NASSCOM®

DSCI
PROMOTING DATA PROTECTION

Response to TRAI Consultation Paper On M2M Communications

Regulatory framework, spectrum, and service quality related requirements

January 2017

NASSCOM® DSCI PROMOTING DATA PROTECTION

NASSCOM-DSCI Response on TRAI Consultation on M2M Communications

Regulatory framework, spectrum, and service quality related requirements

Preamble

India and its development in the coming years now hinges irrevocably on Technology and its adoption in a safe and secure manner. M2M is therefore here to stay and disrupt.

The Internet of Things or M2M, in its simplest formulation, involves an increasing number of smart interconnected devices and sensors (e.g. cameras, biometric and medical sensors) that are often non-intrusive, transparent and invisible. Communication among these devices as well as with related services, may happen anytime, anywhere, it is frequently done over a variety of communication channels e.g. fixed and mobile communications systems, powerline communications, wireless, especially short-range wireless, technologies. For optimum development of the M2M, the resources necessary for connectivity must be ubiquitous.

Communications technologies for both fixed and mobile devices should enable low cost, reliable connectivity for even the simplest of devices.

The IoT / M2M architecture today, like the Internet, is growing in an evolutionary fashion. IoT also makes it simpler and necessary to collect, store, and search information that could include personal information. As a result, security and privacy concerns emerge.

The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures. Some connected devices are low-cost and essentially disposable. Therefore it may be difficult to update the software or apply a patch – or even to get news of a fix to consumers.

M2M devices are always connected and always on. In contrast to human-controlled devices, they go through a one-time authentication process, which can make them perfect sources of infiltration into company networks. Therefore, gateways that connect M2M devices to company and manufacturer networks need to be secured as well as the devices themselves.

Therefore implementing secure access control and device authentication seems to be an immediate solution. But the only long term solution is to drive standards based development to ensure interoperable secure systems.

TRAI/DOT should consider establishing a enabling environment to experiment with different security architectures, including proactive systems for self defence, both at network and device level.

M2M service providers today offer a gamut of services, as recognised in the draft. We believe that there is a need to clearly identify and articulate the specific function of the M2M service provider that should come under regulatory over sight.

Since much of the communication technology maybe outside of the telecom license regime, an information declaration, updation and event reporting mandate maybe considered for connectivity service providers, who are not already under the licensing regime. Anything more rigorous is likely to cause compliance and financial burden to this new segment.

India is on a threshold, with over 100 companies offering IoT solutions across various vertical domains. 70% of these companies have been set up in 2010 or later and the industry requires guidance and support as it aspires to capture 5% of the global market amounting to $20 billion by 2020.

Regulators can play a role in encouraging the development and adoption of the M2M, while promoting efficient markets and the public interest. Our responses, primarily centred around M2M service providers, are detailed below for your consideration.

RESPONSE TO QUESTIONS

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.

An IoT/M2M Platform could typically have the following typical elements (all or some of them)

1. Device Management – The following functions are fulfilled
   - Ensure the ongoing ability of the endpoint to receive and send data, including updates.
   - Device activation, certification, configuration, device monitoring, diagnostics, enablement, and provisioning/OTA software updates.
2. Connectivity Management – manage security, access for connected endpoints
   - Enable IoT service providers to manage security, access, maybe billing activities for connected endpoints.
   - Could include support for multiple connectivity protocols and varying levels of security services.
   - Connectivity management may include SIM management/gateway management, store and forward, monitoring and alarms, diagnostics, and reporting.
3. Application Management –reduce time, cost and complexity in development of applications
   - Enable development of horizontal and/or vertical applications typically via cloud-based APIs that leverage data generated by the connected endpoints in the IoT solution.
   - Application provisioning and application-level security services are key in this function
4. Reporting and Simple Analytics–making sense of IoT data for management decision
   - Allows end user to create automated, repeatable, and management-oriented summaries of M2M data.
   - Dashboard and reporting will include visualization tools, normalization of data in the cloud, and integration of data from/with enterprise systems or data in public clouds.

- Additional compute capabilities maybe offered to generate meaningful interpretation of the data, with fundamental contextualization for example, in social, real-time contexts etc.

