ESYA centre

THE PITFALLS OF REGULATING M2M COMMUNICATION SERVICES UNDER TELECOM LAW

OCTOBER 2023 | ISSUE NO. 036.

The Pitfalls of Regulating M2M Communication Services under Telecom Law

October 2023

Attribution: Mohit Chawdhry, *The Pitfalls of Regulating M2M Communication Services under Telecom Law*, October 2023, Esya Centre.

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The **Esya Centre** is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at esyacentre.org

About the Author: Mohit Chawdhry is a Fellow at the Esya Centre, New Delhi

Image credit: Cover sourced from Stable Diffusion's Dream Studio

CONTENTS

ESYA centre

OBJECTIVE

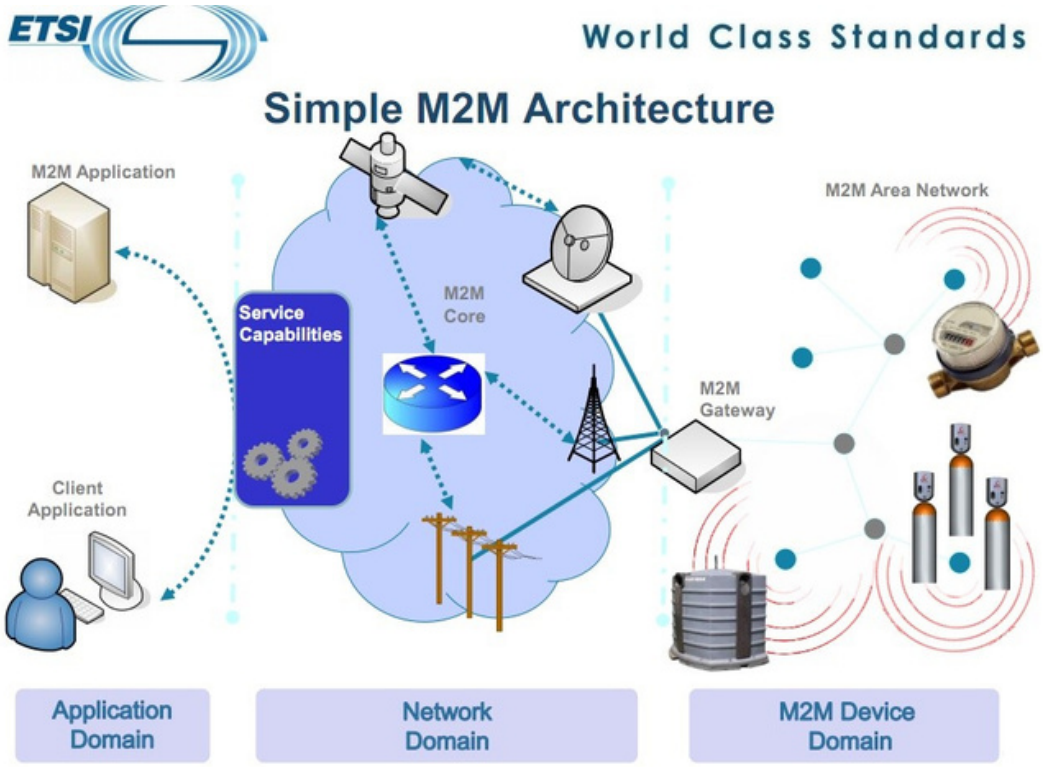
This primer questions the effect of regulating machine-to-machine (M2M) communication services by using telecom law in India. It responds to the Draft Indian Telecommunication Bill 2022, on which comments have been sought by the Department of Telecommunications (DoT), which defines a 'telecommunication service' to include 'machine-to-machine communication services' – suggesting that telecom style regulation may be applied to M2M communications as well. It outlines the technology that underpins M2M services, the regulatory issues that may arise as they gain use, asks whether telecom law is suited to redressing these concerns, and concludes with recommendations.

TECHNOLOGY OVERVIEW

M2M refers to technology that permits direct communication between computers or devices over wireless or wired networks. An emerging technology, it is difficult to exhaustively define, but the definition proposed in 2010 by the Body of European Regulators for Electronic Communications BEREC) and cited in many policy documents defines M2M as *"a generic concept that indicates the exchange of information in data format between two remote machines, through a mobile or fixed network, without human intervention."*[1] A related concept is the Internet of Things (IoT), a collective of devices or other physical systems connected over the internet or another information network enabling interaction and coordination between them and the surrounding environment, including human society. The International Telecommunications Union defines the IoT as *"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"*.[2] The IoT is a broader concept that encompasses M2M and machine-to-person (M2P) communication technologies.

