call: +91-22-2598-3456 email: iMeet@ijunxion.com

January 21, 2019

Submitted by: Mr. Dhananjay Saheba, 9223-405-539, d.saheba@ijunxion.com

Re: Counter Comments on Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services (Nov 12, 2018)

On Regulation

Regulators, around the world, have awesome powers. Essentially they are prosecutors, judge, and jury in many matters – witness the imposition of fines to the tune of over Rs. 3,000 crores in the dispute over interconnection of Reliance Jio with other service providers.

Very importantly there are few tools available to regulators to assess the outcome of regulations which can be both good and bad:

- When the need arose to bypass the ADC regime to enable international BPOs to operate in India a new category of service provider – OSP – was created. This resulted in thousands of mini TSPs, bypassing of the existing telecom networks, and a massive revenue windfall for equipment makers. If on the other hand access providers and ILD providers had been allowed to work together to create a "parallel" network for such services with adequate safeguards the same objective would have been achieved with significant revenue gains for TSPs. The fracturing of the network and the need on the part of the BPOs to create special infrastructure probably also affected the competitiveness of India as an international BPO destination.

Comments, suggestions, etc. to regulators are naturally coloured by the self-interest of the commenters and need to be evaluated with care:

- When BSNL launched an access-network-independent VoIP service it was barred primarily because of objections of other service providers. A couple of years later, once Reliance Jio entered the market, the same (or at least similar) service has been allowed.

On Reliance Jio's recommendations regarding Lawful Interception

In India lawful interception can only be done by around 10 agencies specifically notified by the Government of India. Very interestingly none of these agencies seem to have responded to the issue raised by this consultation. Furthermore, most of the concerns regarding criminal communications around the world cited by Reliance Jio appear to refer to legislatures not regulators. Very properly these issues should be discussed and acted upon by the Indian parliament not mandated by TRAI.

The underlying statistics also belie Reliance Jio's claims: On Dec. 23, 2018 The Times of India (Mumbai) reported under the tagline "9K phones, 5000 email interceptions under UPA govt.: RTI" that in 2013: '"On an average, between 7,500 and 9,000 orders for interception of telephones are issued by the central government every month. On an average between 300 to 500 orders for

interception of emails are issued by central government per month" government told RTI applicant, Delhi resident Prosenjit Mondal in 2013'. Even if these numbers have grown 10-fold in the last 5-6 years to 1 lakh requests per month, with over 1 billion phones in operation across India the overwhelming majority of Indians are not criminals, as Reliance Jio seems to imply, with its suggestion that every single communication over the network needs to be monitored.

Some statistics on WhatsApp (https://expandedramblings.com/index.php/whatsapp-statistics/)

Item	Value	As of
How many people use WhatsApp?	1 billion	Jan 31, 2018
Average number of daily voice calls made on WhatsApp:	100 million	Jun 23, 2016
Amount of time spent by WhatsApp users making calls on it each day	2 billion minutes	July 31, 2018
Number of messages sent via WhatsApp daily	65 billion	May 18, 2018

I have been unable to determine the number of employees at WhatsApp currently. However in early 2014 when it was acquired by Facebook it had only 55 employees. Thus even if it has grown manifold to say 1,000 employees the messaging traffic alone amounts to 65 million messages per day per employee. Clearly the task of monitoring every single communication and reporting "suspicious" activity to law enforcement is not practicable.

The US regulation, CALEA, on LIM requires network access providers (essentially service providers who provide "access identifiers" such as phone numbers and IP addresses) to enable law enforcement agencies to intercept communications traffic as needed. Very critically the traffic to be monitored must be delivered to law enforcement agencies to a place of the law enforcement agencies' choice. According to Wikipedia: **By law this must be outside of the phone company. This prevents law enforcement from being inside the phone company and possibly illegally tapping other phones.** Furthermore, best I can tell, CALEA does not apply to OTT players such as Facebook, Twitter, Gmail, Youtube, and WhatsApp as cited by Reliance Jio in its quote of an affidavit filed by the Chennai Police. Nor does CALEA require users and/or applications/service providers to deposit decryption keys with law enforcement agencies.

The vast number of users in India for OTT players clearly indicates that these applications provide enormous value to users in India. This also makes India an attractive market for such players. The onerous conditions suggested by Reliance Jio are likely to make India even more unattractive to invest in, especially in telecom:

> *14 b. Restriction of sending user information abroad and mandatory local hosting of all critical subscriber data.*
>
> *14. c. Right to inspect the source code, network or technology layer used for extending the service by the Licensor*
>
> *14. e. Sharing of decryption keys with the Licensor for all bulk encryption deployed in the country*
>
> *15. b OTT Communication service providers should be responsible for monitoring unlawful content on their platform.*

Without encryption the Internet would be pretty useless, especially for financial transactions. In any event ordinary users and citizens of India have an absolute right to encrypt their communications. Reliance Jio's suggestion is equivalent to asking every lock maker in India to deposit duplicates of all keys with law enforcement agencies so they can break into any premise! It is also noteworthy that CALEA in the US does not seem to have such a requirement.

The last cited recommendation by Reliance Jio would make every service provider merely because they have a telecom related license a law enforcement agent. In the interest of a level playing field then telecom service providers should be subject to monitoring by ordinary citizens. I seriously doubt that Reliance Jio would agree to have all its activities monitored by ordinary citizens. On a more serious note this recommendation implies that Reliance Jio should be given a legal mandate to spy on the users – the government, competitors, and even ordinary citizens – of its network and services.