As per the TEC report released in May 2015, a M2M Platform represents some common set of services which perform control, application support and management functions in a M2M service environment. e.g., Device management, Service management, Location management, Discovery, Application Routing, Security, Charging, Service Exposure APIs, etc.

This platform may support services catering to different vertical applications (Home, Health, Industrial Automation, Transport, Power, etc.)

Based on the commonly understood nomenclature of a M2M service provider as outline above, which is echoed in the TEC report released by Ministry of Telecom, it is important to identify the exact nature of services being offered by the service provider that would warrant regulations and monitoring.

The consultation paper suggests that such entities through which 'a hacker maybe able to penetrate into important establishments and pose a threat to national security triggered due to online systems' should have certain obligations cast upon it or be a registered entity.' (Ref 2.5, pp 16 of the consultation paper)

For a platform offering application management, dashboard and analytics services, there is no reason why they should be regulated and licensed. On the other hand, M2M service providers who offer device and connectivity management services, are key in the overall scheme of M2M connectivity and access.

Majority of M2M services globally are not being offered on telecom resources. Short range applications on RFID, ISM band are not covered under licensing norms in India.

We therefore suggest that

- The ISPs and TSPs are regulated entities under the current law. Therefore, any additional regulatory requirements should be applicable to only those entities who are not covered under the current licensing norms, and maybe offering dedicated network infrastructures and connectivity management services for M2M.
- Our recommendation is to restrict applicability of any regulatory compliance to only those entities that control access to devices. TRAI should clearly articulate the nature of services on offer that will entail regulatory obligations.
- Regarding the framework of regulation, we recommend the following:
- A simple online format should be made available for M2M service providers offering connectivity management services to share information

- This information will mandatorily require an update from the service providers every 6 months.
  - In this context it is important to mandate obligations for reporting any security breaches that may happen on the platform within a specified time frame of the event, with details of action taken etc.
  - The DoT will have rights to seek more details and information on such events and if required, issue advisory based on such events to ensure that other platforms are not similarly compromised.

We believe that a simple information declaration process is ideal for such entities, and rigors of licensing is not necessary.

The DoT along with CDAC should continue to focus on standards to drive security in M2M configurations. Focus should be on encouraging standards driven deployments to offer secure interoperable platforms to the developer and user community.

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.

As outlined above, the framework proposed for M2M service providers, who are offering connectivity management and therefore have control on IoT device access, should have regulatory obligation to register through an online self declaration process. This is restricted to only those entities who are otherwise not covered by the existing licensing norms.

We recommend that there should not be any bank guarantee, performance guarantee for such registration. A nominal fee maybe charged to cover cost of website and online registration process, including any records that maybe maintained by DoT.

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

It is widely acknowledged that IoT will be disrupting various Industries like healthcare, agriculture, smart city etc. While this will be supported by the existing communication infrastructure, there remains scope for IoT networks that are tailored to the cost, range, load and power requirements of an IoT system. The wide scale adoption of Bluetooth for medical devices, is one such example, where, network is not based on Internet Stack (TCP/IP). New approaches e.g. Narrow band options LoRa, SigFox, Ingenu, Weightless-N and other proprietary mesh networks are being experimented with and adopted. Increasingly, a wide range of highly integrated, ultra-low-power semiconductor components are becoming available at cost-effective price points. Ultra-low-power MCUs and wireless ICs with flexible architectures supporting multiple protocols will lead the way in enabling a smart, connected, and energy-friendly M2M world

It is therefore important that any regulation that is proposed does not restrict choice or inhibits development of new solutions for connectivity.

There can be many local instances of M2M communication –a village where local devices are connected and are able to talk to each other for facilitation of agriculture and other services. In such cases the communication remains local and not get onto any public network.

Therefore, for use of such unlicensed frequencies, an information declaration with periodic updates should be enough. Information regarding frequency band being used, possible range, power and expected device density could be indicative information that maybe provided by the entity responsible for connectivity management of the devices.

It would be the responsibility of the entity to ensure that the communication is local and does not get onto any public network. Incident reporting should also be mandated.