The main goal of M2M technologies is to let devices such as sensors capture and relay data about their environment or their current state to each other. The connected machines are programmed and controlled remotely,[3] through a unified network of sensors, servers, applications and communication systems.[4] Their interactions can be explained with the example of a smart farm, where various sensors deployed throughout the farm to detect soil moisture, temperature, humidity and other variables collect data from their surroundings and send it across a wireless network for storage and processing in online cloud servers. A software program or app may analyse the data and display it to farm workers in user-friendly ways. The app may also alert farmers if the soil moisture drops below a certain level, or automatically activate the irrigation system based on data received from the sensors.

The figure below shows a simple M2M network, drawing on reports and documentation by the European Telecommunications Standards Institute[5] and the Indian Telecommunication Engineering Centre.



- **Devices:** The hardware used to collect and transmit data from machines, equipment or other sources. It may include sensors, gateways, routers, modems or controllers.
- **M2M platforms:** The software platforms used to manage M2M devices, applications and data. They are used for device management, data analytics, app development, integration with other systems and more.
- **Application services:** The end-user services built on top of the M2M infrastructure. They may include apps for fleet management, remote monitoring and control, predictive maintenance, or automating smart homes.
- **Network connectivity:** M2M technology relies on a combination of short, medium and long range communication services to exchange data between devices and platforms. The sensors on a smart farm, for instance, may communicate over short range networks like Bluetooth or ZigBee, while the sensor data is communicated to a cloud network or platform using long range technologies like LoRA or NB-IoT. **It is expected that low-range, non-cellular networks will be the primary enablers of M2M and IoT, as they provide last-mile device connectivity.**[6] A fuller overview of the network technologies used by M2M services is in **Annexure 1.**

A typical M2M network depends on many entities. A hardware manufacturer might build the sensors and devices, while a telecom company provides connectivity, and software-as-a-service providers make the software applications and platform. The participants involved in managing and hosting an M2M network are collectively known as its value chain. The value chain is a multifaceted system permitting a wide array of applications in many sectors, from infrastructure development to management, healthcare, education, automotives and agriculture. Table 1 sets out the leading use cases below.

Use case of M2M technology	B2B (Industrial)	B2C (Retail or consumer facing)
Fleet management	X	
Supply chain management	X	
Remote monitoring and control	X	
Industrial automation	X	
Smart grids	X	
Telemedicine		X
Smart homes		X
Wearable devices		X
Connected cars	X	X
Smart retail	X	X

Table 1: Leading applications and use cases of M2M technology

KEY POLICY CONCERNS

M2M technology connects a vast number of devices (expected to number in the billions) using communication networks. This interconnected and global network of devices may give rise to certain regulatory policy concerns. Some of the key issues in the rise of M2M technology are explored below – they were identified by studying policy proposals, consultation documents, and the stakeholder response to regulatory consultations in India and other jurisdictions, including the United States and European Union. Table 2 outlines the issues identified, along with the consumer group primarily impacted by them.

Regulatory issue	Consumer group impacted
Data protection and privacy	Retail and industrial consumers
Security	Retail and industrial consumers
Quality of service	Retail and industrial consumers
Switching and lock-in	Industrial consumers
International roaming	Industrial consumers

Table 2: Consumer group primarily impacted by M2M policy issues

A) Data protection and privacy – M2M technology relies heavily on data collection, storage, processing and analysis.[7] The data collected may be personal or non-personal – for instance, smart home applications may collect sensitive information about your health, while industry sensors gather non-personal data from products and machines. Concerns about privacy arise because the data collected by M2M devices (whether personal or non-personal) may be combined and analysed to build detailed profiles of users without their knowledge or consent.[8] It may also be stored at different points along the value chain, each of these an avenue to compromise user data.[9] The privacy risk of M2M communications depends to a large extent on the use-case and the sector of application. The risk may be higher in sectors like education or healthcare, and arguably lower in infrastructure or manufacturing. While M2M services do raise privacy concerns, regulators in the US and EU markets have observed the technology needs no special treatment as their existing data protection framework is enough to address potential concerns.[10]

B) Security – Security issues with M2M may arise at the device, network or platform level. When previously unconnected devices are connected through a network their security (such as passwords, encryption or software updates) is often neglected. Limits on energy and computing power also leave such M2M devices vulnerable to attack.[11] If the networks carrying device data are inadequately encrypted it can increase the risk of unauthorised access and data breach.[12] The platforms and apps operating an M2M network can also be exploited as a point of entry to gain access to the entire network.[13] As with privacy, the security risk of M2M services depends on the sector. With critical infrastructure (such as dams or electric grids) M2M technology may present a far higher security risk than with automated homes. Regulatory authorities and industry associations around the world have issued a number of guidelines and standards to ensure that system-wide security is maintained.

