GSMA response to the draft BEREC Report for public consultation on enabling the Internet of Things

London, 6th November 2015

Introduction

The GSMA welcomes the BEREC report on enabling the Internet of Things (IoT) and the opportunity that it provides to contribute to the debate.

There will be over 2 billion M2M connected devices in Europe by 2019, these will represent roughly 50% of all connections but they will only generate 3% of the total traffic.1 Only a small fraction of connections will be based on cellular technologies. The GSMA intelligence estimates that by 2019 in the EU these will be only 140 million.

In this context, the GSMA helps operators to add value and accelerate the delivery of new connected devices to mobilise the IoT. This is being achieved by industry collaboration, optimising networks and developing key enablers to support the growth of the IoT.

The positive impact of the IoT on citizens, consumers, businesses, and governments promises to be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety. For example, a PWC[2] study shows that mHealth could save 99 billion EUR in healthcare costs in the European Union (EU) and add 93 billion EUR to the EU GDP in 2017 if its adoption is encouraged.

Governments can realise these significant social and economic benefits through the growth of IoT services by ensuring supportive policies and regulation that are relevant, flexible, and technology neutral. The GSMA produces a wealth of information on the IoT; its ecosystem, size and market development, as well as economic and technical reports. These are all key aspects that policymakers should usefully consider to maximise the benefits of this opportunity.

In the following parts of the document, you will find the GSMA position for IoT on selected topics which the BEREC report addresses and, in addition to that, there is an Annex that includes the answers to the questions that the consultation raises.

[1] CISCO VNI global traffic forecast : http://berec.europa.eu/files/document_register_store/2015/10/BoR%20(15)%20177_BEREC%20Stakeholder%20Forum-M2M-CISCO.pdf

[2] http://www.pwc.in/assets/pdfs/consulting/strategy/socio-economic-impact-of-mhealth-the-european-union.pdf

Executive summary

- The GSMA encourages the development of a **spectrum policy** environment based on certainty, predictability, and consistency for this nascent industry to grow in Europe. Spectrum harmonisation will be essential for IoT connected services as it enables global scale services and cost-effectiveness. Choosing the right spectrum, in particular, bands below 1GHz will play a crucial role in coverage all the while licensed spectrum will be essential to guarantee the quality of service for the different application.
- It is important that BEREC recognizes the **truly global nature** of these services. M2M users[3] most often require global distribution coverage and managed platforms for economic viability and the provision of consistent global services. The GSMA believes that all parties should have the flexibility to select a model that best suits their needs and no specific provisioning model should be mandated, promoted or imposed by regulatory action.
- For **numbering**, flexibility is essential as different services or M2M users may have different requirements. Both, extra territorial and international global numbers are being used to deploy IoT connected services. European regulators should refrain from introducing any undue restriction or administrative barriers related to the assignment and use of numbering resources, as it would act a barrier to the roll out of a pan-European M2M market.
- Some traditional consumer protection requirements commonly associated with **E.164 numbers, such as number portability,** are not needed or appropriate in the IoT context.
- Maintaining a flexible approach is also necessary in the context of connectivity. **Permanent roaming** is one of the viable connectivity models which facilitates the creation of the IoT market in Europe. However the ultimate deployment model choice depends on a number of factors, such as needs of the mobile network operator, the IoT service provider and the end-user, the scale and geographical footprint of the deployment, the type of IoT application, the device lifetime, its accessibility and the bandwidth requirements.
- On **switching**, when comparing different mechanisms to facilitate changing providers, it is the GSMA view that any relaxation of the current MNC policies should be carefully assessed in light of its costs, and its technical and logistical complexities. The GSMA believes that its specification for remote provisioning of Embedded SIMs is more efficient and is likely to have lower implementation costs.
- On **privacy**, the GSMA believes that the current framework needs to be updated to achieve legal certainty for European consumers and a level playing field for all M2M players irrespective of sector and geographic location. The best way to achieve this legal certainty is to review the European Privacy Directive. In such review, it is essential to ensure that the same protection applies to the same services in a technology neutral way.

[3] We refer on this instance and throughout the document to BEREC adopted definition of M2M user: Purchaser of an M2M service who incorporates the M2M service as one component in his own products and/or services (e.g. a car manufacturer, an electricity provider who also includes a smart meter in his services).

