**Reliance Communications Limited's Response to the Consultation Paper on Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications**

## Executive Summary

A. **The framework for introduction of M2M Service providers should be through registration similar to OSP registration category with some additional mandatory obligations.**

B. **The definition of end user of M2M services should be described in terms of the devices as well as the human owner.**

C. **There is a need to define obligations for the MSPs (KYC of the OEMs, provisioning of traceability and monitoring facilities to the LEAs, privacy of human end user's of M2M services) as well as the OEMs (mandatory KYC of the end user devices) who avail the services from the MSPs and provide the devices to the customers.**

D. **The provisioning of end to end M2M services, especially for Indian customers, should be mandated from within Indian territory, i.e. the M2M services It Application, their Data base and management setups should be hosted locally in India and that they should be mandated to use Indian TSPs SIMs.**

E. **The obligations for Entry Fee, Performance Bank Guarantee (PBG) or Financial Bank Guarantee (FBG), etc should be similar to OSP registration.**

F. **No separate quantum of spectrum is required to meet the M2M communications requirement.**

G. **No specific spectrum band(s) can be attributed as being more suitable for M2M communication.**

H. **No portion of the 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) should be used separately for M2M communications.**

I. **It is not advisable to delicense any more bands for general public use. Instead, nominal charges, on the lines of charges recommended by TRAI for the usage of 'E' and 'V' band in its "Recommendations on Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers", should be implemented.**

J. **National roaming for M2M / IoT devices should be free.**

K. **Use of only domestic TSP SIM / eUICC should be mandated for use in M2M / IOT services being provisioned in India.**

L. **As a policy, roaming on permanent basis should not be allowed for foreign SIM / eUICC.**

M. **If the M2M devices are to be used in India for more than 1 year's duration, then the SIMs of foreign TSPs should be mandated to be converted to domestic TSP SIMs within a period of 1 year from the date of activation of the device in India.**

N. **It is ideal that the tariffs for international roaming be negotiated mutually between the roaming partners and the MSPs to enable extraction of the best price for the roaming charges of the M2M devices.**

O. **Separate allocation of MNCs should not be done for the MSPs.**

P. **Provisioning free roaming for M2M services would provide the operational and roaming flexibility for M2M services sans the complexity and cost of deploying the switch and the HLR.**

Q. **The existing measures taken for security of networks and data would not be adequate for security in M2M context. India should have maximum possible number of "Mutual Legal Assistance" agreements for getting information from M2M services setups hosted in cloud setups outside of India's territorial boundaries.**

R. **There is no need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets) as well as any distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network.**

Our specific comments on the issues posed by the Authority are given in the subsequent paragraphs.

**Detailed Response**

**Q1. What should be the framework for introduction of M2M Service providers in the sector? Should it be through amendment in the existing licenses of access service / ISP license and / or licensing authorization in the existing Unified License and UL (VNO) license or it should be kept under OSP Category registration? Please provide rationale to your response.**

**Q2. In case a licensing framework for MSP is proposed, what should be the Entry Fee, Performance Bank Guarantee (if any) or Financial Bank Guarantee etc? Please provide detailed justification.**

**Q3. Do you propose any other regulatory framework for M2M other than the options mentioned above? If yes, provide detailed input on your proposal.**

**Our Response**

**The framework for introduction of M2M Service providers should be through registration similar to OSP registration category with some additional mandatory obligations.**

**The obligations for Entry Fee, Performance Bank Guarantee (PBG) or Financial Bank Guarantee (FBG), etc should be similar to OSP registration.**

1. The present licensing and regulatory regime is totally focused on provisioning of Voice and Data service for usage by humans. Accordingly, it covers issues such as customer acquisition, their KYC, customer data retention and sharing, security and LEA requirements, QoS compliances, tariff controls, roaming, etc. However, M2M services encompass a plethora of other services that have evolved from the IT domain.

2. The Consultation Paper (CP), at para 2.4 page 15, has listed 7 business models of M2M service providers. It is observed that out of these only the 'underlying network', listed in the last M2M business model that is presently under licensing regime. The balance, i.e. first 6 of these M2M business models cover areas such as devices, gateways, platforms and applications which predominantly belong to the IT domain and are hence totally out of purview of the existing licensing regime.