From a regulatory perspective, best practise and guidance notes maybe shared for reference of the community. These notes should be developed in consultation with stakeholders, academia and researchers.

We recommend that this process be a standalone process and not be incorporated under any of the existing registrations.

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.

As per the M2M Power working group's analysis and report of November 2015[1], it has been concluded that the existing de-licensed frequency band of 865-867 MHz would not be sufficient to cater to the billions of connected/smart devices that would be deployed in the near future. It has further recommended an allocation of a band of 10-12 MHz for low power RF devices.

Currently the unlicensed space is 2MHz only available in 866 MHz and 433 MHz. As IoT devices grow exponentially in number, this space is going to be totally inadequate and needs to increase. While the 2 MHZ may have been adequate for earlier requirements, the Digital India push envisaged by the Government and the increased smartness that will be incorporated not only in businesses but in daily lives will lead to a greater data influx and efflux.

Some data from other economies reflect that a 20 – 40 MHz provision will help being future ready and spectrum will not end up being a bottle neck. We recommend that the DoT also work towards provisioning suitably for the IoT revolution.

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?

Our members have suggested that an overall 12 MHZ is minimum for current and 20-22 Mhz for a 25 year roadmap.

[1] http://tec.gov.in/pdf/M2M/Spectrum%20requirements%20%20for%20PLC%20and%20Low%20power%20RF%20 communications.pdf

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.

No.

At this stage of consultation process, it is not clear if this spectrum portion for NB-IoT (M2M) in unlicensed FDD mode or TDD mode.

It may not be possible to use the duplex gap (748 to 758 MHz) of Band 28 for NB-IoT applications because this band has a dual duplexer and filter design that would essentially need at least 10 MHz of clear duplex gap to avoid any uplink-downlink type of interference issues.

There are several concerns related to use of this centre gap for unlicensed deployment

1. Interference in licensed usage from unlicensed usage could devalue the entire 700MHz band
2. If centre gap of this band is used for unlicensed deployments, there is risk of no global harmonization as different regions/countries have different band plans in this band. Therefore, delicensing of part/entire center gap of APT 700 MHz band will not have global or even regional support for creating a M2M ecosystem and there will be no economies of scale.

   ITU-R Recommendation M.1036-5 contains details of these different frequency arrangements. As per this recommendation arrangements A4 (USA, Canada), A6 (China), A8 and A10 (Europe) and A11 (Iran) will overlap with the center gap of frequency arrangement A5 (APT 700 band plan).

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?

Ideally, charges for roaming between operators should be left to market forces, and service providers. Inter-connect charges between operators should be based on FRAND (Fair, Reasonable, and Non Discriminatory terms).

However, the regulator should maintain oversight to avoid exploitation. Case in point, how mobile roaming charges were brought down after intervention. It is important that the cost component be minimal for adoption and propogation of M2M.

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.

Many of the high end devices have preloaded foreign SIM where equipment warranty would be void in case of tampering that may include changing SIM . Therefore, in some cases changing SIM may not be a possibility. The process to be followed in such cases should be clarified by the regulator. We recommend provision for regulatory oversight similar to Indian SIMs, in cases where the SIM cannot be changed within a specified time as notified by the regulator.

The regulator may consider security verification and testing for SIM based devices.

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?

There is a possibility that for imported M2M devices, that may have SIM in-built, change or remove of SIM leads to nullification of the warranty and support as it amounts to device tampering.

As standards are being driven for an interoperable and secure ecosystem, it is important for the Government and Industry, to address issues related to SIM. Should there be a regulatory imperative to have localised SIMs, then there should a mechanism for regulators oversight as roaming partners agree on rates.

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

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?

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.

Factoring in security is a growing need as M2M would also mean more vulnerabilities, as evident from recent Dyn attack which resulted in DDoS attacks that created Bots and generated traffic of more than one tbps, leveraging the vulnerabilities of the devices.

Security-by-Design is an approach in the system development lifecycle process to ensure that our applications and systems are built, deployed, maintained, upgraded and disposed of securely. Subscribing to Security-by-Design will reduce piecemeal implementation and the need for costly and often ineffective retrofitting. All the manufacturers of M2M devices should be encouraged to adopt 'Security-by-Design' practices to address cybersecurity issues upstream and along the supply chain.