Definitions

The GSMA agrees with BEREC that "*M2M services are in varying phases of development and take various shapes, hence there is not yet a common understanding or definition of what M2M services and devices really are. For the purposes of this report, it is not necessary to determine in a detailed manner which definition is most appropriate.*"

The GSMA recognizes that in the existing literature, a number of definitions for M2M and IoT exists and by no means there is industry agreement on these terms definitions. exist. However, coherently with our previous communications to BEREC in this document, we use the following definitions:

Internet of Things (IoT): Coordination of multiple vendor machines, devices and appliances connected to the Internet through multiple networks. Devices include everyday 'objects' such as smartphones, tablets and consumer electronics, such as machines, vehicles, monitors and sensors equipped to support M2M services.

IoT Connected Services: are those delivered via devices where the connectivity is provided by authenticating a SIM and where the service has at least one of the following characteristics:

- Open internet or open voice communications are not the primary purpose of the service; mobile connectivity is utilised to deliver value-added functionality
  OR
- Services that have a closed user group and service provider managed connectivity which excludes open internet or open voice access

Machine to Machine (M2M): Devices and appliances connected wirelessly or via IP. In most cases, communication takes place autonomously, with limited human intervention. M2M is an integral part of the IoT.

Relevant, flexible and technology neutral policies

Governments and regulators will realise significant social and economic benefits through the growth of IoT services by ensuring policies and regulations are relevant, flexible and technology neutral.

The GSMA encourages that a pro-investment environment is established and maintained in Europe across the IoT value chain. In order to reach not only European but also global scale across consistent and reliable platforms, service providers, and IoT device manufacturers need a flexible regulatory approach that in turn would enable technical and commercial flexibility.

It is crucial to note that the IoT sector is a nascent industry and its value chains, business models, markets and services, are fundamentally different from traditional mobile voice and data messaging. In most cases, IoT services have a closed user group, whereby open internet or any-to-any voice communications are not the primary purpose of the service. In addition, customers are generally not the service end-user, but a business that requires global distribution coverage and managed platforms for economic viability and the provision of consistent global services. Finally, these services are characterised by significantly lower average revenue per connection than traditional voice and messaging.

In addition, regulation should avoid technology restrictions, while relying on competition. Excessive or technology biased regulation can stifle innovation, raise costs, limit investment and harm consumer welfare. Therefore, we encourage BEREC to support a policy framework that is based on equal services and technological neutrality.

Spectrum Policy for IoT

The GSMA encourages the development of a fertile European spectrum policy environment centring on certainty, predictability, and consistency for this nascent industry to grow in Europe.

The GSMA agrees with BEREC that M2M services have different spectrum requirements. Indeed, M2M has very different characteristics, a plethora of existing and planned technologies as well as diverse spectrum usage and access methods. Mobile cellular solutions already play a significant role given M2M can operate in spectrum allocations intended for mobile. In addition, a number of harmonised standards have been developed recently (e.g. 3GPP or GERAN) to optimise the use of mobile spectrum bands for IoT. Thus, the mobile industry is an important enabler and well placed to lead the sector, in particular for Connected Cars and Mobile Health.

In particular, machine-type communication (MTC) extensions to LTE are emerging, including category 0 devices in releases 12 and 13, providing enhanced coverage and power options, operating in licensed spectrum, which will meet a much wider range of M2M requirements. This will provide operators with greater predictability than the uncertainties implicit in licence-exempt bands.

Licensing regime and Quality of Service

Cellular based MTC solutions should be developed to operate in existing licensed spectrum bands, to allow operators maximum flexibility in the use of their spectrum, while providing adequate quality of service for critical applications. M2M connectivity uses wide area, local area, and personal area wireless technologies, either individually or in various combinations to meet the requirements of a given M2M application. In the near term, proprietary Low Power Wide Area (LPWA) systems, operating in a combination of licence-exempt (LE) and licensed spectrum, will continue to serve some wide area M2M requirements, which are not met by existing cellular technologies. Such LE spectrum is however intrinsically not ideally suited to wide-area M2M applications: permitted power levels and

duty cycles are generally low and interference risks over long distance paths are high, especially as multiple systems from different operators proliferate. As such, the inherent nature of the LE spectrum makes it so that quality of service cannot be guaranteed.

Frequency bands

BEREC rightly targets the sub 1GHz spectrum, as it would be essential for M2M applications. However, the report also lists the licensed and licensed exempt (LE) bands in Europe as adequate for M2M applications and goes as far as including the lower part of the C-Band, suggesting big scope for growth. The GSMA would like to emphasise that in practice most of the bands that make the best case for M2M type applications will be in the sub-1GHz. The higher frequency bands are less optimal for M2M services while the lower ones are needed to enable for better coverage, limiting the options available further. In particular, wide area applications are good examples where spectrum below 1 GHz is needed for sufficient coverage as it allows those areas to be covered in a very cost effective manner.