C) Quality of service (QoS) requirements – QoS parameters are used to evaluate whether technologies, services or applications meet consumer expectations for quality, availability and reliability.[14] In traditional communication networks meant for person-to-person (P2P) communication, the QoS parameters may include the call drop rate, voice call quality, and the accumulated downtime.[15] The QoS parameters for M2M communication will likely differ from P2P, and with the use case in question.[16] For instance, M2M applications in remote healthcare or driverless transport will need high reliability and availability and low latency, while these requirements can be less stringent in the case of agriculture.[17] Given the variation in QoS requirements with the application of M2M, regulators have so far refrained from imposing obligations specifically on M2M service providers.

D) Switching and lock-in – M2M devices that connect to public networks using a SIM may present user switching and lock-in issues. Switching network providers for these M2M devices may need hardware modifications, such as replacing the connectivity module or SIM, entailing high costs for subscribers and creating lock-in.[18] This is true especially of M2M applications in areas difficult to access. The industry and regulatory authorities are exploring solutions like 'over the air' (OTA) SIM card provisioning to let subscribers change their SIM profile or service provider remotely without hardware modification. The GSMA has issued specifications on embedded Universal Integrated Circuit Cards (eUICCs) that let users store multiple operator profiles on a single device and remotely switch between them.[19] In 2022 the TRAI released a consultation paper in this regard, on 'embedded SIMs for M2M communications', seeking stakeholder feedback on the regulations needed to deploy eUICCs in Indian telecom at scale.[20] The consultation, which received comments and counter-comments from a range of stakeholders, was closed in September 2022. Follow-on eUICC guidelines or regulations from the TRAI are still awaited.

E) International roaming – As mentioned earlier, M2M devices are often manufactured with an in-built SIM card. In such a device shipped abroad the SIM cannot connect with the 'home' provider network and must rely on international roaming to connect with the rest of the M2M network.[21] It is important for the business model for M2M devices to always be able to roam internationally, and to ensure this device manufacturers enter into 'global SIM' arrangements with mobile network operators (MNOs) in every country they seek to export to.[22] The MNO then enters into commercial, contractual arrangements with network providers in countries where it does not provide network services to ensure the devices have global connectivity. This single-platform approach to M2M deployment substantially lowers the barriers to entry for device manufacturers, enabling technology adoption at scale.[23]

In India however, international roaming with foreign numbering resources is thought to raise security and regulatory concerns. Some responses to the TRAI consultation on 'Spectrum, Roaming, and QoS related requirements in M2M Communications' observe that SIM cards enabled with permanent roaming would not have KYC validity at the same level as domestic SIMs, as the required checks would accord with the laws of the country where they were purchased and not with Indian law.[24] The ability of enforcement agencies to legally intercept communications and access data may come to be restricted with foreign SIMs.[25] Responses to the TRAI consultation note these security concerns are raised especially with M2M devices deployed in critical infrastructure such as Smart Cities.[26] Despite these concerns, only a handful of nations such as Brazil have restricted permanent international roaming and require that M2M devices use domestic numbering resources and SIMs.[27] While India does permit foreign SIMs/eUICCs, they must be converted to Indian SIMs/eUICCs within three years of activation.[28]

CURRENT REGULATORY STATUS OF M2M TECHNOLOGY IN INDIA

For many years now, regulating M2M technology has been on the government anvil. The National M2M Telecom Roadmap released in 2015 was the first policy document to articulate the government's vision for the sector.[29] It acknowledges the potential of M2M technology to help realise ambitions of a Digital India and identifies some policy issues that need resolving to promote the use of M2M technology. These include establishing a registration framework, privacy and security regulations, quality of service obligations. It makes the following recommendations on the key policy issues identified in the section above.

- **Registration** – Mandatory registration with DoT of M2M service providers (M2MSPs) using telecom resources from TSPs.
- **Privacy and security** – Implementation of KYC requirements for M2MSPs using wired or wireless communication services in their services or products. Adherence to provisions of the Information Technology Act, 2000 pertaining to the handling of user data and standards developed by bodies such as the OneM2M alliance and the TEC.

