AT&T Comments on Telecom Regulatory Authority of India Consultation Paper—*Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications* dated 18th October 2016

Introduction

AT&T Global Network Services India Private Limited ("AT&T India"), an affiliate of AT&T, Inc. ("AT&T"), is pleased to provide comments on the Consultation Paper—*Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications*—issued by the Telecom Regulatory Authority of India ("TRAI") on 18 October 2016 (the "Consultation"). AT&T India is licensed to provide National Long Distance ("NLD"), International Long Distance ("ILD"), Voice Mail / Audio Tex and Internet Service Provider ("ISP") services in India.

AT&T and its affiliates operate globally to provide mobile, video and data solutions. With operations throughout the U.S. and more than 60 other countries, AT&T has extensive experience as an incumbent and new entrant, and as a fixed-line, mobile and satellite operator in the dynamic areas of converged technologies and services. AT&T serves nearly all of the Fortune 1000 companies with a consistent strategy and long-term investment plan to expand in growth areas like India. In particular, given its leadership in working with enterprise customers to develop global machine-to-machine ("M2M") solutions,[1] AT&T welcomes the opportunity to inform policies that will further promote the deployment of M2M communications and the Internet of Things ("IoT")[2] in India and help India achieve its objectives stated under the prestigious Digital India and Smart Cities program. Although the TRAI raises in the Consultation a comprehensive list of policy issues relevant to capturing the opportunity of M2M communications for India, AT&T's comments focus on the global business models of M2M communications and importance of developing a framework of polices that will promote the rapid development and deployment of M2M communications. Such framework should allow for the extra-territorial use of national numbering resources through roaming to make M2M services viable. Given the unique and challenging economics of the IoT marketplace, IoT device manufacturers would face an almost

[1] AT&T has a proven M2M/IoT success record, with more than 29 million connected devices, roughly 2,700 approved devices and industry analyst recognition for its solution deployment experience and capability. For example, in Current Analysis' latest global M2M product report on AT&T, principal analyst Kathryn Waldon recognizes AT&T as "one of the undisputed" leaders in the global IoT services market and writes that AT&T has "excellent traction for IoT initiatives" and "expertise in key verticals" (Current Analysis, *AT&T Global M2M Services and Strategies Product Assessment*, May 2016). And AT&T continues to introduce industry firsts, most recently announcing the launch of North America's first LTE-M site to deliver the IoT to more markets and devices. *See* AT&T Press Release, at http://about.att.com/story/north_americas_first_ltem_site_to_grow_iot.html. AT&T also collaborates with other global industry leaders such as Cisco, GE, IBM, Intel, Qualcomm, Ericsson and Deloitte.

[2] As the TRAI notes (Consultation, at 1.6), M2M is used interchangeably with various other terms, including the IoT, which refers to the addition of communications and sensing capabilities—in essence, a broader definition. In these comments AT&T generally refers to M2M as a subset (*i.e.,* type of communications or connection) of the IoT.

insurmountable obstacle when seeking to deploy IoT products and services on a global scale if they were required to follow the traditional business models for mobile handsets and tablets. Further the TRAI should avoid the application of existing regulatory frameworks / licensing to IoT, and promote security and privacy through voluntary and collaborative industry self-regulatory efforts. Specifically, AT&T directly addresses questions on the issues of M2M Service Provider framework (Q1), roaming (Q8, Q9, Q10, Q11), security (Q12) and privacy (Q13(a)), and provides a *general* response relative to questions on spectrum (Q5, Q6, Q7).

Overview: M2M Communications are Inherently Global with Unique Business Models

The TRAI outlines a range of industries with M2M applications, including automotive/transportation, utilities/energy, healthcare, safety and surveillance, financial/retail, public safety, smart cities and agriculture.[3] The number and variety of M2M applications continues to accelerate and is limited only by the imagination - whether vehicle diagnostics and tracking, smart metering, waste management, remotely-controlled irrigation systems or wearable health devices.[4] According to a recent report, India's internet economy is projected to reach US$200 billion by 2020 and will contribute 5 percent of GDP.[5] By any measure, M2M communications will stimulate substantial growth, possibly exponentially, leading to a profound societal impact.

IoT generally, and M2M more specifically, are inherently global business models which require norms, standards and regulatory policies that reflect this global business model . In particular, policies must recognize and facilitate cross border data flows and permanent M2M roaming and should not impose "Know Your Customer" ("KYC") norms at variance with international best practices. Any attempt to regulate or place restrictions on these will severely undermine development both with regards to the operational aspects and investment opportunities where the M2M and IoT sectors are concerned.

The impact will be far reaching, with global cross-border opportunities. The global nature of M2M communications is not only a defining characteristic, but a strong asset. M2M solutions not only create social welfare benefits in India, but can create economic benefits to India's industry overall, , for example, enabling manufacturers to have success with exports to world markets. Cisco, one of the major participants in the IoT, estimates that the IoT will create up to 19 trillion dollars (US$14.4 trillion private

[3] Consultation, at Table 1.1.

[4] For example, in late 2015, UNICEF named two U.S.-Indian teams winners of the 'Wearables for Good' challenge: Kushi ("happy") Baby (necklace that stores immunization records for children) and SoaPen (a soap crayon worn around the neck to encourage hand washing). *See* https://www.wareable.com/saves-the-day/necklace-khushi-baby-unicefs-wearables-for-good-challenge-1938

[5] *See* http://www.vccircle.com/news/technology/2015/01/15/indias-internet-economy-grow-200b-2020-bcg-iamai-report

sector [6]and US$4.6 trillion public sector[7]) in turnover opportunities through 2022. In countries with regulatory policies that facilitate market entry by new and varied participants and encourage innovative M2M business models, M2M communications are poised to deliver significant economic and social benefits.[8] Critically, supportive M2M policies must be based on the premise that the new business models for the IoT differ greatly from the traditional business models that have supported the mobile phone and tablet industry segments in the past.

The new business models vary both in terms of the nature of the wireless connectivity provided to the end user, and the economics of providing that connectivity. For example, with most M2M devices, mobile network operators ("MNOs") do not provide a communications service directly to individual end users or consumers. Rather, MNOs provide wireless connectivity to manufacturers and other enterprises. Manufacturers may use the wireless service for internal purposes, e.g. to extract data from a product in order to evaluate its performance, or may distribute wirelessly-enabled products and services to end users.[9] The MNO, as the network operator providing the telecommunications service may properly be subject to regulation as a telecom provider, but the manufacturer who incorporates the service into its product or uses the service for its own internal purpose should not be subject to any telecom regulation

Manufacturers of products that contain a communications capability between two devices or machines typically do not view themselves as the provider of an electronic communications service to the end user and therefore generally do not charge the end user for a communications service. Instead, the manufacturer develops a product that may be enhanced via the integration of wireless connectivity. As such, data transport is merely an ancillary component, not a principal feature, of the overall product or featured service (*e.g.*, data analytics, fleet management) sold to the end user customer. For instance, an M2M-enabled smart meter fundamentally measures electricity usage; the M2M enhancement allows the near real-time transmission of that usage information to the electric utility company, who provides electrical power (not telecommunications).