To make the most of cellular M2M technologies there is a case for 'earmarking' some spectrum for M2M applications. This need not necessarily restrict its use to only M2M but could identify it as a default band for such applications. The 700 MHz band, European configuration is a clear candidate where compatibility studies are in hand to test the feasibility of the approach to dedicate 2x3 MHz band for M2M, following the results of the CEPT report[4]. Such earmarking would pave the way to address a market of several billion devices in the near future.

Harmonisation

Harmonisation is essential in personal mobile communications – but is arguably even more so for M2M devices. To drive prices for endpoints to levels, which can compete with LPWA technologies, devices need to support just one or two frequency bands and to achieve truly global - not just national or even regional – scale.

Currently there is no harmonised dedicated spectrum allocation for M2M and it is fitted in where it can be. To remedy this situation, operators are using spare capacity on 2G, 3G and 4G systems for M2M services within existing spectrum allocations. The GSMA supports harmonisation of frequency bands for mobile services as it would ensure the efficient use of spectrum while also galvanising the cellular IoT market by driving the widespread creation of low cost devices, which can be used worldwide. In order to realise this goal, regulatory bodies should work with the mobile and M2M ecosystem, including mobile network operators and vendors, to examine which bands should be harmonised and band plan considerations. Harmonised bands need to be able to support the full range of potential M2M scenarios. This includes high data-rate applications, which could require substantially more spectrum than forecasts based on today's usage profiles would suggest.

In this context, the GSMA recently announced the establishment of the 'Mobile IoT Initiative', a new project backed by 26 of the world's leading mobile operators, OEMs, chipset, module and infrastructure companies, designed to address the use of Low Power Wide Area (LPWA) solutions in licensed spectrum. The new group will work to accelerate the commercial availability of mobile IoT technology by facilitating demonstrations, proofs of concept and trials of a selection of complementary LPWA licensed spectrum technologies. LPWA technologies in licensed spectrum can be deployed in a simplified and cost-effective manner, without sacrificing key customer requirements, such as battery lifetime and security. Mobile operators already provide reliable end-to-end IoT platforms that allow customers to scale and manage their business requirements. They also have

[4] ECC Report 242

unrivalled global network coverage as well as technical and business support to react to a customer's changing needs.

Future Spectrum

5G will likely be the first cellular technology that will be optimised for M2M from the start and indeed M2M is one of the core drivers for 5G. Whilst at this stage there is little clarity about the performance, details and services are unlikely to commence until 2020 or beyond. Therefore, in the longer term, 5G is expected to play a crucial role in further M2M developments. This should include supporting vast numbers of M2M devices and improvements to signalling and spectrum efficiency as well as measures to reduce device cost. This will help drive applications, which require better quality of service guarantees, much lower latency, increased integration within the mobile network, and extended range. As such, 5G spectrum considerations must strongly incorporate M2M requirements. Policy makers should lend their full support to action at WRC-15 to place an item on the WRC-19 agenda to identify spectrum for 5G, with M2M as one of the prime motivations.

Global deployment models

The GSMA believes that all parties should have the flexibility to select a model that best facilitates a rapid and economically viable deployment of IoT services and provide a platform through which IoT customers can deploy high quality services worldwide while maximising economies of scale.

No specific model should be preferred, mandated, or imposed by regulatory action. All deployment model alternatives for IoT connected services considered by MNOs have their merit. The ultimate choice of deployment model depends on a number of factors, such as needs of the mobile network operator, the IoT service provider and the end-user, the scale and geographical footprint of the deployment, the type of IoT application, the device lifetime, its accessibility, and the bandwidth requirements.

The GSMA identified three main deployment models can be used to deploy IoT connected services:

- **M2M Roaming Model:** Use of a SIM from a single MNO in a device, and reliance on international roaming partners of that MNO, to provide connectivity outside of the MNO's home country. In this context M2M roaming, describes a situation where a mobile SIM is permanently connected to one or multiple visited networks, and does not regularly attach to its home network. The connectivity is provided through commercially negotiated roaming agreements as between mobile operators.
- **Localised Connectivity Model:** Use of domestic mobile connectivity made feasible in multi-national deployments through the use of the GSMA specifications, for the remote over-the-air (OTA) provisioning of Embedded SIMs.
- **Hybrid models**: Combinations and variations of the previous models where international roaming and localised connectivity are combined and where different commercial and technical arrangements are established

Each of these models are viable alternatives for global deployment of IoT services, depending on the service requirements, the MNOs' strategies and their customers' needs. Other technological solutions may become available in the short or medium term and provide valuable additional alternatives. Regulation, which prohibits particular technical or commercial approaches, should not be introduced.