- **Quality of service** – Making no specific recommendations regarding QoS, the Roadmap acknowledges that QoS requirements for M2M communications are different from P2P connections and need a nuanced approach. It also identifies the creation of M2M-specific QoS requirements as an agenda item for inter-ministerial consultation.
- **Switching and lock-in** – Embedded SIMs based on GSMA standards should be permitted to facilitate switching between telecom operators at user discretion.
- **International roaming** – Foreign SIMs and international roaming should be permitted only if lawful traceability requirements for law enforcement purposes are fulfilled. In the short term only devices with SIMs from Indian TSPs should be allowed.

Further, in 2018 the Government of India released a National Digital Communications Policy to lay the groundwork for a holistic and harmonised approach to regulating emerging technology including M2M and the IoT.[30] It calls for simplified licensing and registration frameworks for M2M that ensure appropriate security safeguards. It also suggests earmarking adequate spectrum for M2M and IoT and other emerging technology like 5G.

Together the 2015 National M2M Telecom Roadmap and 2018 Digital Communications Policy establish the contours of a regulatory framework for M2M technology that has since been fleshed out with instructions, guidelines and recommendations issued by the DoT and TRAI. (An overview of these is in **Annexure 2.**) These policy statements collectively build a regulatory framework establishing registration, security, privacy, quality-of-service and international roaming requirements for M2M communications in India. They apply not only to connection providers for M2M communications (such as TSPs and WLAN providers) but, given the broad definition of an M2MSP in the DoT Registration Guidelines 2022, can be extended virtually to all stakeholders in the M2M/IoT value chain. Besides M2MSPs that directly use TSP telecom resources, the definition includes third parties that use 'M2M services' from a registered M2MSP in their products or offerings to consumers.[31] This means that entities offering connectivity to end-users without directly using telecom resources (such as fleet management services or car manufacturers) also need to comply with the Registration Guidelines.[32]

Evidently a light-touch regulatory framework is already in place to address the policy concerns raised by M2M technology. Now however, the inclusion of 'M2M communication services' in the definition of 'telecommunication services' in the Draft Indian Telecommunication Bill suggests the DoT may favour more comprehensive regulation, telecom style for the sector. The next section examines the tradeoffs of such an approach.

THE PITFALLS OF ADDRESSING M2M COMMUNICATION THROUGH TELECOM REGULATION

The Draft Indian Telecommunication Bill 2022 includes M2M communication services in the ambit of telecommunication services, suggesting they may be subject to a regulatory framework similar to that governing TSPs.[33] This would subject M2MSPs to the regulatory requirements and obligations placed on telecom service providers, such as licensing, quality of service and tariff requirements. Proponents argue that because the underlying network infrastructure for M2M and P2P communications is the same, both should be governed by the same legal framework.[34]

While much depends on how M2M communication services will be defined and the licensing framework that will be adopted for them, it is worth asking if regulating M2M communication using telecom laws can address the policy issues identified above without harming innovation. Fundamental differences between M2M and traditional telecom suggest the telecom regulatory framework is not suited to regulating the M2M sector. These key differences are outlined below.

Criterion	Telecom	M2M
Role of connectivity	Providing connectivity services to users is the central focus of telecom providers.	Connectivity plays only a small role in the overall M2M network. Service providers generate a larger revenue share by offering users a bouquet of goods, services and applications.
Nature of connectivity	Telecom services rely on long-range public networks to enable communication and data exchange between users.Telecom services, such as calls and video streaming, require high-speed transmission of large data volumes.	M2M service providers rely primarily on short-range communication technologies for data exchange between devices, sensors and the rest of the network.M2M services involve transmitting smaller data packets at less frequent intervals than telecom.
Target user groups and business models	Most telecom providers cater mainly to retail users over public networks.	Business enterprises are the primary consumers of M2M services, delivered by service providers using private captive networks.
International connectivity	Telecom networks are meant primarily to provide calling and data features to users within national boundaries.	M2M devices pre-fitted with foreign SIMs need permanent international connectivity to function effectively.

A) Connectivity is a small element of M2M services – Telecommunication refers to services comprised wholly or mainly of conveying signals.[35] The primary source of revenue for telecom providers is facilitating connectivity between users of devices that receive and transmit signals. While services in the M2M value chain do depend on connectivity as an input product, it forms only a low proportion of their overall revenue.[36] M2MSPs generate more revenue from device and application management, data analytics and similar services than by providing connectivity. In fact, in many cases wireless connectivity for M2M devices is weighed as a cost of doing business, meaning that service providers do not separately charge their users for it.[37] As most M2MSPs are not connectivity providers, but only use the existing telecom infrastructure to offer users different collections of goods and services, they differ considerably from TSPs.[38]

These differences make it worth asking whether M2MSPs should be made subject to the licensing requirements asked of telecom providers. Telecom licensing requirements seek to ensure the optimal use of spectrum, and imposed on M2MSPs may discourage market entry and innovation by raising the compliance costs for small and medium enterprises in particular.[39] Only a handful of nations worldwide (such as Singapore, Saudi Arabia and the UAE) impose licensing requirements on M2MSPs.[40] Further, connectivity providers to M2MSPs are already subject to the licensing requirements of the DoT, and M2MSPs that use telecom resources to offer services to others must also register with the DoT. For these reasons the rationale for imposing additional licensing requirements on M2MSPs in the Draft Telecom Bill remains unclear.