3. The innovation of services, be it in the telecom domain or the IT domain, evolved from the needs of the society. The experience of the past decade and a half shows that the deployment and availability of IT domain services was possible due to the lack of a formal policy framework for provisioning of these services. The prevalent framework for IT domain services is for OSP registration. Since most of the business models for M2M services have a predominance of IT services and that the majority of end user of the M2M services shall be machines, **there is a strong case for adoption of the registration framework to be persisted with for M2M Service Providers (MSP).**

4. M2M services are distinguished from the classical Telecom services from the facts that,

a. The M2M service provider has a B2B business model with the TSP as well as the OEM instead of the direct B2C business model of a TSP. E.g. M2M service provider sourcing SIMs, in bulk, from the TSP for connectivity between his servers and the end devices and providing these SIMs as part of M2M services' integrated solution to the OEMs.

b. In the B2B model, there are use cases wherein the M2M services are prepaid by the OEM for lifelong services and the end user just enjoys the utility of the service. E.g. A car manufacturer paying upfront for the M2M services, for the next 10 to 15 years, to the M2M service provider for integrating the M2M service provider's SIMs into the cars or Amazon having a worldwide 3G connectivity contract for its Kindle devices.

c. Unlike the Telecom services where the SIMs are directly associated with the user, the SIMs have an indirect relationship with the user and the relationship can change hands after the original user undertakes a second hand transaction. E.g. A M2M service enabled white good being resold by its original buyer or the SIM fitted car getting resold to another user.

5. In the scenarios described above, it is suggested that the definition of end user of M2M services should be described in terms of the devices as well as the human owner.

This would be required to accommodate the requirement of B2B as well as B2B2C services and transactions of the MSPs. Consequently, instead of burdening the M2M service provider with obligations similar to those of the Telecom domain, which has the potential to stifle the proliferation of M2M services itself, **there is a need to define obligations for the MSPs as well as the OEMs who avail the services from the MSPs and provide the devices to the customers.** Suggested obligations of the MSPs and OEMs are as given below,

a. **MSPs.**

   i. Ensuring the KYC of the OEM who avails the services of the M2M Service provider.

   ii. Provisioning of the M2M device usage information to the LEA for traceability and monitoring purposes.

   iii. Protection of privacy of human end user's of M2M services.

   iv. B2B services sales contracts to mandatorily have requisite SLAs for the B2C KYC of the end user utilizing the M2M services.

b. **OEMs.** Ensuring the KYC of the customer who avails the M2M services post the sale or resale of the device.

6. The CP, at para 2.5 on page 16 has highlighted the case of electronic signboards being subjected to hacking and subversive use. The scenario has been used to advocate the deployment of "dedicated network infrastructures and services that are reliable and secure". Firstly, it is brought out that the deployment, operations and maintenance of a physically separate and dedicated network for M2M service shall not be an economically viable option. Secondly, there exist adequate security solutions, including virtual separation of the networks through creation of private APNs, for ensuring separation and security of the network applications. However, from latency and security perspective it is imperative that the applications and the data base of these applications, especially of those M2M services which capture an individual's information, should be stored locally in a secure environment. It is equally important that this data base, its encryption algorithms and physical infrastructure should be easily accessible to the LEAs in India. In view of the criticality of latency and security requirements for a country like India which is at the receiving end of terrorist actions and is potentially one of the largest markets of M2M services, it is suggested that **the provisioning of end to end M2M services, especially for Indian customers, should be mandated from within Indian territory, i.e. the M2M services It Application, their Data base and management setups should be hosted locally in India and that they should be mandated to use Indian TSPs SIMs.**