---

[6] J. Bradley/J. Barbier/D. Handler, *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, Cisco, 2013. *See* http://ioeassessment.cisco.com/learn/value-stake-analysis

[7] J. Bradley/C. Reberger/A. Dixit/V. Gupta, *Internet of Everything: A $4.6 Trillion Public-Sector Opportunity,* Cisco, 2013. *See* http://ioeassessment.cisco.com/learn/value-stake-public-sector http://www.cisco.com/c/dam/en_us/services/portfolio/consulting-services/documents/internet-of-everything-public-sector-white-paper.pdf Note: in its latest Visual Networking Index (June 2016), Cisco reported that "[g]lobally M2M connections are calculated to grow nearly three-fold from 4.9 billion in 2015 to 12.2 billion by 2020, representing nearly half (46 percent) of total connected devices." *See* https://newsroom.cisco.com/press-release-content?type=press-release&articleId=1771211

[8] Cisco estimates that from a non-defense public-sector perspective, India can gain US$116.2 billion by embracing the IoT. *See* http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_value_at_stake_public_sector%20_analysis_faq_121913final.pdf

[9] The TRAI notes that "M2M services are changing the relationship between connectivity providers and end-users" such that the "connectivity providers are losing the direct relationship with the end user." Consultation, at FN 4.

Further, the connectivity that supports M2M services is not limited to commercial cellular networks. M2M devices will connect over many other available types of networks.[10] In addition to cellular LTE and 5G, M2M service and the IoT will encompass devices on Wi-Fi, satellite, mesh or low power networks on unlicensed spectrum, and wired networks—and in some cases multiple and different connection capabilities will be incorporated in a single device. Therefore, as the TRAI determines its recommendations, the Authority should not establish restrictive measures or measures that focus on a particular technology (e.g. cellular) which ultimately may only account for a small fraction of the market worldwide.

Internet of Things solutions enable remote machines or devices to communicate wirelessly with back-end IT infrastructure. Devices—as diverse as trucks, turbines, heart monitors, and vending machines—use a cellular data link to communicate with a computer server. In an IoT solution, a database stores and responds to the data that the devices exchange, and management applications enable the enterprise to report, analyze, and act upon the information.

Remote devices can uplink to IT systems to report inventories, status or usage information, and systems can downlink to the devices to send instructions, update software, or remotely monitor equipment. When a vehicle, meter, instrument, house, or business can transmit real-time information wirelessly and receive valuable feedback, enterprises and Governments can automate manual processes and streamline service provisioning and billing. IoT solutions can help improve business efficiency for many types of services. This will be very helpful in Government's agenda for building a digitally savvy society as well as in implementing the prestigious smart city program by Government of India. For example:

- Healthcare providers can remotely monitor patients' conditions after medical procedures so that patients can recover in comfort at home.
- Power companies can electronically transmit data from power meters to company billing systems and minimize the cost and time of on-site readings. In addition, they can monitor electricity grids in real time for capacity and outage conditions to help isolate and repair disruptions.
- Shipping or other service companies can track container or vehicle temperatures, jitter and locations and plan service routes and monitor pick-ups and deliveries.
- Construction companies can monitor the status of remote assets like construction equipment or pipelines.
- Farming equipment can take soil samples in the field and transport data instantaneously to a data center for evaluation and, in return, receive instructions for amending the soil.

[10] In fact, according to IoT research firm, Machina Research, IoT connections will grow to 27 billion in 2025, of which only 2.2 billion will be cellular connections. And only 1 percent of data traffic will be cellular during that same timeframe. *See* https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/

As the above examples show, IoT solutions can help customers streamline processes, save time, reduce labor expenses, and improve service quality.

Following upon the National Telecom M2M Roadmap released by Department of Telecommunications in May 2015, there is a tremendous opportunity to make enormous positive impact for consumers, Indian manufacturers, and Government by adopting policies that encourage competition and innovation in the M2Mmarket in India. For example, TRAI could facilitate new business models for M2M services by permitting the use of "Global SIMs" for the delivery of M2M services in India. Global SIMs are the SIMs of one MNO used globally, on a single platform. Global SIMs allow a manufacturer, for example, to contract with only one operator for all its global needs, and to use one platform for global ordering, provisioning, rather than having to acquire services from different operators in each country into which they distribute their products, each of whom has different platforms that may record information in different ways, preventing the consistent collection of information across countries. International roaming is the vehicle for data transport for the Global SIM. In each country, an underlying MNO that is subject to local regulation provides the wireless service, but the service is sold to operators in other countries who can then offer roaming on their Global SIM, using a single platform worldwide, to their customers who have global distribution needs. The efficiency of such an arrangement is imperative to the success of M2M services in a very low margin business (relative to cell phones and tablets). By permitting business models that rely on Global SIM model, TRAI would help accelerate IoT solutions offered by industries relying upon on a single global platform and service delivery model and signal to the industry that TRAI appreciates that the business models that apply to M2M services are significantly different from the business models that apply to standard handsets and, therefore, require much more flexible policies to encourage flexible solutions.

In the M2M environment, economies of scale are essential:

- Compared to mobile phones and tablets, M2M devices typically have low data consumption and very low average revenue per user ("ARPU") (*e.g.*, a smart meter sending a few hundred bytes of data per day vs. a smartphone or tablet consuming tens of gigabytes.

- Manufacturers typically do not sell, or charge, end users separately, for wireless connectivity. Instead, wireless connectivity is a cost of doing business that may be included in the overall price of the M2M product.

- Because their products usually have very low ARPU, manufacturers are *extremely sensitive* to development and deployment of input costs.[11]

- To efficiently amortize their costs, manufacturers tend to develop standardized products with long useful lives that can be sold in significant volumes across many countries.

The emergence of new M2M and IoT business models pose unique challenges that require fresh thinking and innovative solutions, such as a light-touch regulatory approach for the introduction of a Mobile Service Provider ("MSP") (which has been the draft registration based framework led by DoT with industry consultation)., liberalized policies for the allocation and use of numbering resources, and industry-driven security and privacy practices.[12] Given that M2M communications, and the IoT, are evolving at a dynamic pace, government and industry must work together to create flexible, global, interoperable and future-focused policies to ensure the IoT and M2M communications deliver their potential for economic and social development in and across all sectors, private and public.[13]

[11] The TRAI rightfully acknowledges that "M2M device manufacturers would face challenge when seeking to deploy products and services on a global scale if they follow traditional handset or tablet business models." Consultation, at 2.34.