B) Even where connectivity is used, cellular connectivity is used minimally – As noted in the prior section, M2M applications rely on short and long range technologies to enable communication between networked devices. Only a small proportion of M2M devices rely on cellular/public networks for connectivity. A presentation by the TEC observes that only 15–20% of M2M connections in India will need to rely on SIM connectivity.[41]

Further, the nature of cellular connectivity required by M2M devices as well as the traffic they generate differ considerably from human-to-human services. As compared with P2P, most M2M devices use smaller data packets, need uplink-dominant communication, and are characterised by long intervals between data exchange.[42] They differ markedly from P2P communications, characterised by large volumes of data transmitted at frequent intervals and high speeds, such as for video calls or to view digital content like OTT.[43]

C) The business model for M2M services is fundamentally different from telecom – Telecom services and M2M communications are meant for different consumer groups and follow different business models. The primary source of revenue for telecom operators are their B2C services. An analysis of 33 global telecom operators estimates that nearly 69% of their collective revenues flow from consumer facing services.[44] In most M2M use cases on the other hand, the users are businesses seeking deployment at scale, not end consumers.[45] For this reason, the KYC norms meant to verify individual subscribers may not fit a situation where, for instance, a single business entity buys SIM cards in bulk for use in M2M devices. Some respondents to the TRAI consultation on 'Spectrum, Roaming and QoS-related requirements in M2M Communications' have noted that M2M communication services may not need an onerous KYC process as they are used primarily in industry.[46]

It is likely also that M2M devices especially in the enterprise sector will rely on private captive networks and not the open public networks used for P2P. The DoT's own 'Guidelines for Captive-Non-Public Network License' have cited M2M communications as a leading use case for private

captive networks (the high speed and ultra-low latency networks designed specifically for business and industrial applications).[47] The QoS requirements for such networks also differ significantly from public networks.

In view of the above it is worth asking whether the QoS and KYC requirements of telecom law, designed with person-to-person communication in mind, are suitable for M2M communication services. It is also doubtful whether more regulatory intervention in the M2M sector is needed without clear evidence of market failure. Premature regulation has the potential to undermine the emerging M2M sector, by promoting rent-seeking and enlarging the government's role thereby crowding out private participation.[48]

D) M2M services are inherently global in certain sectors – As noted earlier, the M2M sector involves a transnational service market. A significant number of M2M devices rely on permanent international connectivity for their operation, and the terms and conditions by which crossborder services are provided will play an important role in the growth of the sector.[49] Applying restrictions on roaming and connectivity from legacy telecom may impact growth and innovation. For instance, mandating the conversion of foreign SIMs/eUICCs into local ones within three years may limit the domestic availability of M2M devices manufactured abroad.[50] Likewise, Indian manufacturers may be deprived of global export markets if they are prevented delivering M2M services outside India using Indian international mobile subscriber identity numbers.[51]

WHAT SHOULD M2M REGULATION FOCUS ON?

The previous section described the pitfalls of adopting telecom-style regulation for M2M services. Such an approach will likely hamper technology innovation given the fundamental differences between M2M and telecom services. M2MSPs are subject already to a comprehensive regulatory framework addressing the key policy issues raised by the new technology, including privacy, security and quality of service concerns.

Rather than seeking to regulate M2M services in the same vein as telecom, policymakers should consider how the current framework and standards can be improved to boost innovation and adoption of the technology. Some recommendations on what policymakers should focus on are given below.

A) Exercise regulatory forbearance in the absence of market failure.
India's M2M industry is still developing, and stakeholders determine the avenues for revenue generation, supply chain links, and opportunities for deployment at scale. Imposing telecom-style regulation on an emerging sector may stifle innovation and growth in the longer run. The Economic Survey 2019-20 recalls instances of government intervention without evidence of market failure, explaining how the intervention undermined the markets in question.[52] It states that government regulation of drug prices under the Drug Price Control Order 2013, for example, caused the prices of regulated pharmaceuticals to increase relative to unregulated drugs.