**Our Recommendations**

7. In view of the foregoing, our recommendations are as given below,

a. **Registration framework should be adopted for M2M Service Providers (MSP).**

b. **The definition of end user of M2M services should be described in terms of the devices as well as the human owner.**

c. **There is a need to define obligations for the MSPs (KYC of the OEMs, provisioning of traceability and monitoring facilities to the LEAs, privacy of human end user's of M2M services) as well as the OEMs (mandatory KYC of the end user devices) who avail the services from the MSPs and provide the devices to the customers.**

d. **The provisioning of end to end M2M services, especially for Indian customers, should be mandated from within Indian territory, i.e. the M2M services It Application, their Data base and management setups should be hosted locally in India and that they should be mandated to use Indian TSPs SIMs.**

e. **The obligations for Entry Fee, Performance Bank Guarantee (PBG) or Financial Bank Guarantee (FBG), etc should be similar to OSP registration.**

**Q4. In your opinion what should be the quantum of spectrum required to meet the M2M communications requirement, keeping a horizon of 10-15 years? Please justify your answer.**

**Q5. Which spectrum bands are more suitable for M2M communication in India including those from the table 2.3 above? Which of these bands can be made delicensed?**

**Q6. Can a portion of 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) be used for M2M communications as delicensed band for short range applications with some defined parameters? If so, what quantum? Justify your answer with technical feasibility, keeping in mind the interference issues.**

**Our Response**

**No separate quantum of spectrum is required to meet the M2M communications requirement.**

**No specific spectrum band(s) can be attributed as being more suitable for M2M communication.**

**No portion of the 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) should be used separately for M2M communications.**

1. M2M services have evolved as part of the internet eco-system. As brought out in our response to question Nos 1, 2 and 3, the M2M services eco-system encompasses IT devices, gateways, platforms and applications. The devices, gateways and platforms of the internet are sewn into a coherent system by attaching them as nodes of the network. The provisioning and access to the applications is made available to the users over this underlying network. Therefore, **for the M2M services to be enabled and provisioned, availability of an underlying network is indispensable.**

2. In India, mobile services network is the predominant network that provides almost ubiquitous connectivity across the length and breadth of the country. The mobile network is supplemented by other LANs / PANs / HANs for enhancing their reach within a small area like a building / for covering coverage gaps. In addition, the terrestrial network is laid for supporting the backhaul connectivity of the mobile network.

3. It is well known fact that establishment of a heterogeneous network of the magnitude and scale to cover an area as big as India as well as within the buildings requires substantial investments. It is once again reiterated that the deployment, operations and maintenance of a physically separate and dedicated network for M2M service shall not be an economically viable option. Therefore, **it is not advisable to allocate / earmark separate spectrum, especially for M2M services.** Moreover, M2M services would be provisioned over multiple hops comprising of multitude of existing access networks, including land lines, or the devices with mobility would access services through connectivity over multiple existing networks. With technologies like Carrier Aggregation (CA) becoming the norm, **segregation of a single spectrum exclusively for M2M services would be a retrograde step and hence not advisable.**

4. Also, given the fact that the, existing delicensed bands have started experiencing extensive interference due to their unregulated use and has led to decrease in QoS of the services provisioned through them. Therefore, **it is not advisable to delicense any more bands for general public use. Instead, nominal charges, on the lines of charges recommended by TRAI for the usage of 'E' and 'V' band in its "Recommendations on Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers", should be implemented.**

**Our Recommendations**

5. Summary of our recommendations are as follows.

   a. **No separate quantum of spectrum is required to meet the M2M communications requirement.**

   b. **No specific spectrum band(s) can be attributed as being more suitable for M2M communication.**

   c. **No portion of the 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) should be used separately for M2M communications.**

   d. **It is not advisable to delicense any more bands for general public use. Instead, nominal charges, on the lines of charges recommended by TRAI for the usage of 'E' and 'V' band in its "Recommendations on Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers", should be implemented.**

**Q7. In your opinion should national roaming for M2M / IoT devices be free? (a) If yes, what could be its possible implications? (b) If no, what should be the ceiling tariffs for national roaming for M2M communication?**