[12] Another example of an area needing a unique approach is Know Your Customer requirements. KYC obligations initially surfaced in response to voice communications through mobile handsets—typically identifiable to an individual. However, in the M2M context, most M2M applications are not identifiable to an individual and do not typically involve voice communication, except perhaps emergency calling from a "connected car" or a push button connection to a help desk. This is particularly true for industrial M2M applications. Another major difference with M2M applications is that the SIMs contained in M2M devices are mainly used to take measurements, retrieve data from sensors and transport that data to data centers. With billions of SIMs and M2M devices to be deployed in the next few years (i.e., by 2020), tracking possession or control of a SIM will not be practicable. It is unlikely there will be enough computing power or data storage to track this information, and tracking it will stifle economic development. Therefore, alternatives to standard KYC requirements are needed for M2M applications, including potential exceptions under certain conditions.

[13] Policies, such as those to promote an open internet, should be sufficiently elastic so as not restrict the deployment of M2M services. Specifically, so-called net neutrality guidelines should allow flexibility for the provision of specialized business services (i.e., a premium business service that offers a higher level of quality at a higher price). In fact, various jurisdictions that have reviewed open internet policies have proposed to exempt specialized services. For example, in the United States, the Federal Communication Commission's *Open Internet Orde*r, excluded specialized services. *See* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1_Rcd.pdf, at para. 35.

[Spectrum

Spectrum is an essential building block for M2M device connectivity. Ubiquitous, affordable, high-speed broadband connections over licensed and unlicensed airwaves is crucial to enable consumers and the public and private sectors to benefit from this emerging technology format throughout the IoT ecosystem. Thus, effective and technologically neutral management of this increasingly scarce resource must be a priority for policymakers.

On the issue about spectrum and its requirements under M2M/IOT,, it is to be noted that the projected number of IoT devices will place additional demands on spectrum resources, requiring a continued growth in spectrum available for general commercial use, both licensed and unlicensed. Even if just ten percent of the total number of IoT devices were to be directly connected to commercial mobile networks (i.e., with a SIM card and on a 3G/4G/5G network), that still represents billions of new devices operating on wireless networks worldwide. Additionally, the absolute growth in, and the heterogeneity of, IoT traffic will combine with the continued growth in overall demand for mobile broadband to pressure licensed spectrum resources. Similarly, a very high portion of those devices that are *not* directly connected to commercial mobile networks—though they may be indirectly connected via gateway devices that are on a commercial mobile network—will be using unlicensed or non-commercially allocated spectrum.

However, there is no need for governments to allocate dedicated spectrum specifically for IoT or IoT segments. Government should continue efforts to find and reallocate spectrum for commercial mobile broadband use. Provided that sufficient licensed spectrum is allocated for mobile broadband use, there is no reason to expect that dedicated spectrum to support IoT devices should be needed: it should be left up to spectrum licensees to manage and employ their spectrum in an optimized fashion for the mix of traffic types that may be simultaneously using licensed bands. Government should continue to support the progress being made by industry standards bodies in the development of new standards, and work toward international harmonization of spectrum allocations where appropriate.

Questions

M2M Service Provider Framework

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?

TRAI has in the current consultation under clause 1.2 stated that “M2M communication has potential to bring substantial social and economic benefits to governments, citizens, end-users and businesses”. TRAI has further stated under clause 1.3 that “Although forecasts indicate a significant opportunity in this field,

this industry us still in a nascent stage. The M2M ecosystem is composed of a large number of diverse players, deploying innovative services across different networks, technologies and devices. Providing clarity and consistency of regulation for equivalent services, as well as policies that enable growth will play a significant role in fully capturing its opportunity to stimulate this market". Therefore it is imperative that such a nascent and emerging technology service format should not be placed under licensing or regulatory barrier which impedes its growth.

The provision of M2M communications encompasses a complex ecosystem of innovative players—most notably connectivity providers (mobile, fixed and satellite network operators), hardware manufacturers (equipment manufacturers and device manufacturers), software/application service providers (telematics, data analytics, billing solutions, etc.), and system integrators—that are developing new services and capabilities for the benefit of consumers, industry and society. Newer players, such as those companies providing networks based on low-cost, energy-efficient ultra-narrowband cellular networks or newly established solutions using drones[14] or power lines[15] continue to enter the market unabated. While these newer players, or traditional players with newer innovative solutions, may fall under a traditional moniker (*i.e.*, connectivity provider), their new solutions may not fit neatly into traditional network concepts and regulatory frameworks. Traditional, older connectivity solutions, e.g. cellular networks, should not be handicapped relative to new market entrant connectivity providers by being subject to regulations to which the new entrants are not subject.

Moreover, as the industry grows, policymakers should expect and encourage further innovations that will encourage investment and propel the IoT ecosystem forward. Indeed, having a pro-investment climate open to diversity is essential for India to capitalize on the global M2M opportunity to meet its ambitious Digital India program to "transform India into a digitally empowered society and knowledge economy."[16] Importantly, M2M will be a key enabler of Digital India, as well as India's other development and growth programs. Moreover, with India's prominence as a global offshoring hub—including providing backend IT support for most companies—there is significant scope for job creation, resource efficiency gains, and technical innovation.

Because of the diversity of solutions and potential MSPs, the best path forward is to encourage market entry and investment. And the best way to encourage market entry and investment is to have a clear, predictable and proportionate approach to MSP designation. AT&T, therefore, supports a light-touch

[14] *See* AT&T Blog, *Taking Flight with Connected Drones: AT&T Foundry Envisions the Future of Unmanned Aerial Vehicles*, May 2015 at http://about.att.com/innovationblog/connected_drones

[15] AT&T announced a new approach to smart grid applications and connected experiences. *See* AT&T Press Release, *AT&T Labs' Project AirGig Nears First Field Trials for Ultra-Fast Wireless Broadband Over Power Lines*, September 2016 at http://about.att.com/newsroom/att_to_test_delivering_multi_gigabit_wireless_internet_speeds_using_power_lines.html

[16] *See* http://digitalindia.gov.in/

regulatory framework that requires a simple notification to DoT, such as that used for Other Service Providers (OSPs).

There are many different kinds of companies that are involved in the provision of M2M services. Generally, the MNOs provide the connectivity part of the M2M service as a telecom operator along with the SIM provisioning and related billing services. Licensing for the service provided by MNO is, therefore, related to its role as a telecom operator and provider of connectivity services.

In our experience globally, no unique licensing is required for M2M Service Providers[17]. If an M2M Service Provider is a mobile network operator or a virtual network operator ("VNO"), they will be licensed and regulated as such. The provision of the telecom service is already regulated through the licensing of the MNO or VNO. Any other party in the supply chain is merely a subcontractor of the product manufacturer. The product manufacturer is regulated by rules on product safety and homologation and should not be further regulated as one who merely uses the connectivity of an MNO for its own internal purposes (is, essentially, a consumer of those services) or to enable capabilities within a device or product it distributes.

If M2M Service Provider registration is required, then it is the enterprise who first puts the wirelessly enabled finished good on the market in India who should be responsible to register as an M2M Service Provider and to pass along, through its supply chain, requirements for reporting information needed to satisfy its KYC compliance requirements. Again, since the communications part will always reside with MNO or VNO, the M2M Service Provider should work with the MNOs/VNOs to ensure DoT requirement on KYC/traceability, etc., are met.