Policymakers should instead observe regulatory forbearance, a principle of economic regulation that discourages regulatory intervention in the absence of market failure.[53] Government involvement in the sector should be limited to facilitating growth and monitoring potential market risks rather than heavy-handed regulation.

B) Introduce specific regulatory requirements for different components of the M2M value chain.
The first section outlined how the M2M value chain comprises many different components including devices and sensors, platform and cloud servers, applications, and communication networks. All components of this value chain are currently subject to similar regulatory requirements under the 2022 Registration Guidelines of the DoT. The process of registration these envision is meant primarily for entities that provide the connectivity element of M2M servers, and may be unsuited to the other components of the value chain. For instance, the requirements to maintain user logs and report to the DoT may be onerous for entities solely involved in manufacturing M2M/IoT devices or providing value-added services. The potentially large numbers of logs and players will also be a challenge to monitor efficiently for decision making purposes. Policymakers might therefore consider a nuanced minimal framework to address the regulatory and policy issues raised by different components of the M2M value chain.

C) Promote industry-led standard setting.
Technology standards for M2M services will help build a shared communication architecture for different devices to plug into for seamless service to consumers. The 2015 National M2M Roadmap recognises the importance of standard-setting for M2M technology, identifying it as a key area for policy intervention.[54] The unique nature of M2M communication, with its diverse range of devices and applications, necessitates a flexible approach to standard setting. This is best achieved by industry-led initiatives that respond swiftly to technological advancements and market trends. A prime example[55] of industry-led standard setting is the OneM2M Partnership Project involving key players from sectors including telecom, automotives and healthcare.[56] The project aims to achieve a universal standard for M2M communications to ensure the interoperability of a wide range of applications and devices.

D) Pursue global collaboration on standards.
M2M communications often involve devices and networks located in different jurisdictions, each with its own regulatory framework and standards. This can pose a significant challenge to the seamless operation of M2M services. By fostering global collaborations, policymakers can help harmonise standards across jurisdictions, enabling the smooth operation of crossborder services. Such collaborations also promote sharing best practices and lessons learned and yield more effective and efficient standards in tune with the global nature of M2M communications. The Telecommunication Standards Development Society – an industry-led, nationally recognised telecom Standards Development Organization (SDO) – is already an active member of 3GPP and the OneM2M partnership with more than 50 contributions in developing M2M service layer standards.[57] Building on these participations would further align India's M2M standards with global best practices.

ANNEXURE 1

Technology	Definition	Range	Speed
Non-cellular connectivity			
RFID	Radio Frequency Identification uses electromagnetic fields to automatically identify and track the tags attached to objects.	Short (up to 100m)	Low
ZigBee	A low-cost, low-power, wireless mesh network developed specifically for short-range M2M connectivity.	Short (up to 100m)	Low to Medium
Bluetooth	A wireless technology standard for exchanging data over short distances. Developed as alternative to short-range data transfers using cables	Short (up to 100m)	Medium
Wi-Fi	A family of wireless network protocols based on the IEEE 802.11 standards and used for the local area networking of devices and Internet access.	Short to Medium (up to 100m indoors, 300m outdoors)	High
Sigfox and LoRa	Low Power Wide Area (LPWA) network technologies designed for long-range communications at a low bit rate.	Wide (up to 50km for Sigfox, 5km for LoRa in urban areas)	Low
Cellular connectivity			
Legacy Cellular (2G, 3G, 4G)	Cellular technologies primarily used for mobile and voice communication that can also provide the required data connectivity for M2M communications. However, traditional cellular networks typically require significant battery power and can suffer from network gaps, which is not ideal for M2M communications.	Wide (up to 35km for 4G)	High
NB-IoT	Narrowband IoT is an LPWA radio technology standard developed by 3GPP to enable a wide range of cellular devices and services. It is primarily focused on low power devices in hard-to-reach places and is best suited for stationary M2M applications such as smart homes	Wide (up to 35km)	Low

LTE-M	LTE for Machines is a type of low power wide area network (LPWAN), a radio technology standard developed by 3GPP. It uses the same architecture as 4G but is specifically geared toward providing extended mobile coverage with lower device battery consumption, albeit at lower speeds.	Wide (up to 100km)	Medium
5G	5G is the latest iteration of mobile connectivity and promises improved speeds, reduced latency, and efficient spectrum management through network slicing. It also enables connecting a larger swarm of devices (1 million devices/sq km) to a network. Overall, 5G is expected to significantly improve the adoption and deployment of M2M and IoT devices.	Wide (up to 100km)	Very High

ANNEXURE 2

DoT instructions on restrictive features for M2M SIMs[57] (16.05.2018)	
Target stakeholders	TSPs M2MSPs

Key obligations /provisions	• Issuance of M2M SIMs by licensed TSPs must adhere to relevant KYC norms
	• M2MSPs shall record and maintain details of all physical custodians i.e. end-users of M2M devices and SIMs
	• TSPs shall impose restrictive features on M2M SIMs vis-a-vis H2H SIMs. The restrictions include:
	  ◦ Outgoing/incoming calls shall be allowed to/from one number only
	  ◦ Data communication shall be allowed only on two numbers with predefined IP addresses.
	• Licensed TSPs may provide embedded M2M SIMs with OTA update facility.

