information:** The data protection framework could distinguish between sensitive personal information and other

[33]Report of the Group of Experts on Privacy chaired by Justice A P Shah, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[34]Justice K.S. Puttaswamy (Retd.) v. Union of India (2015).

information and accord enhanced protection to sensitive personal information. This categorisation is already present in data protection instruments across jurisdictions[35] and is also incorporated in Section 43A of the IT Act, which penalises the failure to protect data by body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates.

ii. **Globally accepted data protection principles:** This framework should also incorporate protections based on globally accepted principles that have been adopted by various instruments across jurisdictions such as the EU General Data Protection Regulation[36] the UK Data Protection Act, 1998[37], and the South Korean legislation onthe Development Of Cloud Computing and Protection of its Users.[38] These principles have also been reiterated by the Planning Commission's Report of the Group of Experts on Privacy released in 2012.[39] These principles are as follows:

- Notice
- Choice and consent
- Collection limitation
- Purpose limitation
- Access and correction norms
- Disclosure of information norms
- Security

---

[35]Under the UK Data Protection Act, 1998, "sensitive personal data" is defined as personal data consisting of information as to—

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

[36]Article 5, of the EU General Data Protection Regulation, 2016 available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[37]Schedule 1 of the UK Data Protection Act, 1998 available at http://www.legislation.gov.uk/ukpga/1998/29/schedule/1.

[38]Article 27 (Protection of User Information)(1) of South Korean legislation onthe Development Of Cloud Computing and Protection of its Users.

[39]Report of the Group of Experts on Privacy available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

- Openness
- Accountability

iii. **Set out provisions governing the cross-border transfer of data:** The Authority recommends that this framework should delineate the principles that will address the privacy concerns emanating from cross border transfer of data that is collected, stored and processed in the cloud market.

iv. **Create a structural framework for the effective enforcement of the data protection related provisions.** For instance, this may include the appointment of specialised data commissioners and/or assigning sectoral regulators with the responsibility of formulating enhanced regulations pertaining to their sectors. Accordingly, the Authority recommends that in order to administer the data protection framework across all sectors, appropriate regulatory authorities should be identified under the data protection law.

The data authority may be entrusted with the responsibility of overseeing compliance by various bodies, including CSPs, investigating into data breaches and submitting compliance reports to the Parliament. The 2012 Report of the Expert Group also recommended the appointment of privacy commissioners and entrusting them with the abovementioned responsibilities.

v. **Incremental sectoral regulations**: Additionally, certain sectors such as health, information technology, Telecom, insurance, banking etc. may have specific data protection requirements due to their sensitive or distinct nature. In such cases, the appropriate ministries/sectoral regulators may formulate additional data protection regulations applicable to each sector. These sectoral regulators may consult with the designated data authority while drafting such sector specific data protection regulations.

3.27 In view of above, Authority recommends-

i. The Government may consider to enact, an overarching and comprehensive data protection law covering all sectors.

ii. This data protection framework, inter alia, may incorporate the following:

a. Adequate protection to sensitive personal information;

b. Adopt globally accepted data protection principles as reiterated by Planning Commission's Report of Group of Experts on Privacy 2012;

c. Provisions governing the cross-border transfer of data;

D. Interoperability and Portability

3.28 Cloud interoperability means that data can be processed by different services on different

cloud systems through common specifications.[40] It also encompasses the possibility to use different cloud facilities to achieve diverse business goals. Another aspect of interoperability in CC Services is portability, which is the ability to move data, software, platforms and such other entities from one system to another so that it is usable on the target system.[41]

3.29 As highlighted in the consultation paper, lack of interoperability and portability in CC services can lead to issues like vendor lock-in and inflexibility to use multiple CSPs. The greatest level of interoperability is likely to be found in Infrastructure as a Service (IaaS), followed by Platform as a Service (PaaS) and then Software as a Service (SaaS). As acknowledged in the consultation paper, there are very few standard APIs for SaaS applications - switching from one SaaS application to another even with comparable functionality typically involves a change in interface.

3.30 Standardisation and interoperability has a positive impact on the adoption of CC services by the consumers. However, addressing this problem may require development and widespread utilisation of interoperability standards.

3.31 ACMA, the Australian telecom regulator, has also recognized the need to develop standards for interoperability and portability in cloud services. Portability and interoperability standards are still under development in the CC environment. However, the regulator has acknowledged that data portability in cloud services is critical and has the potential to promote competition in communications and media because it would remove existing barriers in the cloud to end users' ability to easily change services.[42]

3.32 The progress in developing standards that enhance interoperability in CC services has been encouraging. The Cloud Standards Coordination report released by the European Commission points out that significant progress has already been made in developing and standardizing compute and storage APIs, IaaS data models and high level cloud vocabularies.[43] However, the report also notes that there is fundamental challenge in interoperability of CC services: "for maximum adoption, flexibility and automation it is important for arbitrary terms (including service monitoring requirements and service level agreement concerns) to be unambiguously defined". Therefore, further efforts might be required to address this challenge.

3.33 Given the growth of the market in terms of competition among CSPs and the significant

---

[40]National Institute of Standards and Technology, "NIST Cloud Computing Standards Roadmap", 2013, Available at: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913661

[41]"Interoperability and portability for cloud computing: A guide", 2014, Cloud Standards Customer Council.

[42]The cloud: services, computing and digital data, Emerging issues in media and communications, Occasional paper 3 (2013) available at http://www.acma.gov.au/theAC*MA/About/The-ACMA-story/Connected-regulation/emerging-issues-cloud-computing*.