There are far too many stakeholders involved in the M2M chain apart from MNO/MVNO like System Integrator (Sis), software developers, vendor companies, solution providers, distributor or sellers, etc. To require registration by each of them would result in a vast bureaucracy, drive up social costs unnecessarily and undermine efficiency. None of these entities should be required to register with DoT.

At least initially, an authorization / registration and not license framework should serve as a means to collect statistical information for identifying the number of M2M players in the industry.

As note just above, in general, we are aware of only one or two jurisdictions that require registration, authorization, unique licensing or a special license category for MSP. In many cases, the MSP is an MNO or a Mobile Virtual Network Operator ("MVNO"), and they will be licensed and regulated as such. The

[17] Singapore, as the TRAI notes (Consultation, at 2.10), is one country that has such requirements. However, in contrast, the United States, Australia, New Zealand and Canada do not, nor have any of them ever announced that is it currently considering, licensing or registration for M2M service providers. The same is true throughout Europe, which even for MNOs operates under a notification and compliance, rather than licensing, regime. Nor are we aware of any instance of M2M Service Provider registration or licensing in Latin America.

provision of the M2M connectivity (*i.e.*, the telecom service) is already regulated through the licensing of the MNO or MVNO.[18] Where an MSP uses the underlying network facilities of a licensed MNO or other Telecom Service Provider ("TSP"), directly or through an MVNO, the MSP is a non-network service provider who could register under the OSP category with the Department of Telecommunications ("DoT").[19] With this approach, responsibility for compliance with the telecom regulations appropriately belongs to the MNO, TSP or MVNO and not the MSP, unless the MSP is found to be in non-compliance from a use perspective. Finally, the definition of an MSP should be limited to the provision of M2M services to third parties. This distinction would exclude the need for M2M devices used exclusively internal to an organization (*i.e.*, not sold as a product to a third party). Unless the MSP provides a service to a third party, many businesses using M2M applications for self-use could be unnecessarily subject to registration.

AT&T believes a simple MSP registration[20] under the OSP type light touch registration category provides the DoT with a starting point for identifying the M2M players in the industry. This flexible approach gives the DoT and TRAI insight into the M2M services market in India without being unduly burdensome. To summarise below are the specific reasons why M2M MSP should not be linked to a UL or UL-VNO.

1. VNO is essentially a licensing requirement. It comes with a cost of US$1.1 million and multiple compliances. Making VNO a precondition to M2M MSP Registration, is an attempt to reduce competition and erect an entry barrier where none-exist and none are needed. Moreover, VNO in India has been structured for using voice resale.

2. The reason why VNO option was perhaps not considered by DoT during the formulation of the draft M2M MSP Guidelines was they do not wanted to restrict innovation, growth and competition by burdening M2M ecosystem with legacy voice linked license regime.

3. M2M is at very early stages of development. It requires very light touch regulation. Any regulation beyond that would be considered heavy handed, and dampen the ecosystem for investments due to costs, compliance and other related issues, included in the UL VNO licensing specifications.

4. M2M business is very different from voice. M2M is a high volume and low ARPU business. UL-VNO license has huge financial entry cost (Entry Fee of INR 7.5 crores (USD 1.2 Million), Recurring license fee and spectrum charges totaling to 13% approximately, coupled with bank guarantee cost will make the M2M business unviable.

[18] Notably, quality of service, law enforcement requirements and other regulatory measures are addressed through the MNO network license.
[19] The MSP could either be a licensed entity or a registered agency with the DoT. Consultation, at 2.5.
[20] As a practical matter, an MSP registration would require a review of each product or service. It would be an administrative burden, and could substantially delay innovation, if an MSP were required to register separately for every new service. Moreover, an MSP should have the flexibility to offer services with the most viable technology available.

5. As against the usual Unified License (UL) which is valid for 20 years, the VNO license is valid for just 10 years. This is a very short time period to even break even when the usual telecom license takes atleast 12-15 years to breakeven.

6. There is no need for having any substantive domestic infrastructure. This is also envisaged in the draft M2M SP Guidelines. However under UL-VNO, there will be requirements for every M2M SP to install mandatory infrastructure much beyond what may be needed or envisaged under the draft M2M SP guidelines.

7. Globally there are no precedents of having a separate license for providing M2M based services or making VNO a precondition for providing such services.

8. A UL-VNO in India for M2M suggests that devices will work solely on the underlying cellular connectivity. GSMA and Machina Research 2016 confirms that by 2021 there will be merely **8.4**% connected devices on cellular connectivity. This implies vast majority of the potential M2M service providers who neither come from the traditional telephony business nor wish to offer voice as a part of their portfolio.

9. Other connectivity options (sensors, RFID, blue tooth, zig bee protocol etc.) are expected to proliferate the M2M connectivity in a significant manner. Provisions for these connectivity options donot require any telecom license or authorization.

10. M2M is inherently a global business which requires regulatory policies to reflect the global essence, such as recognizing and facilitating cross border data flow, amongst many other requirements. The inherent restrictions in voice related licensing framework do not always permit free flow of cross border data and would be inappropriately applied to M2M MSPs

11. It is estimated that there will be 50 billion connected devices by 2021. Apart from the uniform underlying connectivity piece there will be multiple M2M based applications. The telecom license can only regulate the underlying connectivity which is already part of the license provided to mobile operators. Consequently, no license should be prescribed for the application part.

12. M2M application works on connectivity neutral platform. The device will work so long as there is underlying connectivity (from any operator). A UL-VNO will ensure that the M2M application is tied to the specific connectivity resources provided by the parent MNO, with the effect of restricting the widespread use of M2M application / services. This is at variance with the draft M2M SP Guidelines offered for public consultation, by DoT.

13. An M2M application / device will work or roam on the connectivity provided by mobile operators (access). The UL-VNO license restricts multiple MNOs for access services. This will restrict the growth of M2M services as it will not be able to benefit from synergies due to multiple connectivity providers (MNOs).

14. Any telecom license carries a host of compliance requirements spreading from technical, financial, commercial, etc. Non-compliance attracts heavy penalty. The current licensing framework does not align with the requirements of M2M business.

Roaming

Q8. In [the] case of M2M devices, should:

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

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

(c) [Should] there be a timeline/lifecycle of foreign SIMs to be converted into Indian SIMs/eUICC?

(d) [A]ny other option is available? Please explain implications and issues involved in all of the above scenarios.