Security at architectural level:

M2M entails a layered architecture which are three interlinked domains of M2M - device domain, network domain and application domain. M2M communication poses unique security challenges as the Internet grow steadily and rapidly.

In addition to providing security at network and device level, it is imperative to also incorporate following points while developing Security framework for M2M infrastructure in the country:

- All the communication protocols should ensure security-by-design, whether open source or proprietary
- All sensitive and critical channels of M2M communication should be encrypted by default
- The regulator must clearly outline segregation of critical and non-critical services with regard to M2M. The roadmap document should clearly list out the two categories
- There is a need of **security at gateway level** which is a critical component of any M2M architecture at network level. This could include security solutions at a level to ensure non-tamperable devices for sensitive and critical infrastructure.
- Unique identifiers such as IMEIs and ESNs may not suffice to secure M2M as they can be easily tampered with, there is a need to **combine other M2M device attributes to strengthen M2M device/sensor level security. Experiment to derive and use device biometric like PUF (An aadhar like identified for device) may be considered.**
- Apart from the Requirements of Confidentiality, Integrity, Authentication, Access Control, Privacy & Availability, it is extremely important to **factor in the safety of OT and ICT technologies which are part of M2M Services.**
- Resilience to Cyber Security attacks – identifying and responding to security breaches – will become a critical survival trait in the future. Ergo, the principle of Resiliency must be given due attention.
- The M2M/IOT ecosystem requires interoperability to create the "seamless" programmability of the very devices or sensors that enables the full potential of a connected experience. This means IoT requires standards to enable horizontal platforms that are communicable, operable, and programmable across devices, regardless of make, model, manufacturer, or industry. The vision is that connectivity between people, processes, and things works no matter what screen type, browser, or hardware is used. The reality, however, is that the IoT is fragmented and lacks interoperability; disparate or overlapping solutions can't easily "talk" (connect) to each other.

Other Recommendations from Security standpoint

- It is critical to establish capacity, capabilities and institutions which can do security testing of m2m hardware and software for its secure usage.
- In order to ensure robust security of M2M ecosystem, it is vital to patch legacy systems so that the existing vulnerabilities could be plugged. As legacy systems continue to get more out-of-date while the world around them continues to evolve, the risks are increasing. A few of the things that make legacy systems risky include unpatched software, hard-coded passwords, and a failure to draw any budget money for upgrades and updates.
- Connected devices should be designed with security as the priority to reduce the possibility of long-term risks. Securing by design builds security measures directly into the device for a core-to-edge approach to protecting access to the device and data.
- Standards groups should strive to create an M2M Security Standard (MSS) that is measurable and defines a minimum standard of security for devices. This is particularly important from providing a reasonable or acceptable level of security for common use.

IoT security requires significant thought including deliberation on issues related to proactive defence. The scientific, technology and regulatory regime should be open to adopt and evaluate technology options.

Data Confidentiality in M2M

Data confidentiality represents a fundamental challenge in M2M devices and services. In M2M context, not only the user may get access to data but also authorized objects. This requires addressing three important aspects:

I. Access control and authorization

II. Authentication and identity management (IdM)

III. Securing the data – at rest, in motion and during processing

The device needs to be able to verify that the entity (person or other device) is authorized to access the service. Authorization helps determine if upon identification, the person or device is permitted to receive a service. Access control entails controlling access to resources by granting or denying means using a wide array of criteria. Authorization and access control are important to establishing a secure connection between a number of devices and services. The main issue to be dealt with in this scenario is making access control rules easier to create, understand and manipulate. Another aspect that should be consider when dealing with confidentiality is authentication and identity management. In fact this issue is critical in M2M, because multiple users, object/things and devices need to authenticate each other through trustable services. The problem is to find solution for handling the identity of user, things/objects and devices in a secure manner. To ensure data confidentiality, appropriate security controls across the information lifecycle should be adopted so that data and any given point in time – whether at rest, in motion or during processing – is secure.