Numbering

In relation to numbering, the GSMA would suggest that BEREC considers the following subjects:

- Supporting 15-digit MSISDN for growth
- E.164 - regulatory exceptions for IoT connected services
- Mobile Network Code (MNC) allocation policies

Supporting 15-digit MSISDN for growth

The GSMA notes that there is already widespread industry support for roaming M2M devices that use 15-digit MSISDNs. Standardised support in core network and roaming support systems, carrier and signalling providers, together with a competitive roaming marketplace, have ensured that MNOs with multi-national IoT deployments will not encounter any significant technical barriers due to the allocation of 15-digit MSISDNs to their IoT connected devices.

E.164 - regulatory exceptions for IoT connected services

Some of the requirements associated with the use of E.164 ranges are inappropriate for the large majority of IoT connected services and should not apply. For instance, for an electricity smart meter or an asset-tracking tool, some or all of the following requirements are neither required nor relevant:

- Reachable from any device on any other network
- Integration in public national numbering plans with associated pricing transparency rules
- Number portability
- Possibility to call emergency services
- Calling Line Identification (CLI) rules

Regulators should link any requirement to the nature of the service offered independently of the chosen numbering range.

MNC allocation policies

Mobile network codes (MNC) numbering allocation policies enabling the use of shared MNC should be carefully assessed in light of their implementation costs, and their technical and logistical complexities. The GSMA believes that its specification for remote provisioning of Embedded SIMs is more efficient and is likely to have lower implementation costs.

The GSMA specification for remote provisioning of Embedded SIM addresses concerns regarding the ability to switch connectivity providers for IoT connected devices. Technical solutions for changing connectivity provider are available today that eliminate the need to physically replace the SIM or to loosen MNC allocation policies. The use of a remote provisioning capability, such as that defined in GSMA Embedded SIM specifications, provides a solution that enables providers to select a connectivity partner at a later stage in the product lifecycle, i.e. when it reaches its customers, potentially in another country. It also facilitates ease of switching connectivity provider. The GSMA Embedded SIM specifications were developed specifically for large multi-national deployments where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical

Data protection and Privacy

To realise the opportunities that the IoT offers, it is important that consumers trust the companies who are delivering IoT services and collecting data about them. The GSMA and its members believe that consumer confidence and trust can only be fully achieved when users feel their privacy is appropriately respected and protected.

There are already well-established data protection and privacy laws around the world, which have applied to mobile operators for years. The GSMA believes that it is possible to apply existing data protection regulations and principles to address privacy needs in the context of IoT services and technologies.

However, IoT services typically involve more parties than simply mobile operators, such as device manufacturers, online platforms and even the public sector. It is important that there is regulatory clarity and legal certainty around IoT services and that privacy and data protection regulations apply consistently across all IoT providers in a service and technology-neutral way.

Regulators should support industry measures that identify and mitigate risks to privacy, and through which service providers can demonstrate accountability – such measures could include privacy enhancing technologies and tools that help consumers to manage their privacy and control how their data are used.

The data protection and security practices developed for a given IoT service should reflect the overall risk to an individual's privacy and the context in which data about the individual is collected, distributed, and used. Any regulatory interventions should be limited to areas where identified risks emerge and existing measures are insufficient to address these.

The GSMA and its members draw on their extensive experience in addressing privacy and security issues and work collaboratively with their IoT partners, such as device manufacturers, mHealth and mEducation service providers, to embed privacy and security into IoT technologies and the overall consumer experience. This on-going collaboration will ensure IoT industry partners are able to identify and mitigate the relevant consumer privacy risks in the context of the service being delivered.