As previously discussed, the business models for M2M communications, and the broader IoT market, have unique challenges. Presently, these challenges are being effectively addressed by M2M device manufacturers and the wireless industry through various solutions, including the use of roaming. AT&T believes that the use of so-called permanent roaming[21] as a technical and commercial platform brings unparalleled efficiency for the deployment of M2M communications across the globe. Moreover, in most cases, without roaming M2M applications simply may not be viable. Therefore, in order to facilitate the growth and development of M2M services, as well as to mitigate unnecessary demand for numbering resources, the TRAI should explicitly allow the extra-territorial use of national numbering resources (*i.e.*, E.212 and E.164 number resources).[22] This will foster M2M objectives that are broadly important to the Indian government, such as advances in agriculture. Notably, agriculture is one of many industries being transformed by the IoT.[23]

To illustrate, in order to achieve the necessary economies of scale, M2M device manufacturers often seek to partner with a single MNO that can deliver wireless connectivity in all, or nearly all, of the countries where the M2M manufacturer seeks to sell its products. By relying on a single MNO for its global wireless

[21] Roaming is considered 'permanent' in the context of M2M or IoT applications, as opposed to temporary roaming used while traveling.

[22] The TRAI highlights that there are global commercial models between mobile operators that provide a practical solution for "accommodating and facilitating the extra-territorial use of IMSIs and MSISDNs on a bilateral commercial basis." Consultation, at 2.35.

[23] Jahangir Mohammed, *3 Industries Being Changed by the Internet of Things (16 June 2015):* "Amid the global water crisis, agricultural irrigation also stands to benefit greatly from IoT innovation. The World Economic Forum recently identified water scarcity as the top threat to prosperity, and in most locations around the world, agriculture accounts for 90% of water consumption. Whether we achieve sustainability through new policies, investment in new infrastructures or a combination of methods, technology will be part and parcel of the solution." *See* https://www.weforum.org/agenda/2015/06/3-industries-being-changed-by-the-internet-of-things/

connectivity needs, the M2M device manufacturer can negotiate one wireless connectivity contract, use one Mobile Country Code ("MCC") and Mobile Network Code ("MNC") for the IMSIs in all of its SIMs (*i.e.,* E.212 resources), use Mobile Station International Subscriber Directory Numbers ("MSISDN") (*i.e.*, telephone numbers or E.164 resources) sourced from one MNO (if needed for its M2M product), and use the ordering, provisioning and billing systems of one MNO in delivering its IoT products globally. This single platform, or "global SIM," approach to M2M service deployment substantially reduces barriers to market entry for M2M device manufacturers, particularly for those smaller entrants who would not otherwise have sufficient resources to compete on a global scale.[24] As discussed further in response to Q11 below, the wireless industry is already helping M2M manufacturers achieve their goals for efficient international operation with a variety of commercially available solutions. India should support this effort.

AT&T believes that permanent M2M roaming with foreign numbering resources is one of the most effective methods to facilitate the deployment and development of M2M services and the IoT at large. We, therefore, see no need or, indeed no benefit, to mandating the eventual migration to Indian SIMs. First, India's consumers and businesses risk exclusion from the benefits of the global M2M marketplace if rules were to prevent the delivery of M2M services in India that use foreign IMSIs and numbering resources. Likewise, Indian device manufacturers would be deprived of global export markets if prevented from the delivery of M2M services outside India using Indian IMSIs. Without a flexible policy in this area, India's efforts to develop a broad national M2M policy will be compromised because the proliferation of global M2M services in India will be significantly impaired, as will the global prospects for M2M services developed and originated in India. Second, as the M2M and IoT market is evolving, it does not seem necessary to impose regulations on a timeframe within which a transition to an Indian SIM is required when a solution may be on a path toward obsolescence prior to the transition period's expiration. AT&T, therefore, urges the TRAI to adopt the extra-territorial use of global numbering resources for M2M devices, without a mandatory transition to an Indian SIM, as a priority.

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?

AT&T wishes to highlight that commercially negotiated bilateral roaming arrangements that enable customers to receive service outside their home country have been in place for decades and are mutually

[24] From the perspective of the M2M device provider, the desire to use a global SIM in this context is both logical and efficient. IMSI codes are merely a way to identify (i) the subscriber of the service (last 9 or 10 digits) and (ii) the network operator to whom the subscriber is subscribed (first 5 or 6 digits). E.164 numbers are merely an addressing scheme used to route calls to the appropriate destination and to identify the home network operator for purposes of billing. Using IMSIs and E.164 numbers sourced from a single MNO accomplishes the twin numbering goals (identification and addressing) in a much simpler, cost-effective manner than would be possible using traditional business models with unique IMSIs and E.164 numbers for each country.

beneficial to the participating MNOs: the MNOs' customers receive service in foreign countries and the MNOs receive compensation from the other party for providing the service. Generally, commercial considerations and not regulatory mandate drive adoption of innovative and efficient infrastructure sharing models, such as network roaming. Typically, roaming arrangements are made at the discretion of the MNOs to their mutual benefit. Benefits include reducing operating costs, expanding network coverage into unserved geographic areas and provision of new services. Absent any findings of anti-competitive behavior (*e.g.*, collusion, abuse of dominance, margin squeeze), the rates for international roaming charges should be based on commercial agreement between the MNO partners. In view of the availability of commercial roaming possibilities in India, AT&T does not see any need for regulatory intervention in terms of setting international roaming rates.

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

AT&T agrees with the TRAI that there are existing, well-defined and well-established commercial roaming models used between mobile operators that provide a practical basis for accommodating and facilitating the extra-territorial use of IMSIs and MSISDNs on a bilateral commercial basis.[25] Foremost among these is the international M2M roaming framework that addresses and makes transparent international roaming used explicitly for M2M services. The roaming framework, currently the most efficient manner of delivering global M2M service, enables the use of the home carrier's IMSI and MSISDN to provide services on a global basis through a single (global) SIM architecture. This architecture allows the most innovative devices, from large or small companies, to be deployed to any country in the world, thereby bringing the benefits of leading-edge technology to all countries, businesses, mobile operators and citizens. With the business models used for M2M, where end users typically do not pay for data transport, the traditional policy considerations relative to the level of roaming charges are not relevant. Under the M2M roaming framework—recognized by the wireless industry association, GSMA, and endorsed through the MNOs' adoption of an M2M Annex—procedures are in place to transparently identify, measure and distinguish M2M roaming traffic from traditional handset or tablet roaming traffic. The international roaming framework has been globally adopted by hundreds of MNOs who currently enjoy the bilateral benefits of offering these services.[26] Moreover, this bilateral framework has enabled large and small manufacturers

[25] Consultation, at 2.35. Notwithstanding the acceptance of roaming for the delivery of M2M services, roaming should not be viewed as the only means to facilitate the provision of international M2Mproducts and services. So long as the parties mutually agree, MNOs should have the flexibility to develop other commercial arrangements whereby M2M services are supported via the extra-territorial use of numbering resources (*e.g.*, resale).

[26] Today, AT&T has bilateral roaming agreements in place with MNOs worldwide. These agreements support the provision of international M2M and IoT services, with virtually all agreements using the GSMA M2M Annex. Pursuant to these agreements, the MNOs, their M2M or IoT customers, and the customers' end users enjoy the benefits of international M2M roaming in each other's country. These types of arrangements are fast becoming

alike to develop and export devices around the world, and to scale their business without the upfront entry barrier of establishing a distinct platform for each country before selling a single device. Thus, global roaming for M2M applications use promotes robust competition, and ensures competitive telecommunications markets because MNOs will continue to compete with each other to provide an international roaming platform for MSPs. Meanwhile, visited network MNOs benefit from the revenue earned from roaming traffic on their network.

