IT *for* CHANGE

NGO in Special Consultative Status with United Nations' Economic and Social Council

IT for Change, Bengaluru's
Response to Pre-Consultation Paper on Cloud Computing
Issued by Telecom Regulatory Authority of India

We believe that the consultation paper covers many broad issues for regulating cloud computing, and, more generally, the society's digital ecosystem, including the Internet. These issues are interconnected and represent a new area of regulation in India. Accordingly, our response first treats these issues from a higher, principles-level vantage. Only then it moves to responding to specific questions raised in the consultation paper.

We thank TRAI for making this important beginning in exploring the regulatory issues involved with the far-reaching manner in which the digital technologies are transforming our societies. Thinkers have compared the expected extent of systemic and institutional shifts in this era to what happened at the advent of the industrial revolution. Policy, law and regulation must keep pace with such deep and far-reaching changes to protect and promote the public interest.

Cloud computing combines the power of the Internet and computing. Networked and remote computing is clearly the mainstream way in which digitalisation of our society will take place. For this reason, cloud computing may not be considered as just one specific sector, it denotes the central paradigm of digitalisation of our societies. Even the Internet as we experience today is largely cloud computing, and it will increasingly be more so in the future. Cloud computing, although often treated as a specific set of technologies, can be treated as a stand-in for the entire, current and emerging, digital ecosystem of our societies.

In the various questions that it raises, the consultation paper speaks about regulating cloud computing. Before the specifics of such questions are addressed, it must be understood that what is being spoken of here is essentially the regulation of the larger digital phenomenon, and its central artefact, the Internet. Appropriately dealing with the depth, enormousness and outstanding importance of these issues requires us to clearly and openly discuss the real facts that underlie them.

We would therefore like TRAI to frame these issues in their full context; how the digital is fundamentally transforming all social systems and institutions, employing the key technologies of digital networking, big data and data analytics, and advanced computing that will increasingly include artificial intelligence; and, how we require new regulatory paradigms and interventions to ensure public interest in this process.

In default, we will continue to have the somewhat discordant and unproductive situations like, if we may say so, with regard to the issues raised in the current consultation. Here, relatively mundane issues like how to make SLAs for cloud computing services and develop technical standards for cloud computing security are being dealt at the same level as extremely fundamental socio-political questions of how to ensure completely interoperability between platforms/infrastructure layers and portability of data, who owns various forms of data, and, how to deal with the relatively borderless Internet in a largely nationally-bound policy systems. These, in our view, constitute two entirely different level of issues.

It is therefore important that TRAI resolves the latter set of fundamental issues first and then follow it up with the matters of relative detail within the agreed broader framework. Such a framework will be based on a set of larger policy principles, that must first be established. Larger policy principles would provide guidance to framing law and regulation, as and when necessary, but also to forbear from them when the circumstances are not yet mature, while still giving everyone a good idea of the policy thinking, and therefore likely legal/ regulatory interventions in the future. This ensures consistency for current regulatory efforts and predictability vis a vis the future ones.

It is therefore an utmost important and prior issue to lay out larger policy/ regulatory principles regarding the nature of public interest in the emerging architecture of our digital ecosystem (which has a huge overlap with what is called as 'cloud computing'). These should follow from a detailed analysis of how the digital ecosystem fundamentally impacts the nature of our emerging social institutions.

In this regard, TRAI must look first at the larger social aspects of how cloud computing/ digital systems are changing all sectors of the society, and not just of enabling and promoting Indian cloud computing industry, which no doubt remains a key priority. But before that we have to deal with the prior issues of what kind of governance and democracy, what kind of marketplace (which is different from individual businesses), what kind of health and education systems, and so on, our society will like to have. The nature of our emerging digital ecosystems will determine these all important questions, and it is at this level that we must begin our inquiry. Within this framework should then be addressed the subsidiary issues of the cloud computing industry.

Clarifying and asserting TRAI's mandate

We are quite confident that very many of responses to the current consultation will simply question TRAI's competence and authority over issues that manifestly belong well beyond the infrastructural layer of the Internet. We see that this consultation paper has presented a view whereby it could be possible to consider cloud computing as a form of 'telegraph signal' and thus included in definition of telegraph and telecommunication as considered in the Indian Telegraph Act and other legal provisions from which TRAI derives its mandate and authority. When new a social area takes shape, it is indeed common for law and regulation to seek connections with and competence from its relationship to the closest existing area that is legally recognised and provided for. To that extent, deriving TRAI's mandate from existing language in statutory documents may be fine, and we can accept it. However, as will be evident from a large number of responses, others are likely to contest this derivation.