[43]European Commissions report on Cloud Standards Coordination, available at https://ec.europa.eu/digital-single-market/en/news/cloud-standards-coordination-final-report

adoption of international CC standards, the Authority is of the view that there is no need for regulatory intervention on the issue of interoperability in CC services at this stage. However, it is recommended that the industry body/ bodies should take steps to promote interoperability in CC industry. For example, cloud interoperability plug-fests may be organised where CSPs can test the interoperability of their cloud infrastructure in relation to other CSPs and demonstrate their cloud products and services.[44] Such forums can also help in promoting common standards for the CC industry.

3.34 Interoperability and portability in CC services have multiple facets and different components of the CC architecture are involved. Therefore, the customers - individuals, businesses and the government organisations - should carefully select their CC services taking into account the associated cost, security and risks. Information pertaining to CC standards and the compatibility of cloud services provided by different TSPs should be easily available to customers so that they can take an informed decision while selecting their CSPs. Hence, the authority recommends that, in order to inform the users of Cloud Services, the industry body/ bodies may incorporate a disclosure mechanism in order to promote transparency about interoperability standards followed by the CSPs.

3.35 Development and utilisation of standards is one of the principal means to ensure interoperability in CC services. The standards should be developed keeping in mind the needs of the industry, technology, trade and other sectors of an economy. The authority is of the view that apart from adopting international standards from various bodies, it is also important that interoperability standards be developed within the country for wider adoption of the CC services in India. Therefore, the Authority recommends that the task of development of CC interoperability standards should be entrusted with the Telecommunications Standards Development Society, India (TSDSI). Through this process, TSDSI should also contribute towards development of international standards for interoperability in CC services. DoT may direct TSDSI to develop interoperability standards based on international standards along with specific requirements of the country, if any.

3.36 The authority notes the critical importance of interoperability and portability in Cloud services. Therefore, if after a period of time, it is realised that interoperability in Cloud Services is a matter of concern and requires regulatory intervention, the Government may consider other mechanisms in order to protect the interests of the consumers and businesses.

3.37 In view of above, Authority recommends-

i. No regulatory intervention is necessary for interoperability and portability in Cloud services at this stage, these aspects may be left to the market forces. for the time being. However, industry body should be tasked to promote

[44]For example, see http://www.cloudwatchhub.eu/cloudwatch2-virtual-interoperability-plugfest-march-17-2017

interoperability in Cloud Services industry.

ii. **The industry body for Cloud Services should also be mandated to incorporate a disclosure mechanism that promotes transparency regarding interoperability standards followed by the CSPs.**

iii. **Telecommunications Standards Development Society, India (TSDSI) may be tasked with the development of Cloud Services interoperability standards in India.**

E. Legal framework for CSPs operating in multiple jurisdictions

3.38 Cloud technology allows CSPs to store, process and transfer data belonging to citizens or companies of one country in another country or countries. This transfer of data across national borders creates legal issues. First, it creates ambiguity regarding the territorial application of data protections norms i.e. countries are unsure if the privacy of their citizens' data is adequately protected when it is hosted in other countries. Secondly, it creates ambiguity regarding the ownership of data that might be hosted offshore and the ownership of metadata originating from processing user data. Thirdly, this technology has also made it difficult for law enforcement authorities to investigate or gather evidence in criminal and taxation matters, as evidence in form of data may be hosted in a different jurisdiction from where the offence was committed. Lastly, many jurisdictions may refuse to share evidence despite the existence of mutual legal assistance treaties due to specific human rights consideration. Countries across the world have sought to evolve a range of solutions to tackle this issue.

▪ *Data localisation*

3.39 Some jurisdictions have resorted to enforcing various degrees of data localisation to prevent critical criminal evidence from being stored in a foreign country. "Data localisation" refers to measures that specifically prohibit the transfer of data across countries. These measures may include regulations prohibiting information from being sent offshore, or requiring prior consent of the data subject before information is transmitted across national borders, or requiring backup of such information to be stored domestically, and even the levying of a tax on the export of data.[45] For instance, in Russia, the law on personal data processing in information and telecommunications networks requires that any entity operating in Russia to ensure that the "recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data" is to be conducted only in data centres located within

[45] AnupamChander and Uyên P. Lê, Data Nationalism, Emory Law Journal Vol. 64:677 available at http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

the territory of Russia.[46]

3.40 Similarly, the Indonesian government passed the Government Regulation 82 in 2012 which states that any company which provides internet enabled services directly to the consumer is under an obligation to locate their datacentres within Indonesia for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens.[47]

3.41 In India, under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, cross border transfer of sensitive personal data or information abroad is limited to two cases: "when necessary or when the data subject consents to the transfer abroad.[48] In August 2011, the Ministry of Communications & Information Technology (Dept. of Information Technology) came out with a clarification stating the abovementioned rules were meant only to apply to companies gathering data of Indians, and only where the companies were located in India.[49]

3.42 Additionally, in 2013, the sub-committee on International Cooperation on Cyber Security under the National Security Council Secretariat made the following recommendation in favour of data localization requirements:[50]

The control of Internet was in the hands of the U.S. government and the key levers relating to its management was dominated by its security agencies. Mere location of root servers in India would not serve any purpose unless we were also allowed a role in their control and management. We should insist that data of all domain names originating from India should be stored in India. Similarly, all traffic originating/landing in India should be stored in India.

---

[46]Federal Law No. 242-FZ "On Amendments to Certain Laws of the Russian Federation in Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks.

[47]Article 17 of Regulation Number 82 of 2012 Concerning Electronic System and Transaction Operation:(1) The Electronic System Operation for public service shall have a continuity plan of activities to solve with disruption or disaster according to the risk of impacts.

(2) Electronic System Operator for the public service is obligated to put the data center and disaster recovery center in Indonesian territory for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens.