A regulatory sandbox approach, as is being followed by the fintech industry, for experimentation should be encouraged, as the M2M ecosystem evolves. TRAI/DOT should consider establishing an enabling environment to experiment with different security architectures, at network level, device level and various options. This could include aggressive response mechanism, deception based defense, hardware driven solutions like eSIM, device biometric etc. are some examples. Cryptographic approaches uniquely designed for IoT devices like biometric id self-generated as an example, and diversity in solutions should be evaluated.

Sharing security breaches and responses or threat intelligence should be encouraged, similar to how Banks use Indian Banks – Center for Analysis of Risks and Threats (IB-CART)[2].

DoT should formulate an expert committee to develop M2M Cyber Security Framework that aligns with the overall direction of the Cyber Security initiative taken by the government and the industry. NASSCOM- Data Security Council of India would be glad to work with DoT on this initiative.

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.

M2M devices and communications definitely have potential to erode privacy. Interconnected devices, microphones, cameras, sensors etc. can unknowingly track locations, movements and conversations. Governments have potential to surveil citizen's en masse, and businesses horde and mine personal data to harness economic value of personal information.

Director of US Investigation agency CIA David Patraeus hinted that CIA couldn't wait to spy on people via their smart appliances[3]. US Director of National

[2] http://www.idrbt.ac.in/ib-cart.html

[3] http://www.networkworld.com/article/2221934/microsoft-subnet/cia-wants-to-spy-on-you-through-your-appliances.html

Intelligence James Clapper last year testified, "In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials"[4]. Recently, police officials sought data from 'Amazon Echo' device for further investigation and evidences[5]. Such requests will only aggravate going forward.

Objects collecting, storing and transmitting information can, in many cases, reveal information about individuals that may be used to derive behaviour, interests and other personal information (PI). **In M2M this information exchange is not generally noticed by the individual because it is not the human who initiates the communication but the machine**. In many cases, people are therefore either unaware or negligent about this information exchange over a long period of time. Further, since the data transfer is usually automated in nature in M2M communication, the user centric privacy principles such as notice, choice, consent, etc. which require user's direct understanding while sharing PI with machine(s), comes under more scrutiny.

Various interests can motivate the **misuse of personal information** and cause harm and damage not only in financial terms but can also impact the health and life of an individual. For instance, chips in form of body tattoos and sensors are being installed on humans and inside bodies, collecting and transmitting various forms of personal information to mobile devices at medical units. This information which may have one's entire day's lifecycle consisting of information which individual himself may not be knowing, if compromised and misused, has a potential to cause a major and permanent damage. Similarly, in smart metering, power consumption will be measured or monitored continuously. Measurement with such high time accuracy can be misused for profiling. Not only can this reveal whether someone is at home but also what electric devices - coffee machine, washing machine, etc. – s/he is using, and at what moment in time.

For organizations also, developing the comprehensive visibility of all the PI traversing between machines becomes a major task which they have to perform in order to answer questions related to privacy protection to regulator and public, on general. Recently, in October 2016the U.S Federal Communications Commission (FCC) released privacy rules to broadband and telecom service providers in order to ensure privacy protection to consumers. These rules, taken as reference, can provide certain guidance to regulator for ensuring privacy protection in M2M communication. The rules define framework for service providers to follow and comply with addressing the aspects related to specific privacy principles such as consent, notice, choice, transparency, security, data

[4] http://www.networkworld.com/article/3154938/security/mozilla-iot-will-be-the-first-big-battle-of-2017-calls-for-responsible-iot.html

[5] https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case/

use and sharing limitation. Privacy framework for M2M ecosystem needs to be developed and followed by the industry.

It also discuss the nature, category and definition of various sensitive and non-sensitive PI collected and processed by service providers. There is clear demarcation of the scope and applicability of the rules on various type of service providers which can be looked-upon while developing such kind of rules for Indian M2M communication industry.

