COUNTER COMMENTS

CONSULTATION PAPER ON CLOUD COMPUTING

Following our initial comments on the Consultation Paper on Cloud Computing, below is our set of counter comments that serve as responses to the comments made by various stakeholders. Owing to the large volume of comments, our responses address four broad themes that were identified from the submissions made by major stakeholders:

- **Data localization:** Some TSPs have argued strongly in favor of data localization laws i.e. laws requiring businesses that collect and preserve digital data [including but not limited to cloud service providers (hereinafter referred to as "CSPs")], to retain such data within India's jurisdictional limits, rather than on servers in different nations. It has been argued that this is necessary mainly in the interests of security and legal compliance, and that CSPs must mandatorily provide for storage of Indian data in computer systems located within the geographical boundaries of India.

  It is our submission however, that mandatory localization of data (other than Government data) could prove counter-productive, and result in bringing the cloud to the ground while making the Internet less secure.[1] As pointed out in a report by the United States International Trade Commission, "localization requirements are problematic for cloud providers, as 'location independence' is a core aspect of the cloud delivery model. Policies that require providers to locate facilities in a given location may leave them with the choice of selecting a suboptimal location or not serving the target market at all."[2] While we certainly understand and appreciate all security/privacy concerns surrounding digital data, when dealing with

1 P. Ryan, S. Falvey and R. Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, Computer, vol. 46, No. 12 (2013), pp. 54-59, available at: http://research.google.com/pubs/pub42544.html

2 R. Berry and M. Reisman, *Policy Challenges of CrossBorder Computing*, J. Int'l Commerce and Economics, vol. 4, no. 2, 2012, pp. 1-38, available at: https://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf

technologies like cloud computing, it is important for the regulator to understand that data localization is far from a one-stop solution as data is not stored any safer merely by virtue of being located in a selected region. Not only would mandatory data localization be ineffective, but it would also deter crucial economic growth, affect competition, and hamper innovation,as most SMEs would be unable and/or unwilling to function in a country with such requirements due to the substantial complexities and costs involved.[3] Even larger businesses with vast financial reserves may find it difficult if not impossible to build and maintain servers in every country they serve so as to localize data.

Any concerns relating to obligatory data disclosures before foreign governments can be better allayed through international cooperation rather than isolation. The need of the hour is to keep our data secure by having an overarching privacy and data protection legislation coupled with effective enforcement and by the use of strong, open-source security and encryption technologies. In November 2013, Richard Salgado, Google's Director of Law Enforcement and Information Security, while testifying before the US Senate in support of the Surveillance Transparency Act of 2013, predicted that "if data localization and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces, with barriers around each of the splintered Internets to replace the global Internet we know today."[4] If we do not push towards the right kind of policies that enshrine privacy and data protection for our citizens, the free flow of data on a neutral and open Internet would be

3 M. Bauer, H. L. Makiyama, E. V. D. Marel and B. Verschelde, *Data Localisation in Russia: A Self-imposed Sanction* – European Centre For International Political Economy Policy Brief, no. 6, 2015, available at: http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/

4 Written Testimony of Richard Salgado Director, Law Enforcement and Information Security, Google, Inc., *Senate Judiciary Subcommittee on Privacy, Technology and the Law Hearing on "The Surveillance Transparency Act of 2013"*, November 13, 2013, available at: https://services.google.com/fh/files/blogs/google_testimony_transparency_nov132013.pdf

hampered, and Salgado's prediction of the Internet becoming a 'splinternet' may very well become a reality.

- **Sectoral laws for cloud computing:** Various stakeholders have suggested that there is a need for separate sectoral laws to regulate CSPs, including in some cases, light-weight licensing regimes. Some have even recommended that there be a regulatory body like TRAI for dealing with issues and challenges pertaining to cloud computing. However, we do not agree with this view.

  We firmly believe that cloud computing needs neither sectoral laws nor a licensing regime – light-weight or otherwise. As CSPs provide content and services over licensed pathways owned and operated by TSPs, all content and services should be allowed to freely pass over these pathways with no application-specific discrimination. There are no technical distinctions among data packets on account of the content they carry, and by logical extension, there is no reason to treat them differently. Moreover, a licensing regime for cloud computing will bring significant operational hurdles, as if each country starts adopting such a stance a CSP will have to obtain license from each and every country.

  As we have already pointed out in our comments to this consultation paper, the CSPs are already regulated by a number of general and specific legislations that prescribe numerous general, technical, financial and security related conditions that they must necessarily comply with. Some of the existing legislations that apply to cloud providers are:

  - Information Technology Act, 2000
  - Consumer Protection Act, 1986
  - Payment and Settlement Systems Act, 2007

- Indian Copyright Act, 1957
- Income Tax Act, 1961
- Customs Act, 1962
- Central Excise Act, 1944
- Foreign Exchange Management Act, 1999
- Prevention of Money Laundering Act, 2002

Thus, as CSPs are already regulated under the above legislations, we submit that additional regulatory frameworks would be excessive and would only serve to hinder the growth of cloud computing in India.

- **Registration of cloud service providers as OSPs:** Some stakeholder associations have suggested that CSPs must be required to register as Other Service Providers (hereinafter referred to as "OSPs"). This recommendation is made with the apparent intention of categorizing them under an existing regulatory framework, thus bringing in an additional layer of accountability and oversight. However, it is our considered view that such a categorization, besides being fundamentally ill-suited for the cloud computing industry, would impose excessive regulatory hurdles and hinder the growth of cloud computing in the country.