(3) Further provisions on the obligation of placing the data center and disaster recovery center in Indonesian territory as intended in paragraph (2) shall be governed by related Sector Supervisory and Regulatory Agency in accordance with the provisions of regulation after coordination with the Minister.

[48]Rule 7, IT Act Rules, 2011.

[49]Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology Act, 2000, Press Note, available at http://pib.nic.in/newsite/erelease.aspx?relid=74990.

[50]Sandeep Joshi, India to push for freeing Internet from U.S. control,(The Hindu, December 07, 2013, available at http://www.thehindu.com/sci-tech/technology/internet/india-to-push-for-freeing-internet-from-us-control/article5434095.ece

3.43 Any final view on this subject will have to be taken by the Government based on a comprehensive review of the pros and cons of mandated data localisation and its impact on the cloud industry. While on one hand it is often argued that localisation aids the protection of privacy and security of the data, on the other, there is the concern that localisation requirements may "*make it impossible for cloud service providers to take advantage of the Internet's distributed infrastructure*".[51]

- *Privacy shield and restricted transfers*

3.44 In European Union, the Data Protection Directive of 1995 allow data to be sent outside the EU or the European Free Trade Association states) if it is protected adequately either by local law or by contractual arrangement with the foreign company.[52] However, most of Europe's data is transferred and hosted or processed in United States which does not have an overarching and comprehensive data protection law. Therefore, the EU and the US have formulated the 'Privacy Shield' wherein personal data is allowed to be transferred from the EU to a company in the US, only when the said company processes personal data according to a strong set of data protection norms. This protection is applicable to all data originating from the the EU regardless of whether it belong to a citizen of EU or not.[53]

3.45 The above two issues deal with the standard of data protection accorded to sensitive personal data hosted outside the territorial jurisdiction of India. An overarching and comprehensive data protection law may incorporate provisions that govern when and how sensitive personal data of Indian citizens may be allowed to be stored and processed outside India's territory. Further, this data protection law may incorporate specific protections that must be available to sensitive personal data that travels across national borders.

3.46 Accordingly, the Authority recommends that the Government should draft and seek to enact, an overarching and comprehensive data protection law covering all sectors. Further, this framework should delineate the principles that will address the privacy concerns, highlighted above, that emanate from cross border transfer of data that is collected, stored and processed in the cloud market.

- *Mutual Legal Assistance Treaties (MLATs)*

---

[51]Patrick S. Ryan, Sarah Falvey and Ronak Merchant, When the Cloud Goes Local: The Global Problem with Data Localization, Computer, Vol. 46, No. 12, pp. 54-59, December 2013, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2370850&download=yes

[52]AnupamChander and Uyên P. Lê, Data Nationalism, Emory Law Journal Vol. 64:677 available at http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

[53]European Commission, Guide to the EU-U.S Privacy Shield, available at http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf.

3.47 Most countries have executed MLATs with other jurisdictions in order to pave the way for gathering evidence located offshore. MLATs were originally entered into to simplify the process for obtaining evidence relevant to a criminal investigation in one country that was physically located in another.[54] However, the onset of the digital age has meant that the MLAT procedures are used to request another country for digital evidence as well.

3.48 While MLATs continue to be the most commonly relied upon framework for the mitigation of this issue, recent studies point that the framework and the procedure surrounding lawful interception of data is fraught with inefficiencies and delays. Industry bodies and academics have recommended certain improvements that can be introduced in the framework surrounding MLATs.[55] In improving the scope and content of MLATs, some of the key recommendations that may be considered are as follows:

i. **Expand the geographic coverage of MLATs***:* India should consider the evident needs to negotiate new MLATs with countries where cloud data is usually hosted.

ii. **Explicitly cover data that is stored and processed through cloud services***:* Existing MLATs should be amended to cover data stored and processed by CSPs. Such situations often defy neat jurisdictional solutions, and further work on appropriate rules for these situations can reduce uncertainty and improve cooperation for law enforcement authorities and CSPs.

iii. **Explicit timetables for cooperation and response, both by government and CSPs should be set out:** MLATs should set out explicit timelines will to ensure that internal processes are prompt enough for investigatory and judicial needs.

iv. **Designate single point contacts***:* Single point contacts should be established by CSPs and law enforcement authorities. This improves efficiency by reducing confusion about where a request should be sent, and leaving the internal handling of the request to the receiving organization.

v. **Education and sensitization:** Law enforcement agencies should be trained to draft carefully tailored data requests.[56] Further CSPs and others also should be educated about MLATs and their terms, and the manner in which they could cooperate to implement them effectively.[57]

3.49 While the MLAT framework is the most relied upon for lawful exchange of information

---

[54]Krishnamurthy, Vivek, Cloudy with a Conflict of Laws, The Berkman Klein Center for Internet & Society Research Publication, available at https://cyber.harvard.edu/research/cloudywithaconflictoflaws.

[55]Andrew K Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, available at https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[56]Ibid.

[57]Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures, available at http://www.iccindiaonline.org/policy-statement/3.pdf

between contracting parties, it is increasingly being noted to be inadequate and time consuming for meeting the requirements of the digital age. Recent research suggests that emerging technological advancement in CC services is fundamentally incompatible with the outdated manner in which MLATs operate.[58] For instance, CSPs find it extremely difficult to identify legal the jurisdiction involved as data is stored in a fragmented manner across various jurisdiction. Further, CSPs also face difficulty in identifying whose privacy interests are implicated by a digital search until the search is carried out.[59] These problems highlight the increasing incompatibility between CC services and lawful interception through the MLAT process. Therefore, appropriate international and national organizations need to develop a model MLAT framework and deploy it widely. Further, one of the suggestions that have been made in this regard is that key instruments such as the UN Model Treaty on Mutual Assistance in Criminal Matters should be updated and made flexible enough to accommodate (1) provision for both bilateral and multilateral cooperation, (2) optional clauses or protocols providing additional details on particular types of assistance, and (3) transparent cooperation outside of formal MLAT processes. The Indian government should provide inputs for the deployment of such a framework. [60]

3.50 Another suggestion proposes direct data sharing between US companies and law enforcement agencies as an alternative to MLATs. Presently in the US, the Electronic Communications Privacy Act (ECPA) restricts providers of electronic communications from disclosing data to foreign governments. However, proposed amendments to the ECPA would allow US companies to share the content of communications directly with certain foreign governments. Agreements shall be entered into with foreign governments that meet adequate standards of human rights protection to facilitate such direct sharing.