Some of the sectors are independently addressing Privacy concerns. For e.g., the Ministry of Health and Family Welfare, Govt. of India has drafted a standard for electronic health records[6]. There is a such is the case of addressing only sectoral requirements of privacy whereas when it comes to technologies such as M2M, IoT, Big Data, etc., but overall the privacy concerns cut across all the sectors. Hence, there is definitely a need of comprehensive privacy law in India cutting across all the sectors and independent of any technology. Development and adoption of standards, testing and certification mechanisms for security and privacy aspects (e.g. privacy seals or ratings of mobile apps) should be encouraged. For example, lot of work is being undertaken at international standard development organizations (SDOs) to develop standards in the privacy space including in areas of privacy notice and consent. India should participate in such forums to ensure its requirements and concerns are addressed.

Need for a comprehensive Privacy Law

The law should talk about what to protect, not how to protect. The security and privacy approaches in any such law or legislation should be market driven, with practices and procedures evolved from global best practices.

The current regulatory framework is not sufficient to guarantee Privacy protection. There exists a patchwork of legislations governing privacy aspects in India. Information Technology (Amendment) Act, 2008 (ITAA, 2008) discusses privacy protection to an extent, but the coverage is very limited. It does not cover cookies, tracking pixels and other metadata explicitly, nor are the provisions in the Act comprehensive enough to cover all privacy implications that can be caused by data collection and processing by machines. Similarly, the act's applicability only on body corporates, only covering the information in electronic form, silence or very generic statements on privacy concerns arising due to social engineering, data consolidation, encryption, cross-border data flows, etc. makes the ITAA, 2008 incomplete in terms of addressing growing privacy concerns globally.

There are no privacy principles defined explicitly in Telecom licensing condition nor is any data protection authority being set up in telecom sector to regulate privacy matters. Hence, in today's scenario of ever increasing digitization, cloud

[6] http://www.mohfw.nic.in/showfile.php?lid=4138

computing, machine learning, artificial intelligence, etc. there is a dire need of privacy law in India like many other geographies. **India should enact comprehensive privacy law** that has been in making for long. Much work has already been done in this regard by development of privacy framework in form of a report by Justice AP Shah Committee. The report, along with addressing various privacy aspects, has described the privacy principles with detailed issues, their addressal, rationale and scope in India. The 9 privacy principles defined therein are Notice, Choice and Consent, Collection Limitation, Purpose Limitation, Access and Correction, Disclosure of Information, Security, Openness and Accountability. Similarly, the government is yet to release the encryption policy under section 84A of the IT (Amendment) Act, 2008 to "for secure use of the electronic medium and for promotion of e-governance and e-commerce." Increasing the encryption standards in the country will enhance security, safety and privacy of consumers.

In addition to steps taken by the government and by businesses, consumers also have an important role to play when it comes to protecting their information. Consumer education is pivotal in ensuring privacy and security. Further, the organizations along with government can play a role of developing and enacting a co-regulation and self-regulation eco-system. NASSCOM, on similar lines, instituted Data Security Council of India (DSCI) for enhancing the cybersecurity and privacy posture of the country by doing significant work in thought leadership, public awareness, public advocacy, capacity building, etc. DSCI can work with the community to develop privacy best practices guidelines for M2M community.

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.

There may be guidelines defined by TRAI, to pre-empt a call drop like situation at points of interconnections. However, the SLAs should be as per contractual T&C of the MSP and TRAI may offer guidance on minimum performance levels.

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?

While any policy should be technology neutral, guidance on energy efficiency, delay etc are important for optimisation of performance and ensure service levels, both critical for IoT adoption. This will require technical analysis and also discussions with various industrial alliances and research projects who are pursuing standards and technologies in the M2M space including but not exclusively in cellular networks.

The major benefit of supporting M2M applications in cellular networks is the ubiquitous wireless access in both urban and rural environments on the existing wireless cellular infrastructure, which means there is no need to build alternate infrastructures. However, the low mobility, stringent cost and energy efficiency requirements of M2M devices make the design criteria of M2M communication very different from that of cellular networks.

To allow for higher device density, we proposed a lower power level ~0.5 – 1 Watt with a 5-10% duty cycle be evaluated. It is essential to support a large number of M2M devices, and suitable specifications and standards may be adopted, keeping local requirements and global trends in mind, after a thorough technical analysis.

Q16. Please give your comments on any related matter not covered in this consultation paper.

We would like to reemphasize that the policy should be technology neutral. Any technology preference arising out of regulatory arbitrage should be avoided.