Furthermore, there is increasing acceptance of and precedent for the extra-territorial use of national numbers and international roaming to deliver wireless services as regulators become more familiar with how M2M services differ from traditional mobile-based voice service. As the TRAI cited, the German regulator, BNetzA, recently issued new rules to allow the extra-territorial use of IMSI codes.[27] Indeed, after thoughtful consideration of extensive industry input and review of the factual merits and policy objectives, BNetzA issued new IMSI rules. These rules adopt three important and forward-looking policy precedents: (1) the extra-territorial use of IMSI codes for M2M applications, (2) not imposing a separate and specific notification requirement for the extra-territorial use of IMSIs for M2M applications, and (3) the ability of MVNOs to directly apply for IMSI codes. Notably, BNetzA just issued a draft decision to also allow the extra-territorial use of E.164 numbers.[28] And most recently, in December 2016, the Italian regulator, AGCOM, published a resolution to amend the Italian number plan to expressly allow the extra-territorial use of IMSI codes in the provision of M2M services. Like Germany's amended regulations, Italy's new rules, intended to accommodate market needs, allow for the supranational use of Italian IMSI numbering resources with a non-Italian MCC.[29]

Elsewhere in Europe, the Belgium regulator, BIPT, published a summary[30] of conclusions to its 2014 public consultation on the future of the Belgian numbering plan and confirmed its recommendation to formally

---

the norm in the industry, and their continued development and use on a voluntary, mutually-negotiated basis should be encouraged.

[27] Consultation, at 2.37. *See also* "Bundesnetzagentur Promotes Machine-to-Machine Communications Using Public Networks" [Press Release], 15 June 2016, available at http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2016/150615_IMSI.pdf;jsessionid=E5F0B1C360DA35FF0DF081B2EEC75059?__blob=publicationFile&v=2

[28] Draft decision *Extra-territorial use of foreign telephone numbers in the territory of the Federal Republic of Germany within the framework of machine-to-machine communication*. *See* http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/Mobile%20Dienste/Entwurf_Vfg_ExterritorialeNutzung.pdf;jsessionid=B3A309244E321303C5CDCB48E1F7361B?__blob=publicationFile&v=2 at 2.2 (German)

[29] *See* https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_kidx9GUnIodu&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_kidx9GUnIodu_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_kidx9GUnIodu_assetEntryId=6609734&_101_INSTANCE_kidx9GUnIodu_type=document (Italian).

[30] *Summary and further analysis answers to the consultation at the request of the BIPT Council of 25 November 2014 on reviewing the policy regarding the numbering plan management of 28 July 2015* ("BIPT Summary") at

introduce more flexibility in the extra-territorial use of numbering resources.[31] For M2M services in particular, BIPT calls for Belgium's Royal Numbering Decree to be amended to expressly authorize the permanent use of Belgian numbers abroad and of foreign numbering capacity in Belgium.[32] Contributing to BIPT's decision is industry consensus that there is market demand for the extra-territorial use of numbering resources[33] and, importantly, that the proposition does not pose any significant problems.[34] BIPT's approach does not involve any requirement for notification.

Regional policy forums also support the extra-territorial use of national numbering resources. In Europe, the regulatory body for the European Union, BEREC, acknowledges that allowing the extra-territorial use of national numbering resources appears to be central to the economic viability of M2M services.[35] And in the Americas, CITEL, recognizing that M2M communications drive economic and social development and constitutes a transnational market of services,[36] recommends that Member States allow the extra-

http://www.bipt.be/en/operators/telecommunication/Numbering/regulation/summary-and-further-analysis-answers-to-the-consultation-at-the-request-of-the-bipt-council-of-25-november-2014-on-reviewing-the-policy-regarding-the-numbering-plan-management-of-28-july-2015 (French and Dutch)

[31] BIPT's conclusions will need to be implemented via amendments to the Royal Numbering Decree. The revised legislation is expected to come into force in 2016.

[32] Article 8 of the Royal Numbering Decree will be amended to include the following statement: "The use on a permanent basis of Belgian numbers abroad and vice versa of foreign numbering capacity in Belgium is authorized for M2M applications." ("L'utilisation sur une base permanente de la capacité de numérotation belge à l'étranger et vice versa de la capacité de numérotation étrangère en Belgique est autorisée pour les applications M2M.") BIPT Summary (French version) section 10 at page 35.

[33] "A majority of respondents indicate the following items: 1) there is a market demand for the extra-territorial use of numbering resources; 2) there are no significant problems except for calls to emergency services." ("Une majorité de répondants indiquent les éléments suivants: 1) il y a une demande du marché pour l'utilisation extraterritoriale des ressources de numérotation; 2) il n'y pas de problèmes significatifs sauf pour les appels vers les services d'urgence.") BIPT Summary (French version) section 10, number 86 at page 29.

[34] BIPT concluded that "[t]he approach to allow the unconditional use of extraterritorial numbering resources on a permanent basis for M2M applications, both for the E. 164 [and] that for the E. 212, has no impact on the emergency services." ("L'approche pour permettre l'utilisation extraterritoriale inconditionnelle de ressources de numérotation sur une base permanente pour les applications M2M, tant pour les E.164 que pour les E.212, n'a pas d'impact sur les services d'urgence.") BIPT Summary section 10, number 91 at page 31.

[35] *BEREC Report on Enabling the Internet of Things*, Report BoR 16(39), 12 February 2016 at http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things, at page 19. BEREC also recognized and supported a finding from its consultation leading to this report that a majority of stakeholders favor the extra-territorial use of national numbers to support M2M services intended for a global market.[35] Report, at page 16.

[36] *Recommendation to Incentivize Greater Adoption of IoT/M2M Services in the CITEL Member States*, 28 Meeting of Permanent Consultative Committee I: Telecommunications/Information and Communication Technologies, Final Report (CCP.I-TIC/doc.4000/16), 14 July 2016. *See* https://www.citel.oas.org/en/SiteAssets/PCCI/Final-Reports/CCPI-2016-28-4000_i.pdf, at page 32.

territorial use of numbering resources—E.164 and E.212 numbers—to support global M2M and IoT business models and the development of innovated products and services.[37]

Finally, AT&T asserts that allowing the extra-territorial use, in both directions, of E.212 and E.164 numbers for M2M services is consistent with existing TRAI objectives[38] and does not compromise the ability of the TRAI to perform its statutory functions. In the first place, all cases of permanent roaming in India, as elsewhere, involve an Indian MNO that is directly subject to the jurisdiction of the national regulator. Furthermore, permanent roaming does not involve the purchase of a wirelessservice by a local consumer in the country where the subscriber (*i.e*., the device manufacturer) is roaming; rather the consumer is purchasing a product that contains a capacity for transport of data to or from the device contained in the product. In addition, other government authorities are likely to have oversight of the manufacturer selling the product that contains an M2M device to an end user, depending on the sector.