- *Budapest Convention on Cybercrime*

3.51 Governments across the world are seeking to address the issues pertaining to investigation and adjudication of cybercrimes through the Budapest Convention on Cybercrime. During the course of the OHD, many stakeholders have also stated that Budapest Convention might provide solutions to the problems arising out of cross border transfer of data.

3.52 The Budapest Convention criminalises conduct such as illegal access, data and systems interference to computer-related fraud, and child pornography. Further, it also provides for procedure to make the investigation of cybercrime and the securing of e-evidence in

[58]Krishnamurthy, Vivek, Cloudy with a Conflict of Laws, The Berkman Klein Center for Internet & Society Research Publication, available at https://cyber.harvard.edu/research/cloudywithaconflictoflaws.

[59]Id.

[60]Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures, available at http://www.iccindiaonline.org/policy-statement/3.pdf.

relation to any crime more effective, and international police and judicial cooperation on cybercrime and e-evidence. However, to sign the Budapest Convention or not is a foreign policy issue for India to consider.[61]

3.53 The jurisdictional issues arising in access of data hosted by CSPs by law enforcement agencies could be addressed through following measures:

i. Robust MLATs should be drawn up with jurisdictions where CSPs usually host their data.

ii. Existing MLATs should be amended to include provisions that ease lawful interception of cloud data. The Authority recommends that concerned Government arms should provide inputs relating to jurisdictional issues arising in access of cloud data during negotiation of MLATs.

iii. The MLATs currently being negotiated should incorporate protections specifically to enable lawful interception of cloud data.

3.54 Further, the scope and content of MLATs should be improved:

i. Efficient MLAT procedures should be introduced such as setting out of explicit timelines for cooperation and response to be followed by all parties involved.

ii. Single point contacts should be established by CSPs and law enforcement authorities to reduce inefficiency and confusion.

iii. Government should train law enforcement agencies to effectively draft legitimate narrowly tailored data requests. Further CSPs should also be sensitized about MLATs and their terms, and manner in which they should cooperate to implement them effectively.

iv. Government in collaboration with other national governments, should develop an electronic system for submitting, managing, and responding to data requests originating from the MLAT framework.

3.55 In view of above, Authority recommends-

i. To address the issue of access to data, hosted by CSPs in different jurisdictions, by law enforcement agencies:

a. Robust MLATs should be drawn up with jurisdictions where CSPs usually host their services, enabling access to data by law enforcement agencies

b. Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud.

[61] Alexander Seger, India and the Budapest Convention: Why not?, available at http://www.orfonline.org/expert-speaks/india-and-the-budapest-convention-why-not/.

F. Cost- benefit analysis

3.56 The fundamental driver to move towards cloud technology is the huge potential for cost savings. For any business enterprise, the benefits of cloud services stem from financial and operational perspectives to evaluate savings and efficiency in the enterprise.

3.57 Cloud Services enhances costs savings essentially through four ways- First, by lowering the opportunity cost of running technology. Second, by allowing for a shift from capital expenditure to operating expenditure. Third, by lowering the total cost of ownership of technology and last, by giving organizations the ability to add business value by renewed focus on core activities.[62]

- *Development of the cloud market since 2012*

3.58 The cloud services market has grown phenomenally in the past few years. Reports suggest that CC accounted for about 33% of the total IT expenditure in 2015 across the world.[63] The proportion of cloud IT infrastructure sales in the cloud industry climbed to 33.8% in last quarter of 2015, up from 28.7% a year ago. The revenue from infrastructure sales to the private cloud sector grew by 18.8% to $2.9 billion, while sales to the public cloud rose by 25.9% to $4.6 billion.

3.59 The CC market is projected to grow at a 9.7 percent annual rate between 2013 to 2018.[64] Also, by 2019, cloud IT infrastructure spending is expected to be $52 billion, or 45% of total IT infrastructure spending. According to recent reports, worldwide spending on public CC is likely to increase from $67B in 2015 to $162B in 2020 attaining a CAGR of 19%.[65] Reports by KPMG also predict that Platform-as-a-Service (PaaS) adoption is going to be the fastest-growing sector of cloud platforms according to KPMG, growing from 32% in 2017 to 56% adoption in 2020.[66]

3.60 The sustained growth of CC services through the course of the past decade indicates that the structure of the market and the benefits emerging from the technology are in fact incentivising the adoption of CC services. Therefore, on the issue of cost-benefits of the

---

[62]Cloudonomics- The Economics of Cloud Computing, available at http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Cloudonomics-The_Economics_of_Cloud_Computing.pdf

[63]Worldwide"Quarterly"Cloud"IT"Infrastructure"Tracker,"April"21st 2015.

[64]Available at http://www.networkworld.com/article/2175333/cloudUcomputing/idcUUcloudUwillUbeUU107bUindustryUbyU 2017.html.

