

No.:108/TRAI/2016-17/ACTO

Dated: September19, 2016

Shri Asit Kadayan

Advisor (QoS)

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

Subject: ACTO's Counter Comments to TRAI Consultation paperdated 10thJune 2016 on Cloud

Dear Sir,

This is with reference to the detailed comments filed vide by Association of Competitive Telecom Operators (ACTO) vide it's letter No. 102/TRAI/2016-17/ACTO dated 8th August, 2016on TRAI's Consultation Paper dated 10thJune 2016 on cloud.

We have reviewed comments received from stakeholders. Some of the telecom service providers have a view on data localization/ cross border data flow which is not in agreement with the comments submitted by ACTO and majority of other stakeholders who have filed their comments.

In addition to our comments provided vide letter dated 8th August, 2016, we would like to file our counter comments specific to the above issue for the kind consideration of Hon'ble Authority.

We hope that our counter comments (enclosed as Annexure – I) will merit consideration of the Hon'ble Authority.

Thanking you,

Respectfully submitted,

Yours sincerely,
for **Association of Competitive Telecom Operators**

Tapan K. Patra

Director

Encl.: As above

Annexure – I

ACTO's Counter Comments to TRAI Consultation Paper on Cloud

The responses from some Telecom Service Providers and associations have different view of the submissions made by ACTO. The different view is on largely on the issue of data localisation for mandating to have data centre in India citing security concerns and cross border data flow. We would like to submit our counter responses on this point.

1. Data localization and cross border data flow:

Some TSPs have recommended for mandating to set up data centre in India for those who provide cloud services in India. Government data should not move out from Indian geographical territory.

- Requirement of data localization is a reverse concept of cloud technology as it's features/ benefit lies on seamless cross border data flow. By mandating to have data centre for cloud services in India will have it's reciprocal effect from other countries as well that will lead to completely destroy the cloud services and it's related business. The growth of the Internet has also entailed the growing ability of people, businesses, and governments to collect, share, and use data across borders. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders. Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation.
- Cloud solutions are based on global platforms. Mandating the location of placing the server in India should be avoided and is best left to the market forces. The development of all-encompassing cloud market is yet to take place in our country. Such a mandate may negate the opportunities and will deprive consumers of innovative products and services – just because the prime pre-condition to sell a product is to first set up infrastructure. Such a mandate may have bilateral, economic, and commercial consequences and hence, TRAI should not recommend localization of the server in India. Any such mandate has the possibility of impacting the export market which is the key for success of Make in India program.

- The BPO sector of India (where our country is a net importer of data) and which is one of the best in the world is currently hosting servers in India for managing the bank accounts and health records of citizens of US/UK/Europe. Server geographical mandates may be construed as trade barrier issue and could have negative consequences to our BPO sector in case other countries also start imposing such restrictions. As this will have a far reaching implications on every sector which has even a percentage of global business.
- If there is a mandate on server localisation, then other countries may announce similar mandates. This will destroy the “connected” aspect of Cloud which will close all avenues for a globally connected business opportunities. It is not the mandate of telecom players (especially those who have a different view) to take on issues of international trade and bilateral relationships. Mandating server localisation in India will not be without adverse implications for India across the world. So this aspect needs to be carefully analysed.

In summary, the suggestion from some of the stakeholders on data localisation has serious implications on our country’s trade relations, reciprocal arrangements, existing agreements, and above all, possibility of violation of any international treaties and obligations on member nations.

- The Internet and ICT have in many ways transformed the global economy, including international trade. The Internet and ICT enable more services to be tradable. Roughly half of the global services trade is ICT-enabled, including cross-border data flow. There is also a strong co-relation between Internet usage and competitiveness. Cross-border data flows are closely related to international trade. Nowadays, almost all firms in all economic sectors use electronic payment systems, Internet-based advertising and retailing, and cloud computing in their day-to-day operations. It is hard to imagine an international trade transaction that does not involve transferring data.
- Cross-border data flows have also been a driving force behind the emergence of so-called global value chains in which businesses’ operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production. The flow of data is as important as the movement of goods. **Data needs to move to create value. Data sitting alone on a server is like a static /storage library where it’s information flow is restricted and against value addition to foster innovation.**

- The growth of the Internet has also entailed the growing ability of people, businesses, and governments to collect, share, and use data across borders. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders. Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation. The success of the cloud computing industry depends on robust protections for the privacy and security of customers' data. Consumers rightly expect that the information they entrust to cloud service providers will be highly secure and that CSPs will be respectful of their privacy. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues. So if there are any gaps in addressing "specific" concerns, those need to be defined and discussed with industry to find a plausible solution which is in the interest of all stakeholders.
- Governments can build trust in the cloud computing industry by ensuring that cloud service providers follow industry best practices and guidelines regarding the use and protection of personal data. The consultation paper cites the frameworks developed by the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), and the International Conference of Data Protection and Privacy Commissioners (the Madrid Resolution of 2009), which serve as widely accepted international standards for multinational companies that collect, use, and transfer data, as well as for states when facilitating the transfer of data across borders. Rather than erecting barriers to cross-border data flows, the TRAI should ensure that cloud service providers in India adhere to principles such as these and provide strong accountability mechanisms for customers and others who wish to challenge data management practices.
- Be it government as user, enterprise user or retail user, it should be the user's prerogative/choice where to keep their data, it is not fair on the part of the regulator to recommend any mandate for user's choice for selecting cloud services providers.

2. Security:

Some TSPs are advocating with a belief that Data localization increases security but on the contrary, Data security depends on a plethora of controls, not on the physical location of a server. Location of a server has no relationship to its security. Corporations today are replicating their servers across globe to ensure redundancy in their network and to avoid disruptions due to any inadvertent failure. This is a normal and healthy business practice and as per the best international practices. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take a data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic flexibility and neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions. Limiting the private sector's ability to transfer, store, and process data across borders will somehow protect user privacy and improve security but these well-meaning efforts are ultimately counterproductive. The movement of data is no less important to the global economy than the movement of money. Cross-border data flows, just like cross-border financial flows, allow companies to integrate their personnel, manage their global supply chains and customer networks, and maintain the competitiveness they need to grow and thrive. The free movement of data is fully compatible with legitimate security concerns.

In summary:

In view of our above submissions:

- a. There should not be any prescriptive regulation on Cloud Computing.
- b. The market is still in nascent stage and needs to be developed.
- c. The market forces should be left to define the models for growth.
- d. There should not be any mandate on data or server localization.
- e. There should not be any restrictions on cross border data flow
- f. If there is a case for incentivizing those setting up servers in country, it should be done based on clearly defined parameters.
- g. Location of a server has got no relationship of its security.
- h. If there are security concerns, those need to be spelt clearly so that industry and Government can work together to arrive at plausible solutions.