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?

AT&T believes that while there may be potential benefits to liberalizing some numbering assignment policies to extend the direct allocation of MNCs to MSPs, there are concerns in granting MNCs to parties other than telecom operators (*i.e.,* to M2M users or MSPs, rather than MNOs or MVNOs). According to BEREC, for example, allowing IoT users to be assigned MNCs raises questions of the technical and economic conditions of MNC assignees.[39] Operational and security issues also would need to be addressed, including what infrastructure requirements would apply to the M2M user, how would switching operate and with what risks, and what would be the impact on MNC resources.[40] Thus, before making any policy decisions, it would be prudent for the TRAI to observe what countries with more open MNC assignment polices have experienced relative to uptake and perhaps to consider a phased approach to changes in assignment policy.

AT&T also wishes to highlight that this measure is not necessary to avoid lock-in. Indeed, AT&T believes that over-the-air ("OTA") provisioning offers a preferable way to facilitate switching in the M2M space and highlights the progress that the industry has made in developing and promoting OTA capability since

[37] Ibid., at page 33.
[38] One of the major objectives of the TRAI is to "protect the interest of the consumers of telecommunication service." The Telecom Regulatory Authority of India Act, 1997 (24 of 1997), Chapter III, *Powers and Functions of Authority*, Clause 11(1)(i). Indeed, users of telecommunications services, whether enterprises or individuals, reap enormous benefits from the delivery of M2M services via a "global SIM."
[39] *BEREC Report on Enabling the Internet of Things*, Report BoR 16(39), 12 February 2016 at http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things, at page 30. The TRAI also acknowledges there are "technical challenges in the implementation, allocation and utilization of various network codes." Consultation, at 1.31.
[40] Draft Report at 3.3.1, p.22

the first release of the GSMA embedded SIM specification.[41] With the embedded SIM or embedded Universal Integrated Circuit Card ("eUICC"), the profile of the SIM (which includes the MNC), can be changed over-the-air after manufacture, as the TRAI acknowledges.[42] This allows for changes to profiles of different MNOs over the life span of the product, preventing lock-in to the original MNO. What is important to note is no single business model will meet the needs of all service types or all market participants (*e.g.*, manufacturers, device distributors, systems integrators).[43]

Security

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.

Industry is keenly focused on the security issues around M2M services. Indeed, as devices become ever more connected it follows that security risks are likely to increase across the ecosystem. Threats can include unlawful interception of data transmissions, network and device denial of service attacks, malware infections and other forms of threats—with some as yet unknown. M2M security, therefore, is a necessity, but a prescriptive regulatory approach is not. In fact, any service provider or M2M solution failing to adequately address security from the outset (*i.e.*, security by design) will not have commercial success. For this reason, there are a wide variety of standards bodies and industry coalitions and working on security specifications for M2M.

In fact, the TRAI noted one such example: the "oneM2M" initiative—an international standards body[44] established with the goal of developing technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. With more than 230 members, including AT&T, oneM2M is focused on technical specifications for security, as well as privacy, aspects of M2M (authentication, encryption, etc.) and involves liaison relationships with other standards bodies such as 3rd Generation Partnership Project ("3GPP"), Broadband Forum ("BBF"), Home Gateway Initiative ("HGI") and the International Telecommunications Union-Telecommunications Standardization Sector ("ITU-T"). The Telecommunications Industry Association ("TIA") and the Consumer

[41] *See* http://www.gsma.com/connectedliving/profile-interoperability-now-included-within-gsmas-solution-for-remote-sim-provisioning/
and
http://www.gsma.com/newsroom/press-release/automotive-industry-adopts-gsma-embedded-sim-specification/

[42] Consultation, at 1.32.

[43] While the embedded SIM (*i.e.*, the ability to change the IMSI) may enable new business models, it should not dictate them. The global SIM model offers a superior solution to enable multi-country distribution of, for example, M2M devices.

[44] Consultation, at 1.16. Telecommunications Standards Development Society, India (TSDSI) is one of the eight pre-eminent ICT standards development organizations participating in oneM2M. *See* http://www.onem2m.org/

Electronics Association ("CEA") are also working on M2M standards. The Cloud Security Alliance ("CSA") has published several recommendations for security in the cloud which are relevant to M2M applications that are being deployed in the cloud. More broadly, there is ongoing mobile security standards work at various industry organizations including 3GPP, Alliance for Telecommunications Industry Solutions ("ATIS"), and the GSMA. In fact, the TRAI states that the GSMA developed IoT security guidelines that will "help service providers build secure services by outlining technologies and methods to address potential threats."[45]

AT&T also highlights that we—along with Cisco, GE, IBM and Intel—formed the Industrial Internet Consortium ("IIC"), an independently-run open-member consortium of technology innovators, industrial companies, academia and government focused on accelerating the development and availability of intelligent industrial automation for the public good. The IIC's scope of work includes influencing the global standards development process for Internet and industrial systems and building confidence around new and innovative approaches to security. Recently, the IIC released the Industrial Internet Security Framework, an in-depth cross-industry-focused security framework comprising expert vision, experience and security best practices.[46]

In addition to international efforts, the United States is engaged in national efforts. For example, the National Institute of Standards and Technology ("NIST") Cybersecurity Framework serves as the starting point on all security questions related to M2M services and the IoT. This voluntary Framework is built around the concept of risk management, which we believe is the best means to address cybersecurity, particularly given the rapidly changing nature of the threats. The Framework can be a useful tool for companies to evaluate their cybersecurity risks and build a risk management plan specific to their business.[47]

Privacy

Q13.(a) How should the M2M Service providers ensure protection of consumer interest in data privacy of the consumer? Can the issue be dealt [with] in the framework of existing laws?

[45] Consultation, at 2.52. Indeed, as the GSMA asserts, the mobile industry has a long history of providing secure products and services to its customers and wants to share that expertise with IoT providers. *See* GSMA IoT Security Guidelines at http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

[46] *See* http://www.iiconsortium.org/IISF.htm

[47] AT&T itself employs a cybersecurity risk management program that predates the NIST Framework and that relies upon many of the same widely accepted, international security standards that map to the informative references in the Framework. We use these standards to inform our internal controls that we then apply to our network systems and to help protect customer data. Thus, the Framework serves as a complement to that program. AT&T also has built on its experience with the Framework and the work we are doing with customers across many industries—as well as with our own IoT deployments—to promote better cybersecurity practices in the IoT ecosystem through a series of White Papers. *See, e.g.*, *The CEO's Guide to Securing the Internet of Things*, available at https://www.business.att.com/cybersecurity/

As with the issue of security, AT&T believes that there is no reason for prescriptive privacy regulations. Industry stakeholders—device makers, connectivity providers, application developers, and platform operators—are proactively engaged in voluntary and collaborative processes to provide appropriate privacy protections for M2M applications. Establishing this trusted environment for consumers will be crucial to commercial success, separate and apart from any policy frameworks for these issues. Indeed, with this broad variety of industry players, it will be impossible to regulate a path to effective privacy protection. Rather, those protections will depend on a robust multi-stakeholder process to define the practices that will engender consumer trust—and therefore adoption—across the system. Thus, for privacy concerns, as with security, government should opt for a common, M2M-wide framework that relies not on regulation, but rather on multi-stakeholder efforts that will facilitate development of effective privacy approaches. Indeed, AT&T has participated in a number of industry efforts to develop privacy guidelines.