[65]Pam Miller and John F. Gantz, White Paper on The Salesforce Economy: Enabling 1.9 Million New Jobs and $389 Billion in New Revenue Over the Next Five Years, available at http://www.salesforce.com/assets/pdf/misc/IDC-salesforce-economy-study-2016.pdf.

[66]KPMG, Journey to the Cloud, available at https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/the-creative-cios-agenda-journey-to-cloud.PDF.

cloud computing, the Authority would like to state that while it was an issue when DoT made the aforementioned reference in 2012, it is no longer a key concern as the market has shown significant expansion in the intervening period. With the observed trend and market forecast, the growth of cloud computing services looks promising in the future.

3.61 Therefore, Authority is of view that

i. There is no need to undertake cost benefit analysis of cloud services at this stage as the progress made so far clearly demonstrate the benefit of its use.

G. Incentivise for conceptualisation and implementation of cloud based services in India, especially in government networks

- *Implementation of CC in the Indian government networks:*

3.62 *MeghRaj:* In February, 2014, the Department of Electronics and IT of Government of India initiated a national cloud project termed as 'GI Cloud' Meghraj. The cloud services provided under this project will be used by government departments and agencies at the centre and states following a set of common protocols, guidelines and standards issued by the Government of India.

3.63 The project seeks to set up separate National and State Data centres with the provision of integration as per the need of a state. It will enable the government to leverage CC for effective delivery of eservices.[67] The cloud services available under this project are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Storage as a Service (STaaS). The National Cloud also boasts of features such as self service portal, multiple cloud solutions, secured VPN access and multi location cloud.[68]

3.64 *National eGov App Store*: One of the major parts of the GI Cloud includes establishing National eGovAppStores at the National Clouds. This will aim to be a common platform to host, run and download applications, which are easily customisable and configurable for reuse by various government agencies or departments at the central and state levels without investing effort in the development of such applications. [69] Currently , nearly 300 government users with 6000 virtual servers allocated.[70]

3.65 *NIC CC*: NIC's private cloud enables the Government at various levels - federal, state, and local - a state-of-the-art, high performing, and fully secure hosting operation that

---

[67]5GI"Cloud"(Meghraj)"Adoption"and"implementation"Roadmap,"April"2013,"Department"of""EIT,"GOI

[68]Press Information Bureau, Shri KapilSibal Launches 'National Cloud' Under 'MeghRaj', available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=102979.

[69]MeghRaj Government's GI Cloud initiative (July, 2013),available at http://egov.eletsonline.com/2013/07/meghraj-governments-gi-cloud-initiative/.

[70]http://www.nic.in/services/National%20Cloud%20at%20the%20Core%20of%20Digital%20India.

support secure transaction processing worth several billion dollars per year. NIC's private cloud is supported by a team of technicians with extensive IT management experience.

3.66 *Implementation of CC in Indian MSME sector:* In 2014, the Ministry of Micro Small and Medium Enterprises issued guidelines for the Promotion of Information and Communication Technology (ICT) in MSME Sector. These guidelines state that CC has been found to be capable of providing the requisite ICT solutions to MSMEs at affordable cost. To encourage MSMEs to use CC for ICT applications, the scheme proposed the following key steps:

- To provide subsidy for user charges for a period of 3 years. Initially, CC facilities will be made available to approximately 2300 MSMEs. Each MSME unit will be eligible to a maximum subsidy of Rs 3.0 lakh for 3 years, wherein the cost of usage services will be shared by the GoI and MSME.
- MSMEs will be sensitized regarding the benefits of ICT including CC application for business promotion at a cost of Rs.5 crore.
- The CC component of the Scheme will be implemented by selected Specialized Institutions [like ECIL (Electronics Corporation of India Ltd. Department of Atomic Energy, Govt. of India), STPI (Software Technology Parks of India, Ministry of C&IT), etc.].
- The Specialised Institutions are required to empanel various CSPs through service level agreement who will provide cloud services to the MSMEs.

- *Cloud adoption initiatives in other countries:*

3.67 Several governments across the world have already adopted or are poised to adopt cloud technology to enhance government functioning. For instance, Australia launched its National CC Strategy in May 2013. This strategy states that the Australian Government will aim to be a leader in the use of cloud services in order to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more agile public sector.

3.68 In United States, the federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[71] CSPs offering low or moderate impact cloud services to federal agencies must meet FedRAMP requirements.

3.69 With regard to the incentivisation for conceptualization and implementation of India based cloud services, to CSPs and large private businesses, the Authority notes that the cloud market in India has been functioning well with phenomenal increase in demand

[71] https://www.fedramp.gov/about-us/about/

for cloud services over the last few years. Further, no complaints have been raised regarding the manner in which the market has been functioning by private players. Therefore the Authority recommends that no immediate action for incentivisation is required for the large customers and CSPs at this stage.

3.70 As regards the smaller players in the cloud market, the Authority notes the guidelines issued by the Ministry of MSME for the Promotion of ICT in MSME sector and the initiative to provide subsidies to MSME for usage of cloud services thereunder. This is in line with the policies set out by governments in other jurisdictions. For instance, the South Korean legislation on the Development of Cloud Computing and Protection of its Users[72] states that the government may provide assistance to MSMEs to promote development and use of CC by inter alia providing technologies and subsidizing expenses incurred and by training human resources specialising in CC.[73] Therefore, the Authority recommends that such efforts should be continued in order to incentivise smaller players in the market to adopt CC.

3.71 In view of above, Authority recommends-

i. Government of India's should continue its policy to promote cloud services through cloud infrastructure projects, such as GI Cloud Meghraj, NIC CC and National eGov App Store.

ii. There is no need to give any additional incentive to large customers and CSPs at this stage.

iii. Ministry of MSME may continue to promote adoption of ICT in this sector, including the subsidies as being done at present.