**Our Response**

**Yes, National roaming for M2M / IoT devices should be free.**

1. Devices in the M2M services eco-system would either be totally static (E.g. Electricity Meters, Smart city sensors, etc) or nomadic (E.g. White goods, Home automation, etc) or are mobile within the telecom circle or inter circle (E.g. Cars, personal healthcare sensors, smart transportation solutions, etc). It is observed that the nomadic and mobile devices closely match the characteristics of the existing roaming requirements of the voice and data services. The points of difference however are in terms of,
   a. The amount of data volume that would be exchanged between the devices and the frequency of this data exchange vis-a-vis what is experienced between human interactions.
   b. The M2M services are predominantly data enabled, though SMS too is used for sending information from the device to the application server. They have the ability to make use of the existing voice and messaging channels but on their own they are data services. Voice is primarily used for providing feedback / alerting during an emergency.
2. Since **all operators are providing free domestic roaming for their data services, it is logical that the free national roaming facility is extended for the M2M services as well.**

**Our Recommendations**

3. It is recommended that,
   a. **All operators should be mandated to configure national roaming for M2M / IOT services.**
   b. **National roaming for M2M / IoT devices should be free.**

**Q8. In case of M2M devices, should;**

**(a) Roaming on permanent basis be allowed for foreign SIM / eUICC; or**

**(b) Only domestic manufactured SIM / eUICC be allowed? And / or**

**(c) There be a timeline / lifecycle of foreign SIMs to be converted into Indian SIMs / eUICC?**

**(d) Any other option is available?**

**Please explain implications and issues involved in all the above scenarios.**

**Q9. In case permanent roaming of M2M devices having inbuilt foreign SIM is allowed, should the international roaming charges be defined by the Regulator or it should be left to the mutual agreement between the roaming partners?**

**Q10. What should be the International roaming policy for machines which can communicate in the M2M ecosystem? Provide detailed answer giving justifications.**

**Our Response**

**No, roaming on permanent basis should not be allowed for foreign SIM / eUICC.**

**Yes, use of only domestic TSP SIM / eUICC should be mandated for M2M devices being used in India for more than 1 year duration.**

**The foreign SIMs should be mandated to be converted to Indian SIM / eUICC within a period of 1 year.**

**The international roaming charges should not be defined by the Regulator. It should be left to the mutual agreement between the roaming partners and MSPs.**

1. 'Data', has not only become a source of discerning patterns for business intelligence, but it is also being exploited for understanding national policy requirements. The statement in the CP at para 2.44 (ii) on page 36, "M2M will enable creation of a wealth of information covering various aspects of economy and society which will have immense potential use for public welfare but at the same time it can give rise to privacy concerns of individuals", needs to be taken serious note of for ensuring not only the privacy of individuals but the security of the country as well. It is envisaged that in the future, voluminous data could / would be the currency for holding a country to ransom, especially if the country hosting the data / the MSP's ownership changes hand / MSP decides to move his data hosting setup to a country that is inimical to India's interests.

2. As brought out in our response to questions 1, 2 and 3, the political volatility of the Indian Sub-continent region forces India to take certain steps for ensuring its territorial integrity and the security of its citizens. It is our belief that it is because of these reasons that the licensing conditions of the TSPs mandate that the data pertaining to the subscribers shall remain within the territorial boundaries of India. Since, the usage of M2M services closely shadow their owners' characteristic, it is suggested that **the end to end M2M services setup, for provisioning M2M services in India, should mandatorily be hosted in India.**

3. India is not only one of the fastest growing telecom markets of the world but it is one of the fastest growing economies as well. One of the major consequences of this rapid growth is that it will lead to a commensurate increase in the consumption of M2M services and devices. Therefore, purely from an economic point of view, it makes sense to mandate the use of domestic TSP SIMs for the devices being used in India. However, given the limited technological and manufacturing base of India, and the fact that India is endeavouring to become a global manufacturing hub, mandating use of only Indian TSP SIMs could have a reciprocal effect on the goods that are manufactured and exported from India. Therefore, it mandates a balanced approach towards permitting foreign SIMs in M2M service devices imported to India. Therefore, it is suggested that **if the M2M devices are to be used in India for more than 1 year's duration, then the SIMs of foreign TSPs should be mandated to be converted to domestic TSP SIMs within a period of 1 year from the date of activation of the device in India.**