A case in point in the United States is the development of a Smart Grid Privacy framework. In October 2012, the Future of Privacy Forum (FPF) announced a privacy seal program based upon a fundamental set of privacy principles incorporated in its Smart Grid Privacy Guidelines.[48] Aware of the critical need for privacy and security protections for sensitive consumer energy information, industry members proactively engaged in collaborative, self-regulatory efforts. FPF convened a diverse group of companies—including AT&T—to develop the privacy framework. FPF also requested input from utilities and utility regulators as interested stakeholders. The resulting Guidelines target companies that use consumer information to provide smart grid services (*e.g.*, companies offering home energy management, remote home control or security, smart thermostats and other services). Furthermore, the Smart Grid Privacy Guidelines are designed to help assure consumers that organizations using their information are employing best practices for security, privacy, and dispute resolution and are using consistent approaches to obtaining consent. As the Smart Grid example suggests, self-regulatory measures can deliver real progress toward a more comprehensive, consumer-centric approach to privacy.[49]

AT&T also stresses that to assess any approach to M2M privacy, the first step should be examining the privacy implications of the application in question, rather than treating all applications the same. Many M2M applications do not involve personally identifiable data and consequently present no meaningful privacy risk. When applying any privacy guidelines, therefore, a distinction should be made between strictly consumer applications (*e.g.*, wearable computing, quantified self, and home automation), which may require more stringent risk assessment, and business applications (*e.g.*, energy efficiency, cargo tracking, traffic management and road safety, agricultural monitoring, manufacturing processes), where

[48] *See* https://fpf.org/issues/smart-grid/

[49] A more recent example of a successful multi-stakeholder approach to addressing privacy issues in the IoT is the process NTIA convened for Unmanned Aircraft System ("UAS"). That process resulted in a consensus document setting forth privacy best practices. *See* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

the processing of personal data may be minimal or non-existent. More specifically, exclusively industrial IoT applications are unlikely to have consumer privacy implications. Thus, more rigorous requirements that might be applicable to consumer applications should not be imposed on industrial M2M services.

As stated above, given that security and privacy are central to the commercial viability of M2M services and the IoT, there is incentive for industry to proactively focus on such issues. Industry stakeholders like AT&T have a track record of committing to meaningful, voluntary efforts to improve security and privacy—and will continue to do so. Ultimately, the most productive approach to ensuring robust security and privacy standards is voluntary compliance with broadly accepted industry guidelines. Thus, any further standards efforts should (1) build on work already in progress relative to M2M security and privacy standards, (2) be an industry-led rather than a top-down regulatory standards-based model, (3) be flexible enough to accommodate innovation, (4) be ecosystem-wide as opposed to being narrowly focused on specific sectors such as mobile carriers, and (5) allow data controllers[NPA(1)][50] to determine the best approach for protecting consumer privacy. A good start for any action on the matter would be to establish an inventory of already established or in-progress best practices.

Spectrum

General Response

Spectrum is an essential building block for M2M device connectivity. And the projected number of connected M2M devices will place additional demands on spectrum resources, requiring a continued growth in spectrum available for general commercial use, both licensed and unlicensed. Indeed, if just ten percent of the total number of M2M devices were to be directly connected to commercial mobile networks (i.e., with a SIM card and on a 3G/4G/5G network), that alone represents billions of new devices operating on wireless networks worldwide. Additionally, the absolute growth in, and the heterogeneity of, M2M traffic will combine with the continued growth in overall demand for mobile broadband to pressure licensed spectrum resources. Similarly, a very high portion of those devices that are *not* directly connected to commercial mobile networks—though they may be indirectly connected via gateway devices that are on a commercial mobile network—will be using unlicensed or non-commercially allocated spectrum. However, while ubiquitous, affordable, high-speed broadband connections over licensed and unlicensed airwaves is crucial to facilitate M2M connections, there is no need for governments to allocate dedicated spectrum specifically for M2M generally or IoT segments. The Indian Government should continue efforts to find and reallocate spectrum for commercial mobile broadband use. Provided that sufficient licensed spectrum is allocated for mobile broadband use, there is no reason to expect that dedicated spectrum to support M2M devices should be needed. The Indian Government should also

[50] Data controllers may be the MNO, but could also be the device manufacturer, a third-party system integrator, a value-added reseller of ICT services, an unlicensed Wi-Fi network operator, and the like.

continue to support the progress being made by industry standards bodies in the development of new standards, and, where appropriate, work toward international harmonization of spectrum allocations.

Conclusion

M2M communications are already demonstrating the potential to massively improve efficiency,[51] productivity and social welfare in diverse fields. Indeed, the Government of India, recognizing the potential of M2M communications to advance all aspects of Indian society, enshrined M2M as early as 2012 in its National Telecom Policy ("NTP-2012").[52] And in May 2015, introduced the National Telecom M2M Roadmap[53] to guide the development of M2M-related policies. Today India boasts one of the world's fastest growing economies—as well as telecommunications markets—and is looking to harness the power of telecommunications as a "key driver of economic and social development in an increasingly knowledge intensive global scenario."[54] Therefore, as India develops a telecom platform to transform the country into "an empowered and knowledge=based society,"[55] it must adopt flexible, globally-minded, industry-driven and technologically-neutral policies to create conditions for pioneering technologies, services, business models and investment to flourish.

AT&T commends the TRAI for engaging stakeholders to inform regulatory policy to advance M2M communications and the IoT. The right policies will enable India's numbering resources to be used to the maximum benefit. AT&T would be pleased to answer any questions concerning these comments.

[51] As an example of such potential, according to Gartner, a U.S. research and advisory firm, by 2022 the IoT will save consumers and businesses US$1 trillion a year. *See* http://www.networkworld.com/article/3132015/software/gartner-s-10-strategic-predictions-for-2017-and-beyond.html

[52] "To facilitate the role of new technologies in furthering public welfare and enhanced customer choices through affordable access and efficient services delivery. The emergence of new service formats such as ***Machine-to-Machine communications***...represent tremendous opportunities, especially as their roll-out becomes more widespread" at 11.2 *See* http://www.trai.gov.in/WriteReadData/userfiles/file/NTP%202012.pdf

[53] *See* http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[54] NTP-2012, at page1.

[55] Ibid.