In the circumstances, even as TRAI exercises its competence in this area as per the existing legal and statutory language (which we think is fair to do), it should seeks a clearer, specific and more comprehensive mandate, which fully and clearly covers the very important digital ecosystem sector, which is of fundamental importance to our society.

TRAI should develop a detailed paper on the outlines of such a mandate, describing the great social importance of this area, and also touching upon some key policy principles that much apply to it. Expanding on the earlier initiative of the government of India towards a Communication Convergence Bill, TRAI should recommend some kind of *Communication Convergence and Digital Ecosystems Bill*, which should provide a new expanded mandate to TRAI. TRAI itself may need to change its name to more clearly include all the new issues that it must address, something like, T*elecom, Computing and Internet Regulatory Authority of India*, or *Communications and Digital Ecosystems Regulatory Authority of India.*

Laying larger principles for cloud computing (and our digital ecosystems)

As digitalisation and networking transforms every social system, it is important to understand how the digital ecosystem forms horizontal layers across these systems. The horizontal layer of telecom, or the data transport/ connectivity layer, is well understood, and regulated, but similar horizontal, across-the-sectors, layers in the software, application, and data analytics, etc are also getting formed. Like with the connectivity layers, these other horizontal layers are both of fundamental social importance, with a rapid digitization of the society, as they have strong monopolistic tendencies. Therefore, for the same reasons that the connectivity layer is strongly regulated, these other layers also need regulation.

The key basis for choosing to regulate, and the extent of regulation, will depend on the following factors;

1. Degree of monopolistic/ oligopolistic tendencies in the concerned layer/ services, due to network externalities and economies of scale;
2. Extent of big data employed as a key business resource, which greatly enhances monopolistic tendencies;
3. level of importance of the layer/ service to the society;
4. Size and social footprint of the concerned service/entity.

Horizontal, enabling digital services, like traditional utilities, tend towards monopolies/ oligopolies. The digital sector is characterised by extra-ordinary economies of scale that defy geographies, and therefore these monopolies/ oligopolies are often global. The negative impacts of their monopolistic nature can get considerably enhanced when there is vertical consolidation across horizontal layers like infrastructure, software, applications, etc (net neutrality controversies where application providers seek to inappropriately control access to infrastructure, as in the case of Free Basics, illustrate this point). Regulatory principles like checking vertical consolidation across layers, and ensuring full interoperability within each layer, become very important to ensure an open and competitive field, and prevent lock-ins. Any such lock-ins can become exploitative rent-seeking points for key social and economic sectors.

Monopolistic tendencies are further multiplied when the concerned businesses increasingly depend on the vital resource of big data, collected from digital social interactions over their platforms. Therefore, wherever a cloud computing layer employs big data as an important part of its business, it requires special close regulatory attention. It is required to provide clear and enforceable frameworks of data ownership, asserting that personal data belongs to the concerned person, who should be able to fully control its collection, propagation and use. Further, even if data is rendered personally unidentifiable, issues of who is entitled to the economic value of such data have to be determined – which could be the involved individual, or a larger social entity, for instance, the education department in case of data about schools and educational practices in a region, even if the data is collected by a private entity. This issue has major implication with regard to huge value outflows that take place from India to other countries, which is completely unaccounted for.

The need and extent of regulatory intervention should however be calibrated to the specific social importance of the particular service. Gaming services and platforms, for instance, do not require the same kind of attention as services like social networking, geo-mapping, search, general apps development platforms, and so on. Regulation of cloud computing (or digital ecosystems) therefore requires careful service by service, and sector by sector, classification, and calibrated regulatory approaches to each. The regulator will need to recognise not only important general society level services that require close regulation, and the necessary standards and protocols, but also such key cloud computing services in each sector, like, health, education, governance, and so on.

Next, even for socially important services/sectors, to avoid unnecessary regulatory burden on start ups, which can be detrimental to innovation, it may only be the larger service providers with a very significant social/ business footprint that require the most regulatory attention. Regulatory requirements for these larger providers can and should therefore be different in most cases than for the smaller providers. One good example of such differentiation is seen in the recent EU's Directive on Security of Network and Information Systems. This directive imposes specific regulatory measures on digital services underpinning crucial sectors, and also general society-wise digital services. However, it exempts small and micro enterprises from its ambit.