Annex – Q&A

1. **How do you evaluate the three options mentioned in section 2.2.1.4 (extra-territorial use of national E.164 and E.212 numbers, use of global ITU numbering resources, use of a European numbering scheme) for the provision of M2M services? Which of these solutions is preferable to address the need for global marketing of connected devices? Should these solutions be used complementarily?**

a) The GSMA agrees with BEREC that numbering resources for IoT connected services are not scarce. The GSMA further notes that at present there is already widespread industry support for roaming M2M devices that use 15-digit MSISDNs. Standardised support in the core network and roaming support systems, together with a competitive roaming marketplace, have ensured that service providers will not encounter any significant technical barriers in deploying IoT connected devices using 15-digit MSISDN.

b) The GSMA believes that both models referred to in the question: the extra-territorial use of numbers and the use global numbers are important and respond to different M2M users requirements.

c) On the extra-territorial use of numbers, the GSMA agrees with BEREC's view that '*an internationally harmonised approach could be desirable'*. Furthermore, any undue restrictions or administrative barrier introduced by European regulators related to the assignment and use of numbering resources should be removed as it would act a barrier to the roll out of a pan-European IoT market.

d) The use of global ITU numbering resources is also an important alternative as a number of operators have deployed services based on these resources. As BEREC points out, the ITU-T assigns two-digit identification codes for global services provided by international networks under the shared country code +882.

e) The type of service to be offered to customers using this range is agreed with the ITU based on pre-determined criteria (e.g. the applicant must demonstrate that other reasonable technical and operational measures, such as use of national numbers, are not available). Therefore, the onus is already on providers to demonstrate this supranational requirement and that is why this range is attractive to multi-national providers of IoT connected services.

f) In addition, E.212 resources (IMSI) are also available, and parties may apply to the ITU for MNCs under the MCC 901 that can then be used in a 'country agnostic' manner.

g) The GSMA believes that a European specific numbering scheme is not necessary nor appropriate because:
   - Businesses deploying IoT solutions most often require global distribution coverage and managed platforms for economic viability and the provision of consistent global services;
   - As discussed above in points (d)(e) and (f) global/supranational numbering resources for IoT connected services are already available;
   - Introducing EU specific numbering ranges may disrupt scalability and increase deployment costs to the detriment of European consumers and businesses.

2. How do you regard the market situation in the M2M sector with regard to permanent roaming and national roaming?

a) The GSMA welcomes BEREC's position on permanent roaming, when it recognizes that roaming is currently being used for the provision of a number of IoT services and facilitates the development of this market.

b) The GSMA believes that at this early stage of development of the IoT market, all parties should have the flexibility to select a model that best suits their needs and no specific provisioning model should be mandated, promoted, imposed, or prevented by regulatory action.

c) As a general principle, the EU roaming regulation, as BEREC notes, is a consumer protection instrument applicable when services or devices likely to be '*travelling in the Union*' and delivered on a '*mobile device*'. It is worth noting that a similar interpretation is followed by the Commission in the *provisional agreement on the Telecom Single Market* (TSM). The TSM specifies that the roaming regulation is aimed at regulating *roaming services* used by *roaming providers' end-users while the latter periodically travel within the Union.*

d) The current provisions make no specific reference to M2M or IoT connected services and do not draw a distinction between person-to-person communications and IoT connected services. Nevertheless, while a wide variety of services and deployment scenarios may be possible, most IoT connected services do not meet the criteria identified by BEREC and the Commission for the roaming regulation to be applicable.

e) In most cases, IoT connected services have a closed user group, whereby open internet or any-to-any voice communications are not the primary purpose of the service. In addition, customers are generally not the service end-user, but a business that requires global distribution coverage and managed platforms for economic viability and the provision of consistent global services. For these reasons IoT connected services should be in principle excluded from the applicability of the roaming regulation.

f) BEREC also notes that the proposed Commission amendments to roaming regulation in the TSM by which*: '(…)the wholesale access obligation for such services* (i.e. regulated roaming) *does not apply for permanent roaming scenarios, but this does not prevent that operators may offer permanent roaming services on a commercial basis.*' It then explains that the future introduction of Roam Like At Home (RLAH) provisions may further exacerbate potential distortions to competition by i) increasing the risk of refusal to conclude roaming agreements ii) increasing the arbitrage incentives to use roaming access obligations as a substitute to national commercial MVNO access. BEREC therefore proposes to "*assess, in the context of the wholesale market regulation review, an approach where permanent roaming would be made explicitly eligible to the wholesale access obligation, but would not benefit from the wholesale price control, or would only be subject to the certain wholesale cap levels still to be set."*
The GSMA believes that:

   i. The evolution of IoT connected services delivered through mobile communications networks in Europe should be progressed through the current process of bi-laterally agreed commercial negotiations.
   ii. There is no need for intervention without prior demonstrable evidence that the industry is failing to address market needs, for example by refusing to negotiate roaming agreements. Existing ex-post competition law is sufficient.

g) BEREC further states that "*there seem to be no access and pricing issues related to M2M connectivity with regard to the Roaming III*".