Policy issues dealt with	Security Switching and user lock-in
DoT instructions relaxing restrictions on M2M SIMs[57] (30.05.2019)	
Target stakeholders	TSPs
Key obligations/provisions	The instructions relaxed some of the restrictive features on M2M SIMs imposed by the DoT in 2018. The relaxations include: • Outgoing/incoming calls shall be allowed to/from *four numbers • Data communication shall be allowed only on *four numbers with predefined public IP addresses with fixed APNs.
Policy issues dealt with	N/A
DoT Guidelines for Grant of Unified License and Unified License (Virtual Network Operators)[57] (17.01.2022)	
Target stakeholders	TSPs
Key obligations/provisions	The Guidelines allow prospective TSPs and VNOs to apply for authorisation to provide telecom connectivity services specifically to M2M service providers. Holders of UL(M2M) and UL(VNO-M2M) authorisations may:

	• own the underlying network to provide connectivity services to M2MSPs • access and integrate with resources of other providers • obtain licensed spectrum to exclusively offer M2M services. The M2M service authorisation also includes obligations for service providers, including: • maintaining a 'duty cycle' of 10% at the device and network levels[1] • adhering to KYC guidelines issued by the DoT • maintaining records of details of M2M service consumers, including details of the M2M devices and their physical custodians • maintaining activity logs of M2M devices, including IP detail records and packets originating to/from such devices.
Policy issues dealt with	Security Quality of service
DoT Guidelines for Registration Process of M2MSP and WPAN Connectivity Providers[57] (08.02.2022)	
Target stakeholders	M2MSPs[57] Wireless Personal Area Networks (WPAN)/Wireless Local Area Network (WLAN) Connectivity Providers

Key obligations/provisions	The Guidelines establish the registration process for M2MSPs and providers of WLAN/WPAN connectivity. Registration as an M2MSP entails the following:
	• Providing details of the applicant's T setup/core network at the time of registration
	• Payment of a non-refundable processing fee of INR 5,000
	• Adherence to KYC guidelines issued by the DoT
	• Recording of information regarding physical custodians of M2M devices fitted with SIMs
	• Adherence to DoT instructions on the use of embedded SIMs with OTA profile configurations
	• Adherence to QoS standards the DoT may prescribe
	• Observance of security conditions, including:
	  ◦ Takedown of objectionable, obscene or unauthorised content carried on the registrant's network
	  ◦ Availability of equipment for technical scrutiny and inspection

	◦ Protection of privacy of communication in accordance with existing laws, especially the protection of sensitive personal information as defined under the Information Technology Act, 2000 ◦ Provision of decryption facilities for content carried over a registrant's network ◦ Induction and utilisation of devices that adhere to security standards established by the TEC or other international standard setting bodies, such as ITU, ETSI or ISO ◦ Preservation of tamper-proof data and event logs for one year
Policy issues dealt with	Data protection and privacy Security Quality of service Switching and user lock-in International roaming
DoT advisory guidelines for M2M/IoT stakeholders on securing consumer IoT[57]	
Target stakeholders	M2MSPs
Key obligations/provisions	The Guidelines recommend best practices to ensure that consumer-facing IoT/M2M devices are secured against cyber threats and vulnerabilities. The key obligations include: • M2M/IoT default passwords should be unique • Users should be prompted to change default passwords during device setup • Web services associated with M2M/IoT devices shall use multi-factor authentication • M2MSPs should establish a dedicated point of contact for security researchers and others to report vulnerabilities. Reported vulnerabilities should be acted on in a timebound manner • Software on M2M/IoT devices shall be updateable to address security concerns in a convenient manner that does not disrupt its functioning
Policy issues dealt with	Security