Regulation needs to ensure prior conditions of how cloud computing businesses can be built and run. It should also provide sufficient means of redress for consumers. The market power of most service providers compared to the customers is immense, and they are also often remote and not at all easy to access (including based in other countries). Meanwhile, the importance of these services for continuity of business or social life activities of consumers can be extraordinarily huge – in many cases stopping or poor quality of these services can simply shut down a consumer's business or other key activities. This will be more and more true with increasing digitalisation of the society. The regulator must therefore ensure well-developed and enforceable means of grievance redress for cloud computing services.

Lastly, many cloud computing service providers are based outside India. This brings up issues of application of Indian law and regulation to them, especially in terms of privacy, data protection and ownership, application of mandatory inter-operability and other standards, consumer protection, and general law enforcement. India must take a strong lead in promoting global agreements and standards in this regard. Meanwhile, it should prioritise digital business relationships with countries with whom it is able to develop bilateral agreements, especially on data protection and legal access to data originating from India. (Agreements on mandatory inter-operability standards and data ownership frameworks are more difficult to obtain on bilateral basis and therefore should be pursued at multilateral levels.)

In sum; on the question of whether cloud computing services need to be licensed, we will respond in the negative. At present, this may not be required. However, they need close regulatory attention. Such attention should be calibrated to the social importance as well as the society-wide foot-print of a service. A sector wise approach to the key cloud computing services (or digital ecosystem services) in each sector is also required separately, in consultation with sector experts. This is especially needed for key social sectors like health, education, governance services, and so on.

Such close regulatory watch would require TRAI to build a clear mandate in this area, which area should be recognised more widely than 'cloud computing', as networked digital ecosystems. It should develop key regulatory principles that would inform its work. We must repeat that to do so is of utmost importance and urgency. TRAI must take the opportunity of this current consultations to begin moving in this direction.

Response to specific questions

In the background of the above inputs, which also cover many questions that have been raised in the paper, we now attempt to specifically answer some of these questions. However, we leave unanswered most question that are about business processes and technical specifications. Our approach throughout comes from a larger social, political and economic point of view.

Question 1. What are the paradigms of cost benefit analysis especially in terms of: a. accelerating the design and roll out of services

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

c. Expansion of new services.

d. Any other items or technologies.

Please support your views with relevant data.

As the society undergoes digitally-mediated fundamental transformations in every sector, the costs and benefits have to be foremost assessed at the larger social level, and not just in an industry-centred manner. Cloud computing affords great efficiencies and cost reductions, but they also reduce control at the peripheries (the basic characteristic of the Internet that made it such a powerful social force). This is the key axis of cost benefit analysis that must be employed. While improving efficiencies, regulation should keep a close watch over market power and other forms of control of cloud computing businesses. Strict enforcement is required against vertical integration, for inter-operability within each layer, and across, ensuring data protection and ownership, and enabling complete data portability.

This requires bold measures to inter alia set the larger principles and rules for the emerging architecture of cloud computing, within which businesses should develop their business models. It cannot be done in any kind of half-hearted and piecemeal fashion. Long-term social, political, cultural and economic interests of our country must drive these polices and regulation. We are in a key formative period of digital societies, and digital policy and regulation today will considerably determine the shape of these societies. Once entrenched in a path-dependent manner, major changes to the techno-social structure will not be possible at a later time.

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

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

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

While the technical parameters have to be worked out, policy and regulation must set up strict high level requirements that each layer of cloud-computing must devise its services in a manner that ensures easy and complete migration. General and sectoral standards in this regard must be developed by TRAI in association with other expert bodies.

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

Again, first a political and regulatory commitment at the highest level has to be made that a consumer/ user's data fully belongs to her, and she will be provided full control of it. This policy principle should then be appropriately operationalised. It should be ensured even if it requires deep changes in technical and business models – because these adjustments can only be made at this formative stage, and not later. Clear and bold measures are therefore required, without pandering to short-term industry-focussed considerations, which are otherwise no doubt important.

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

programming and orchestration layer?

We again avoid getting into technical or business models related details, and, in keeping with the other responses above, foremost seek a high level political commitment and policy/ regulatory principles that calls for full interoperability of cloud services at every level. With a strong policy principles established, technical and business model architecture must follow the corresponding guidelines.

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

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

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

This is a common response to questions 8 and 9. Cloud computing, increasingly the mainstream mode of our digital ecosystems, creates conditions that require strong and effective grievance redress mechanisms. Core businesses and key social activities increasingly dependent on cloud computing services, and the service providers are often remote, even outside India. Also, the market power of the latter is mostly huge and highly disproportionate. The regulator and the state must establish strong and effective procedures for complete consumer protection in these rather extra-ordinary conditions. These procedures should form a standing mechanism for this specific purpose.