  OSPs traditionally signify entities that provide application services such as tele-banking, tele-medicine, tele-trading, e-commerce, call centre, network operation centre and other IT enabled services, by using telecom resources provided by TSPs. Upon analyzing the Terms and Conditions of OSP Registration[5], it comes to light that it does not, in any way take into

5 Revised Terms and Conditions of OSP Registration, issued by Department of Technology, dated 05.08.2008 as given at Annexure I, available at:

account the cloud providers and if they are forced to register as an OSP it will restrict and fragment the working of cloud providers. The following non-exhaustive list highlights clauses of the Terms and Conditions that can be considered problematic or seen as creating hindrance if the cloud providers are mandated to register as OSPs:

- For registration as an OSP, it is required that the applicant be a company registered under the Indian Companies Act, 2013 or an LLP (Limited Liability Partnership) registered under LLP Act, 2008[6] and thus excludes CSPs that may not be registered in India but nevertheless provide their services in India.
- Registration is location centric[7] (as it presumes that an OSP will provide services through establishing an OSP centre), which means a company that covers more than one state needs to have more than one registration. After getting the registration certificate for the first location, they have to apply again for registration for other sites to the respective designated authorities.[8]
- For an OSP to operate, they need to make use of the telecom resources from an authorized TSP[9], and registration mandates that no OSP will infringe on the jurisdiction of other authorized TSPs.[10] Thus a CSP that registers as an OSP, will further be prevented from offering services similar to those offered by the respective TSP, including but not limited to switched-telephony.
- OSP registration clearly did not intend to extend to CSPs, as evidenced by Chapter III of the Terms and Conditions, which specifies the that OSPs must at all times ensure that

http://www.dot.gov.in/sites/default/files/OSP%20registration070808.pdf

6 Amendment to Terms and Conditions for Other Service Provider (OSP) Category, issued by Department of Technology, dated 12.01.2016, available at: http://www.dot.gov.in/sites/default/files/u75/2016_01_13%20OSP-CS.pdf

7 Supra 5, Chapter II, Clause 1 (iv)

8 Supra 5, Chapter II, Clause 1 (v) (b)

9 Supra 5, Chapter III, Clause 1 (1)

10 Supra 5, Chapter II, Clause 1(1)

there is a logical separation between the telecom resources for OSP and the telecom resources for their other activities and that there can be no voice/non-voice traffic flow between them.[11]

- Interconnectivity between international and domestic OSPs is not permitted.[12] In cases where infrastructure is to be shared between international and domestic OSPs, it will be subject to prior written approval from the regulator[13] and other conditions such as tender of Bank Guarantees of Rs 50 lakhs or 1 crore depending on the respective terms of registration.[14]

Thus, CSPs should not be asked to register themselves as OSPs as the resulting obligations would be detrimental to CSPs and would have a direct impact on start-up companies and new entrants, who will be forced to comply with regulatory costs over-and-above the costs of incorporation and conduct of business. Over-regulation would therefore inevitably come with hurdles that threaten innovation and progress.

- **Adequacy of existing privacy, data security laws:** Certain stakeholders have suggested in their submissions that existing privacy/data security laws, coupled with contractual privacy/security obligations, are quite sufficient to ensure comprehensive protection of digital data.

We wish to reiterate in response that India currently lacks an overarching law on privacy and data protection. Although there are certain provisions under the Information Technology Act, 2000 that seek to govern the handling of personally identifiable information and sensitive personal data, their limited scope of application leaves much to be desired. To illustrate, with

11 Supra 5, Chapter III, Clause 1(5)
12 Supra 5, Chapter III, Clause 1(6)
13 Supra 5, Chapter IV, Clause 1
14 Supra 5, Chapter IV, Clause 2(b)

respect to personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 merely mandate the existence of a privacy policy with certain clauses, but fails to expand on the principles that need to be followed for the collection, storage, use, access of the data provided by the user.

Even though there have been efforts towards drafting a privacy legislation, an ongoing process for the past 6 years no concrete bill has been laid down in front of our Parliament for consideration. Therefore, the Indian legal system lacks a comprehensive data protection framework that lays down the rights of the users with respect to their data, responsibilities of the data handlers, clear details about security and encryption protocols, or transparency and accountability measures. With the Government rolling out initiatives like Digital India to promote the digital culture and its proliferation across the country, the digital footprint of every user, in rural or urban areas, is expanding substantially and thus, there is a very strong need to have an overarching law on privacy and data protection in India.

The diversity of legal mechanisms (or lack thereof), and their differing application across countries have raised difficulties surrounding the effective transmission and storage of data. While encouraging the use of cloud services in the country, it is important to ensure that there are regulations in place that clarify the principles that should be followed by CSPs while collecting, retaining and handling user data, and shifting it from one jurisdiction to another. In India, the lack of an overarching and comprehensive privacy and data protection law makes it difficult to evaluate adequacy of other countries wherein the data of Indian citizens would be transferred through these CSPs. An effective privacy and data protection regime is also a pre-requisite for cloud service providers to have their data centers located here so that data of citizens from countries with strict data protection laws can be transferred

here. The efforts for finalizing a law on these lines are underway, and we hope that it includes a provision for efficient & secure cross border transfer of data among other things.