ENDNOTES

1 https://www.berec.europa.eu/sites/default/files/files/doc/berec/bor_10_65.pdf

2 https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

3 https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

4 https://ficci.in/spdocument/22943/M2M-Communication1.pdf

5 https://docbox.etsi.org/workshop/2011/201110_m2mworkshop/02_m2m_standard/m2mwg2_architecture_pareglio.pdf; https://tec.gov.in/pdf/Studypaper/White%20Paper%20on%20Machine-to-Machine%20(M2M)Communication.pdf

6 https://www.gsma.com/iot/wp-content/uploads/2015/02/Device-Management-MFORMATION.pdf

7 https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

8 https://www.pdpjournals.com/docs/88440.pdf

9 *Id.*

10 See: BEREC, Enabling the Internet of Things; US Department of Commerce, Fostering the Advancement of the Internet of Things

11 BEREC, Enabling the Internet of Things

12 https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

13 *Id.*

14 https://ieeexplore.ieee.org/document/6671899

15 https://trai.gov.in/sites/default/files/201112230259120171250upwest.pdf

16 https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

17 https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

18 https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-enabling-the-internet-of-things

19 https://www.gsma.com/esim/esim-m2m-specifications/

20 https://www.trai.gov.in/sites/default/files/CP_25072022.pdf

21 https://ntia.doc.gov/files/ntia/publications/gsm_iot_comments_6-2-16.pdf

22 https://www.trai.gov.in/sites/default/files/AT&T_India_AGNSI_CP_18102016.pdf

23 *Id.*

24 https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

25 *Id.*

26 https://trai.gov.in/sites/default/files/Airtel_CP_18102016_0.pdf

27 https://trai.gov.in/sites/default/files/AT%26T%20GNSI%20Counter%20Comments%20TRAI%20%20M2M%20Consultation.pdf

28 https://www.trai.gov.in/sites/default/files/CP_25072022.pdf

29 https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

30 https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

31 "M2M Services" means the services offered through a connected network of objects/devices, with unique identifiers, in which Machine to Machine (M2M) communication is possible with predefined back end platform(s) either directly or through some gateway.
Explanation: M2M services involve communication of end device/ object with predefined back end platform(s) either directly or through some gateway.
Examples of M2M services include fleet management, supply chain management, agriculture automation, smart utilities including power, water, gas etc. The M2M end devices/ objects and the platform(s) collecting and analysing information from these devices/ objects are controlled by some organization.

32 https://www.mondaq.com/india/telecoms-mobile--cable-communications/1161546/dot-issues-guidelines-for-regulating-m2m-service-providers

33 https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf

34 https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

35 https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-enabling-the-internet-of-things

36 https://www.trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

37 https://www.ofcom.org.uk/__data/assets/pdf_file/0020/25562/att.pdf

38 https://trai.gov.in/sites/default/files/AT%26T%20GNSI%20Counter%20Comments%20TRAI%20%20M2M%20Consultation.pdf

39 https://ntia.doc.gov/files/ntia/publications/gsm_iot_comments_6-2-16.pdf

40 https://www.simmons-simmons.com/en/publications/ckoadlwaqd4jb0b59rbrqtabl/290519-uae-s-new-laws-and-regulation-of-the-internet-of-things

41 https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CoESmartcityoct2018/IOT_SmartCity/_M2M%20IoT_Smart%20cities_ITU_ALTTC_30th%20Oct%202018%20-%20Sushil%20Kumar.pdf

42 https://ieeexplore.ieee.org/document/7389044

43 https://www.researchgate.net/publication/273368684_Modeling_and_Analysis_of_Cellular_Wireless_Machine-to-Machine_Communication_Traffic

44 https://www.telecomtv.com/content/digital-platforms-services/b2b-at-heart-of-telco-growth-plans-but-b2c-is-still-the-engine-room-finds-report-45599/

45 https://ntia.doc.gov/files/ntia/publications/gsm_iot_comments_6-2-16.pdf

46 https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

47 https://dot.gov.in/sites/default/files/CNPN%20Guidelines%2027062022.pdf

48 https://www.trai.gov.in/sites/default/files/KOAN_07062022.pdf

49 https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-enabling-the-internet-of-things

50 https://www.trai.gov.in/sites/default/files/ACTO_20092022.pdf

51 https://www.trai.gov.in/sites/default/files/AT&T_India_AGNSI_CP_18102016.pdf

52 https://www.indiabudget.gov.in/budget2020-21/economicsurvey/doc/vol1chapter/echap04_vol1.pdf

53 https://www.uu.nl/sites/default/files/rebo_use_dp_2010_10-18.pdf

54 https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

55 https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

56 https://www.onem2m.org/harmonization-m2m

57 https://dot.gov.in/telecommunications-standards-development-society-india-tsdsi

www.esyacentre.org