[72]Republic of South Korea, Act on the Development of Cloud Computing And Protection of its Users, available at https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=35630&type=part&key=43.

[73]Article 11 (Assistance to Small and Medium Enterprises)-(1)The Government may provide assistance to small and medium enterprises (referring to the small and medium enterprises defined in Article 2 of the Framework Act on Small and Medium Enterprises; hereinafter the same shall apply) engaging in cloud computing as follows in order to promote the development and use of cloud computing and to protect users:

1.Provision of information about cloud computing services and consulting thereon;

2.Provision of technologies and subsidization of expenses as necessary for protecting user information;

3.Training of human resources specializing in cloud computing;

4.Assistance in other matters necessary for fostering small and medium enterprises engaging in cloud computing.

Chapter-4 Summary of recommendations

A. Legal and regulatory framework for Cloud Services

4.1 Authority recommends-

i. **Light touch regulatory approach may be adopted to regulate cloud services;**

ii. **DOT may prescribe a framework for registration of CSPs industry bod(y)(ies), which are not for profit. The terms and condition of registration of Industry body, Eligibility, entry fee, period of registration, and governance structure etc. would be recommended by TRAI once the recommendations are accepted by the Government in principle.**

iii. **All Cloud service providers above a threshold value notified by the Government from time to time in previous financial year have to become member of one of the registered Industry body for cloud services and accept the code of conduct (CoC) prescribed by such body. The threshold may be based on either volume of business, revenue, number of customers, etc. or combination of all these. Industry body, not for profit, may charge fee from its members, which is fair, reasonable and non-discriminatory.**

iv. **Industry body for Cloud Services would prescribe the code of conduct of their functioning. Code of conduct shall include provisions as detailed in para 3.10.**

v. **No restrictions on number of such industry bodies may be imposed to ensure that there is freedom in functioning of such industry body and such body should not become monopoly of few big entities.**

vi. **DoT may issue directions, from time to time, to such industry body as and when needed to perform certain function and procedures to be followed.**

vii. **DoT may also withdraw or cancel registration of industry body, in case it finds the instances of breach or non-compliance of the directions/ orders issued by it, from time to time or non adherence to code of practices notified by it.**

viii. **DoT may keep close watch on the functioning of industry body and investigate functioning of the body to ensure transparency and fair treatment to all its members.**

ix. **A Cloud Service Advisory Group (CSAG) to be created to function as oversight body to periodically review the progress of Cloud services and suggest the Government actions required to be taken. This Advisory Group may consist of**

   a. **Representatives of state IT departments,**

   b. **MSME associations,**

   c. **Consumer advocacy groups,**

d. **Industry experts and**

e. **Representatives of Law Enforcement agencies.**

B. An overarching and comprehensive legal framework for data protection

4.2 Authority recommends-

i. **The Government may consider to enact, an overarching and comprehensive data protection law covering all sectors.**

ii. **This data protection framework, inter alia, may incorporate the following:**

a. **Adequate protection to sensitive personal information;**

b. **Adopt globally accepted data protection principles as reiterated by Planning Commission's Report of Group of Experts on Privacy 2012;**

c. **Provisions governing the cross-border transfer of data;**

C. Interoperability and Portability

4.3 Authority recommends-

i. **No regulatory intervention is necessary for interoperability and portability in Cloud services at this stage, these aspects may be left to the market forces. for the time being. However, industry body should be tasked to promote interoperability in Cloud Services industry.**

ii. **The industry body for Cloud Services should also be mandated to incorporate a disclosure mechanism that promotes transparency regarding interoperability standards followed by the CSPs.**

iii. **Telecommunications Standards Development Society, India (TSDSI) may be tasked with the development of Cloud Services interoperability standards in India.**

D. Legal framework for CSPs operating in multiple jurisdictions

4.4 Authority recommends-

i. **To address the issue of access to data, hosted by CSPs in different jurisdictions, by law enforcement agencies:**

a. **Robust MLATs should be drawn up with jurisdictions where CSPs usually host their services, enabling access to data by law enforcement agencies**

b. **Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud.**

E. Cost-benefits analysis

4.5 Authority is of view that

i. **There is no need to undertake cost benefit analysis of cloud services at this stage as the progress made so far clearly demonstrate the benefit of its use.**

F. Incentives for conceptualisation and implementation of cloud based services in India, especially in government networks

4.6 Authority recommends-

i. **Government of India's should continue its policy to promote cloud services through cloud infrastructure projects, such as GI Cloud Meghraj, NIC CC and National eGov App Store.**