4. Additionally, given the envisaged scales of service provisioning in India, it is submitted that mutual agreements between the roaming partners and the MSPs would be able to extract the best price for the roaming charges of the M2M devices. Therefore, **it is**

**ideal that the tariffs for international roaming be negotiated mutually between the roaming partners and the MSPs.**

**Our Recommendations.**

5. In view of the foregoing, our recommendations are as given below.

   a. **Use of only domestic TSP SIM / eUICC should be mandated for use in M2M / IOT services being provisioned in India.**

   b. **As a policy, roaming on permanent basis should not be allowed for foreign SIM / eUICC.**

   c. **If the M2M devices are to be used in India for more than 1 year's duration, then the SIMs of foreign TSPs should be mandated to be converted to domestic TSP SIMs within a period of 1 year from the date of activation of the device in India.**

   d. **It is ideal that the tariffs for international roaming be negotiated mutually between the roaming partners and the MSPs to enable extraction of the best price for the roaming charges of the M2M devices.**

**Q11. In order to provide operational and roaming flexibility to MSPs, would it be feasible to allocate separate MNCs to MSPs? What could be the pros and cons of such arrangement?**

**Our Response**

**No separate allocation of MNCs to MSPs is neither feasible nor should it be done.**

**Operational and Roaming flexibility for M2M services would be best provided through mandating free national roaming.**

1. As is seen from the figure 2.1 at page 15 of the CP (Reproduced on the next page for ready reference), the Network Services are the underlying end to end binding infrastructure for the M2M services. The scenario here is similar to that of MVNO wherein the underlying network numbering resources are being used for provisioning services. Hence, **it is important that the numbering resources, for the M2M services too, are provisioned through the underlying NSOs only.**

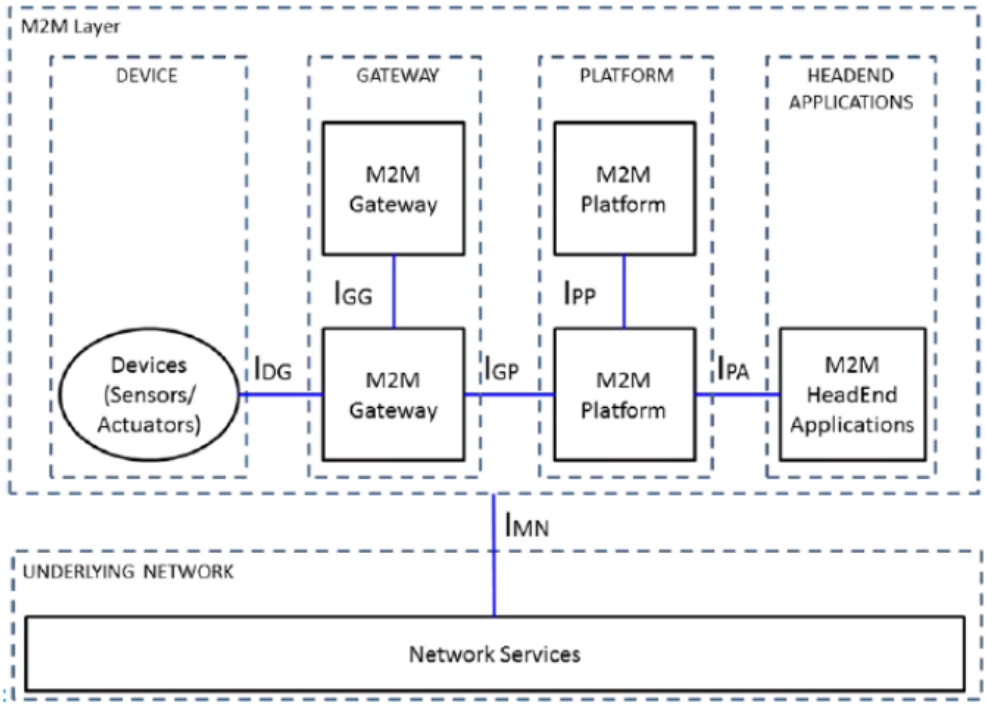


**Figure : Showing A generic M2M Network architecture model**

Source : Figure 2.1 at Page 15 of the TRAI CP on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications

2. The Public Land Mobile Network (PLMN) or Home Network Identity (HNI) which is a combination of Mobile Country Code (MCC) and MNC is used to fully identify a mobile subscriber's 'Home Network'. Identification of the home network of the subscriber enables availability of additional information through the home networks' Home Location register (HLR) for local copying in the Visitor Location Register (VLR). Provisioning of exclusive MNCs to the MSPs would entail,

   a. Either deployment of the entire HLR infrastructure by the MSP thereby requiring substantial investments and extensive roaming agreements with various TSPs.

   b. Or it would require the MSP to ensure that it's International Mobile Subscriber Identity (IMSI) (HNI is part of the IMSI) is available in HLRs of multiple operators. Firstly, undertaking such an exercise of getting entries made into HLRs of so many operators would be highly complex and humungous task. Secondly, it would create problems of routing as the HNI of one network would point to multiple networks. In order to obviate this problem, the MSP would be required to deploy its own switch as well to create a separate network, thereby escalating the cost of services further.

3. As brought out in our responses to earlier questions, M2M services have evolved as an innovation of the data services at a fraction of the complexity and cost of deploying even the HLR. Since all operators provide free roaming for data services in the country therefore, it is submitted that **provisioning free roaming for M2M services**

**would provide the operational and roaming flexibility for M2M services sans the complexity and cost of deploying the switch and the HLR**

**Our Recommendations**

4. In view of the foregoing our recommendations are as follows,

   a. **Separate allocation of MNCs should not be done for the MSPs.**

   b. **Provisioning free roaming for M2M services would provide the operational and roaming flexibility for M2M services sans the complexity and cost of deploying the switch and the HLR.**

**Q12. Will the existing measures taken for security of networks and data be adequate for security in M2M context too? Please suggest additional measures, if any, for security of networks and data for M2M communication.**

**Q13. (a) How should the M2M Service providers ensure protection of consumer interest and data privacy of the consumer? Can the issue be dealt in the framework of existing laws? (b) If not, what changes are proposed in Information Technology Act. 2000 and relevant license conditions to protect the security and privacy of an individual? Please comment with justification.**

**Our Response**

**No, the existing measures taken for security of networks and data would not be adequate for security in M2M context.**

**No, the issue cannot be dealt in the framework of existing laws.**

1. M2M services are a combination of the telecom services and IT services. M2M services are provisioned from a cloud setup that is location agnostic across the globe. Therefore, the security requirements for M2M service shall necessarily have to be a combination of security measures enunciated for the telecom domain, IT domain as well as the cloud computing domain.
2. **Telecom Domain.** It is felt that some of the security measures, of the telecom domain, such as KYC of the end users, activation, deactivation, profiling and change of SIMs, change of support to LEAs would have to be obligated on the MSPs as well. Additionally, adequate security measures for soft SIMs and embedded SIMs shall have to be formulated and notified.
3. It is brought out that the TSPs have unanimously recommended and the DoT's draft registration guidelines for MSPs have fixed the responsibility for customer verification and traceability on the MSPs viz, "M2MSP shall adhere to Know Your Customer (KYC) and traceability guidelines issued by the Authority to Telecom Licensees from time to time for all Telecom resources including SIM enabled devices." Therefore, it is suggested that **these guidelines of fixing the responsibility for customer verification and traceability, on the MSPs, should be persisted with.**

4. **IT and Cloud Computing Domain.**

a. It is submitted that the existence of a light touch regulatory regime has facilitated growth of innovative IT and Cloud based services, of which M2M is also a subset. Therefore, it is most desirable that a similar regime be persisted with. In India, following general and specific legislations prescribe various general, technical, financial, and security related conditions for the IT and Cloud Service Providers.

i. Income Tax Act, 1961.

ii. Consumer Protection Act, 1986.

iii. Payment and Settlement Systems Act, 2007.

iv. Indian Copyright Act, 1957.

v. Central Excise Act, 1944.

vi. Prevention of Money Laundering Act, 2002.

vii. Information Technology Act, 2000.

viii. Foreign Exchange Management Act, 1999.

ix. Customs Act, 1962.