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

Since cloud computing is becoming a kind of essential infrastructure, policy and regulation must pro-actively ensure its security, and set the necessary standards in this regard. These must be strictly enforced.

Many of the defining features of cloud like centrality, multi-tenancy, and outsourced management are also features that put privacy of the users at risk. One of the methods that can be used to protect user data on cloud is encryption. Most cloud services prefer not using encryption as they are computationally heavy and hence cost more. In the absence of user awareness of the option of encryption, data is stored in cost friendly unencrypted formats. The government must step in and mandate through regulation the use of encryption in cloud computing when personally identifiable information is processed.

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

Not only a consumer should be able to exit at any time, she should be able to do it a manner that is easy and efficient, with full protection to her business or involved social/ personal activates, including in the period of transition. To be able to retain all data that belongs to her, in interoperable formats is a key requirement there.

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

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

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

It should be mandated, with strict penalties for violation, that certain kinds of sensitive data – as determined on various public interest considerations – cannot be moved out of the country. All service providers that deal with any such data will need to have a registered presence in the country. Severe penalties must be visited on them in case of unauthorised transfer of such data as is not allowed to be transferred outside the country. There must also be clear disclosures to the consumers about the place of storage of such sensitive data.

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

As data becomes central to most social systems, ensuring full and absolute legal access to data concerning activities subject to Indian jurisdiction will be of utmost importance. This can only be ensured by mandating that data is either retained within India or allowed only to only be taken outside India to such countries that provide full, absolute and immediate legal access to it, under multilateral or bilateral agreements. While India should work towards multilateral agreement in this regard, in the interim it should enter into reciprocal bilateral agreements with various countries. This extremely important issue can only be ensured either by keeping data within our borders, or only allowing it to go to countries that provide full and immediate legal access to it. There is no other way around it. Meanwhile, clear legal procedures for accessing such data, especially personal data must be laid down. The latter should only be possible to do under due judicial oversight.

As this consultation paper mentions initiatives like the Indian Banking Community Cloud and e-health initiatives that make use of cloud are already underway in India (Annexure V). It is important that consumer data on these networks are secure as they may contain sensitive personal information. To bolster the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 cloud service providers should only make use of local servers if they are dealing with sensitive personal data as defined in Section 3 of the regulation .

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

We have discussed this issue in the above general inputs, including in the section of TRAI's mandate and authority. We do not think there is a need to license cloud services, at least at this stage. However, their nature is such that they require close regulatory oversight. (Registering them with minimum burden can be looked into.) Such close regulatory oversight have a few requisites: TRAI should take on a specific, clear mandate for regulating this area, as discussed earlier; and, it should first develop larger policy and regulatory principles that ensures consistency and predictability for regulation, also connecting it to clear public interest requirements. We have earlier indicated some general policy/ regulatory principles in this regard. Within these larger principles, appropriate regulatory interventions should be devised as required.

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

As mentioned in the response to question 15, the only way to do it is to either keep the data within Indian borders, or to allow it only to be sent to countries that have clear and specific agreements for full and complete legal access to such data, and also full protection for data as available under

Indian law. This is should be clearly articulated as a policy principle in this area. India should strongly pursue diplomatic efforts towards multilateral forums and agreements that provide such legal access and full protection to Indian data across the world. In the interim, it should get into bilateral agreements with its important digital trade partners.

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

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

It is absolutely necessary that the government starts to build its own cloud infrastructure for a Government of India cloud. Because of cost saving, scalable and collaborative nature of cloud, much of government work shifting to cloud computing is inevitable. However, use of cloud infrastructure owned by private corporations by the government is fraught with risk. For one, the safety of data on third party vendor cloud is questionable. The government may have no control over the location of the servers of the company, the personnel of the company handling government data, and the companies own security practices. The other concern which has a question mark hanging over it is the portability of data from one cloud to another. Further, governments must be fully able to determine and control various governance processes, including digital ones. Thus, even though building and operating its own cloud with a dedicated and trained IT staff may in the short term appear more expensive, the government will have full ownership and control over its work processes, and over data. Importantly, the sheer extent and scale of activities of various governments in India taken together, that need to be taken to the cloud, is such to make it even a cost-effective option, apart from other advantages discussed here.

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

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can

be given to private sector for the creation of data centres and cloud services platforms in India?

Cloud services can be treated as infrastructural services, with a force multiplier effect across all sectors, which stand to gain hugely from effective digitalisation. It is also an area of great export potential. The sector should therefore be given all possible tax breaks and other incentives.