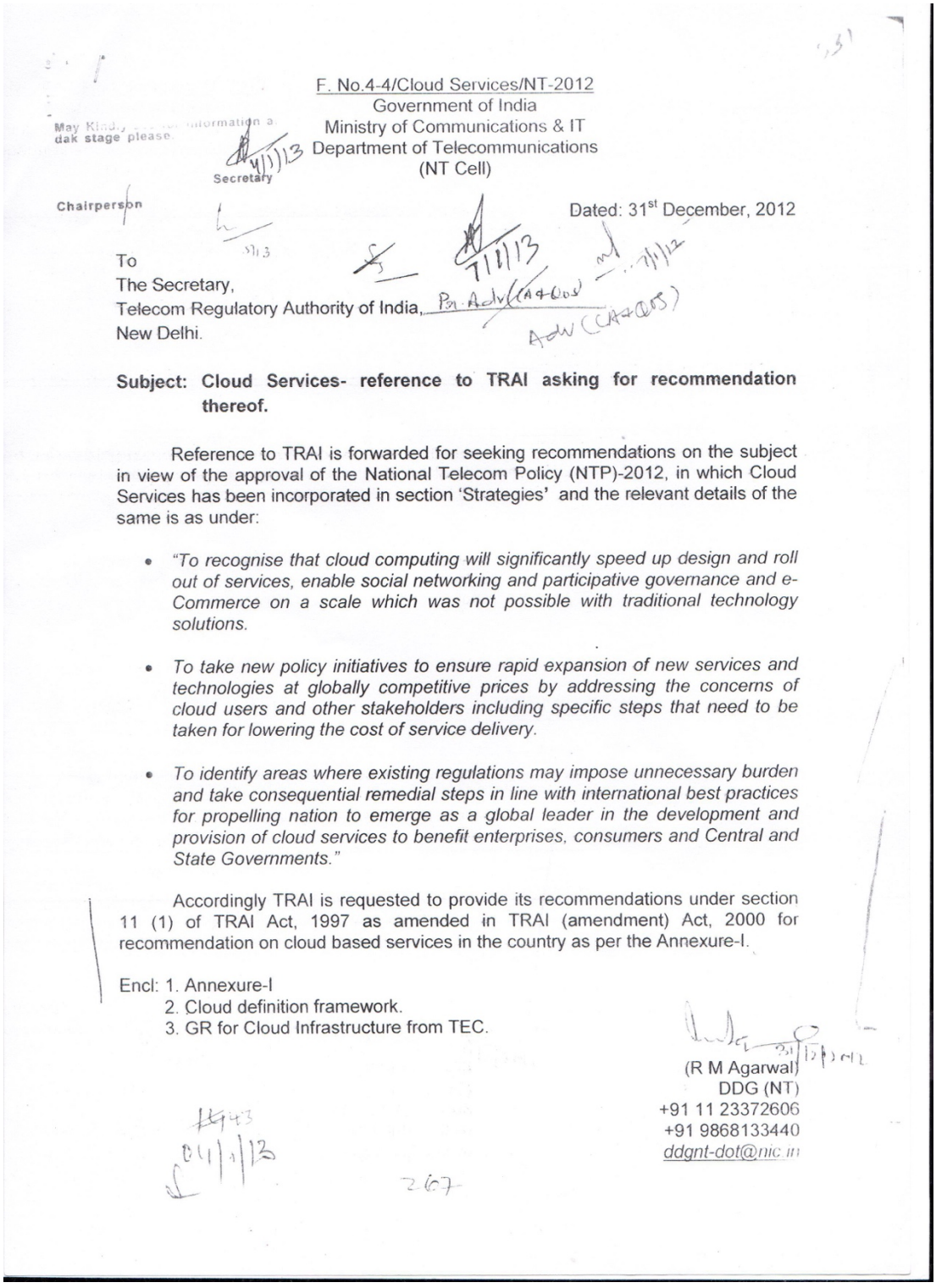
ii. **There is no need to give any additional incentive to large customers and CSPs at this stage.**

iii. **Ministry of MSME may continue to promote adoption of ICT in this sector, including the subsidies as being done at present.**

List of Acronyms

Abbreviations	Description
ACMA	Australian Communications and Media Authority
CAGR	Compound Annual Growth Rate
CC	Cloud Computing
COIR	Cloud Outage Incident Response
CS	Cloud Services
C-SIG	Cloud Security Industry Groups
CSP	Cloud Service Provider
DG-CONNECT	Directorate General for Communications Networks, Content and Technology
DoT	Department of Telecommunications
EC	European Commission
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MeitY	Ministry of Electronics and Information Technology
MLAT	Mutual Legal Assistance Treaties
MSME	Micro Small and Medium Enterprises
OHD	Open House Discussion
PaaS	Platform as a Service
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service Level Agreements
TRAI	Telecom Regulatory Authority of India
TSDSI	Telecommunications Standards Development Society, India

Annexure-I: Cloud Services- Reference to TRAI for recommendations



F. No.4-4/Cloud Services/NT-2012
Government of India
Ministry of Communications & IT
Department of Telecommunications
(NT Cell)

Dated: 31st December, 2012

To
The Secretary,
Telecom Regulatory Authority of India,
New Delhi.

Subject: Cloud Services- reference to TRAI asking for recommendation thereof.

Reference to TRAI is forwarded for seeking recommendations on the subject in view of the approval of the National Telecom Policy (NTP)-2012, in which Cloud Services has been incorporated in section 'Strategies' and the relevant details of the same is as under:

- *"To recognise that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions.*
- *To take new policy initiatives to ensure rapid expansion of new services and technologies at globally competitive prices by addressing the concerns of cloud users and other stakeholders including specific steps that need to be taken for lowering the cost of service delivery.*
- *To identify areas where existing regulations may impose unnecessary burden and take consequential remedial steps in line with international best practices for propelling nation to emerge as a global leader in the development and provision of cloud services to benefit enterprises, consumers and Central and State Governments."*

Accordingly TRAI is requested to provide its recommendations under section 11 (1) of TRAI Act, 1997 as amended in TRAI (amendment) Act, 2000 for recommendation on cloud based services in the country as per the Annexure-I.

Encl: 1. Annexure-I
2. Cloud definition framework.
3. GR for Cloud Infrastructure from TEC.