b. Since M2M services are location agnostic across the globe, there is a need to developed mechanisms for cooperating informally or, alternatively, resorting to what is typically referred to as requests for "Mutual Legal Assistance" for requesting and obtaining evidence for criminal investigations and prosecutions from a foreign sovereign state. Though India has MLAT agreements with 38 countries, as listed on the CBI site[1], M2M services availability shall mandate more of such MLATs.

c. On 15 Jul 16, in a judgement in a US appeals court, Microsoft was exonerated for refusing to give police user data stored overseas even when the data sought belonged to a drug trafficker. The court categorically told the police that "the Stored Communication Act (SCA) does not give US courts authority to force internet companies in the United States to seize customer email contents stored on foreign servers." Microsoft's case was being supported by the Information Technology and Innovation Foundation, a Washington-based tech policy think tank who opined that "data stored in other countries should be sought under auspices of a Mutual Legal Assistance Treaty designed to let police agencies around the world to help one another". As per an article[2] of The Channel News Asia, "the US has such mutual assistance treaties with more than 50 countries, including Ireland".

d. Therefore, MLATs apart, assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. To obviate such situations,

[1] http://cbi.nic.in/interpol/mlats.php
[2] http://www.channelnewsasia.com/news/business/microsoft-wins-appeal-to/2958542.html

especially if the data hosting country is not inclined to India's interests, local hosting of servers and storage should be mandated for those MSPs. India is the fourth largest country in terms of Internet users in spite of having an Internet penetration of a measly 6.9%[3]. Therefore, India is in the envious position to be able to leverage its market size for making other jurisdictions to legislate similar laws to ensure the security and privacy of data of its citizens and also force the MSPs to host their applications in local data centers.

5. Further in-depth details of the requirement of securing data of M2M services and ensuring privacy of the users data, have been provided in our response to the TRAI's CP on Cloud Computing submitted on 05 Sep 16.

**Our Recommendations**

6. In view of the above our recommendations are as follows,

   a. **The existing measures taken for security of networks and data would not be adequate for security in M2M context. India should have maximum possible number of "Mutual Legal Assistance" agreements for getting information from M2M services setups hosted in cloud setups outside of India's territorial boundaries.**

   b. **MSP registration framework should have obligatory clauses for mandatory KYC of the users of their services and owners of the end user devices, provisioning of traceability and monitoring facilities to the LEAs, privacy of human end user's of M2M services.**

   c. **India should mandate provisioning of end to end M2M services from locally hosted setups.**

**Q14. Is there a need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets)? What parameters must be considered for defining such SLAs? Please give your comments with justifications.**

**Q15. What should be the distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network?**

**Our Response and Recommendations**

**No, there is no need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets) as well as any distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network.**

1. In the era of cloud computing, humans are utilizing a plethora of applications through their user devices with ease. The connectivity between the user's device and the cloud computing based application infrastructure is established over HetNets. The fact that cloud infrastructure services have been adopted extensively bears testimony to the end-to-end network performance being well within the stipulated access duty cycle. It is brought out that the scenario for M2M services would be similar to the one

[3] http://royal.pingdom.com/2010/07/27/top-20-countries-on-the-internet/

described above, except that human intervention shall decrease to a large extent for some of the applications.

2. There is a symbiotic relationship between the network providers and the application providers as usage of the app firstly, depends on the access network and connectivity to the applications IT infrastructure and secondly, it leads to the utilization of the network resources thereby generating revenue for both. It is envisaged that defining QoS benchmarks for each and every transfer point between two networks, especially in a HetNet, would be highly complex and unwieldy for ensuring compliance. As has been brought out in numerous earlier representations to the Authority, it is in the network providers' interest that the M2M services utilise their network resources. Hence, the network providers would themselves ensure that the duty cycle remains within the applications latency sensitivity.
3. Additionally, it is brought out that the energy efficiency of the M2M devices is solely dependent on the frequency of feedback from the end devices. Therefore, the optimization of the services shall largely depend on the application that is deployed for provisioning the M2M services.
4. Hence, **there is no need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets) as well as any distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network.**