(R M Agarwal)
DDG (NT)
+91 11 23372606
+91 9868133440
ddgnt-dot@nic.in

Annexure-I

Recommendations may include

Broadly under the following Categories:

- Regulatory framework for Cloud Computing.
- Security over the Cloud.
- Cost benefits analysis.
- Quality (QoS) of the Cloud Service.
- Inter-Operability amongst the Cloud Players.
- Incentivisation for promotion of India based cloud services
- Legal Framework for Multiple Jurisdictions/Areas of Operation.
- Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organisations and other strategic networks.

and subcategories:

- High availability levels.
- Data erasing in the Cloud.
- Data privacy at Service provider end.
- Data Security over the Cloud.
- Data Export Restrictions.
- Monitoring of Data Handling.
- Regulations required for Regulated Industries (financial services, healthcare etc).
- Multiple Jurisdictions / Areas when data is stored at different data centers.
- Enhanced security Cloud Computing services.
- Quality (QoS) of the Cloud service.
- Exit strategies.
- Cloud based different applications viz. Cloud Television/cloud computing on TV – levels of QoS.
- Inter-operability issues amongst Cloud Service Providers (common protocols)
- Legal framework in distributive mode.
- Licensing issues for cloud computing services.

Annexure-II: Clarification sought by TRAI from DoT

सत्यमेव जयते

सुधीर गुप्ता
SUDHIR GUPTA
सचिव/Secretary

भारतीय दूरसंचार विनियामक प्राधिकरण
महानगर दूरसंचार भवन, जवाहर लाल नेहरू मार्ग,
(पुराना मिन्टो रोड) नई दिल्ली-110002
TELECOM REGULATORY AUTHORITY OF INDIA
Mahanagar Doorsanchar Bhawan,Jawahar Lal Nehru Marg,
(Old Minto Road), New Delhi-110002
Tel. : 91-11-23237448, Fax: 91-11-23222816
E-mail : secretary@trai.gov.in

DO No.305-3/2011-QoS (Vol.II)
23rd June, 2014

Dear Sh. Kaushal,

Kindly refer to your D.O. letter No. 4-4/Cloud Services/NT dated 27th May, 2014 to Shri R.K. Arnold, Member, TRAI wherein you have requested for expediting the recommendations of TRAI on Cloud based services in the country. In this regard, I would like to draw attention to your office letter No. 4-4/Cloud Services/NT-2012 dated 31.12.2012 vide which a reference was made to TRAI for seeking recommendation on Cloud Services on the broad categories including Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organizations and other strategic networks.

On this reference, your attention is drawn to the inputs provided by DeitY to the working group meeting held on 23.07.2012 & on 27.08.2012 in DeitY, to "recommend the framework for enabling cloud computing services" that they are capturing all Government Cloud initiatives and providing a comprehensive view of the developments. They have also initiated proof of concept applications on cloud in four states namely Karnataka (based on VMware), Andhra Pradesh (Eucalyptus), Gujarat (Microsoft) and Tamil Nadu (CDAC).(copy enclosed)

In view of above, it may please be clarified, whether TRAI's recommendations should include the Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organizations, since being dealt by DeitY?

Regards

Yours Sincerely,

(Sudhir Gupta)

Shri Anil Kaushal,
Member (Technology),
Department of Telecommunications,
Sanchar Bhawan,
New Delhi-110001

Annexure-III: Response of DoT regarding clarification

68/C

हिन्दी का मान : राष्ट्र का सम्मान

R M AGARWAL
DDG(NT)
Ph: 23372606
Fax: 23372629
Email: ddgnt-dot@nic.in

सत्यमेव जयते

भारत सरकार
संचार और सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, 20, अशोका रोड
नई दिल्ली-110 001

Government of India
Ministry of Communications & IT
Department of Telecommunications
Sanchar Bhawan, 20 Ashok Road
New Delhi-110 001
WEBSITE : www.dot.gov.in

No. 4-4/Cloud Services/NT-2012
Dated 22 June, 2015

Dear Shri Gupta

Kindly refer to your DO letter no.305-3/2011-QoS (Vol. II) dated 23rdJune, 2014addressed to Sh. Anil Kaushal, Member (Technology), DoT regarding clarification on recommendations of TRAI with respect to 'Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organisations'. In this regard, it is kindly intimated that the recommendations on cloud services may be given by TRAI on the broad categories mentioned in this office letter of even number dated 31st December, 2012 without being too specific on its implementation strategies in the Government sector.

Besides, the comments of DeitY as under may kindly be taken into consideration by TRAI while framing its recommendations:

- DeitY had constituted a Task Force and a Working Group to recommend the policy framework and implementation roadmap for adoption of cloud services by Government users in India. The Task Force has published the following reports (available on website of DeitY) after approval by the Hon'ble Minister of Communications & IT in June, 2013:
  - ✓ Government of India's GI Cloud (Meghraj) Strategic Direction Paper
  - ✓ Government of India's GI Cloud (Meghraj) Adoption & Implementation Roadmap
- The first Government National Cloud set up by NIC is operational since February, 2014. DeitY is in the process of setting up a Cloud Management Office for empanelment and accreditation of Cloud Service Providers for providing cloud services to Government users.
- The Working Group has the mandate to come up with policy covering various aspects including incentives, privacy, investment and fiscal incentives to promote cloud services in the country. It is likely to submit draft policy document shortly. TRAI may consider to consult the Working Group to avoid contradiction/ duplication.

It is requested to provide the recommendations at the earliest.

With regards,

Yours sincerely,

(R M Agarwal)

Shri Sudhir Gupta,
Secretary,
Telecom Regulatory Authority of India,
MahanagarDoorsanchar Bhawan,
New Delhi-110 002

Annexure-IV: Issues raised in Consultation Paper

Following issues were raised in the consultation paper on Cloud Computing to seek inputs from various stakeholders:

1. The 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

2. The details on how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

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 small and medium enterprises?

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?

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?

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?

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 that may be suggested.

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?

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

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.

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

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

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

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?

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

16. What shall be the scope of CC services in law? What is your view on providing license or registration to CSPs so as to subject them to the obligations thereunder? Please comment with justification.

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?

18. What are the steps that can be taken by the government for:

    (a) promoting CC 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.

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?

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?

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?