It is worth nothing that:

   i. The current roaming regulation imposes wholesale charging for voice and data services to be based on generated traffic. However for M2M and IoT connected

services alternative charging models may be more suitable and better reflect the specific needs of this industry (for example a fixed fee plus a lower, traffic-related fee).

ii. The operator's ability to choose any charging mechanism and business model for these services should not be constrained by regulatory action. All parties should have the flexibility to negotiate the most suitable and appropriate charging mechanism for IoT connected services.

h) BEREC furthers suggests that '(…) *on certain national markets there seem to be competition distortions stemming from the fact that the roaming operator could benefit from the coverage of all the visited networks, while visited networks in the absence of national roaming are often prevented from doing so themselves. The use of permanent roaming might in some instances reflect the absence of national roaming*'

i. The GSMA considers that the use of permanent roaming does not reflect the absence of national roaming arrangements. Instead, it reflects the truly global nature of IoT connected services and the need to use a deployment model, which enables economies of scale, efficiency and reduces logistical and platform management issues.

ii. As such, the GSMA does not believe that there will necessarily be 'competition distortion' at national level through use of non-national M2M numbering.

iii. It should be noted, that the arbitrage opportunity between regulated roaming and national commercial MVNO access is being created by an artificially low (regulated) roaming tariff. Introducing *additional* regulatory measures (such as an access right for M2M permanent roaming) to compensate a distortion caused by a *previous* regulatory measure would be unjustified and create enduring regulation that does not assist in facilitating the developing this market.

iv. Any issues that arise in this area should be addressed within the industry, not via regulatory intervention. Additional regulation should only be considered if there is evidence of market failure and in line with the 'three-criteria-test', which is a well-established procedure in the EU. The forthcoming review of the wholesale roaming market will be the appropriate place for such assessment.

3. Which solution – OTA provisioning of SIM or MNC assignment to M2M users – do you think is preferable to facilitate switching between connectivity providers in the M2M sector? Which advantages, which disadvantages are attached to the two solutions?

a) A few introductory considerations are necessary. First, it is worth considering whether switching costs are indeed a key feature of a competitive M2M environment.[5] Given the wide variety of existing IoT applications, a straightforward answer may not be possible. However, for most of them, the connectivity element is only an enabler, a feature embedded in the service, and not the key aspect of the value proposition.[6]
b) Second, most IoT connected services are based on B2B or B2B2C models. M2M users are most often businesses with a sufficient countervailing buying power to negotiate appropriate contractual terms, such as the contract lengths and applicable switching mechanisms with their connectivity partners. No regulatory protection is necessary in these instances.
c) Thirdly, even if it was established that switching costs were a key features of IoT connected services, any measure aimed at lowering those costs should be designed and implemented so to apply consistently regardless of the technology used, and not just apply to cellular based IoT connected services.
d) Looking into the advantages and disadvantages of the two solutions referred to in the question, the GSMA acknowledges and agrees with BEREC's analysis of the direct MNC assignment model. In the section dedicated to numbering, above, we report the GSMA views on Mobile Network allocation policies: "MNC numbering, allocation policies enabling the use of shared MNC should be carefully assessed and in principle avoided in light of their implementation costs, and their technical and logistical complexities."
e) In addition to the challenges identified by BEREC, the GSMA has also identified the following disadvantages (these relate specifically to solutions based on shared MNC/HLR proxy) :
    a. The model may require significant time to be defined, standardized and to be set up and made operational;
    b. It presents high security and fraud risk connected with private parties being assigned numbering resources, procuring and issuing SIM cards;
    c. It may cause potential increased signalling load on other national networks;
f) With regard to OTA provisioning, BEREC observes that "*no process have been agreed between MNO which would enable an MNO to re-programme a SIM of a customer of another MNO.*" On this point, it is worth noting that the GSMA has produced a White Paper – a Business process document - identifying and defining potential approaches to these processes. The document is publicly available on the GSMA website.[7]
g) The GSMA has also defined technical specifications for remote SIM-provisioning, now at their third version and including interoperability between SIM vendors.[8]

[5] To put this statement in context: Would for example a user of a smart meter find it useful or even consider changing the connectivity provider of its device? Would the user of fitness wearables ever consider connectivity for their devices?
[6] For example a diabetic using a IoT based mHealth glucose reader finds it useful to have its glucose readings taken from home without having to operate manual readings and send them to his physician.
[7] At the link: http://www.gsma.com/connectedliving/wp-content/uploads/2015/02/CLP-05-v1-0.pdf
[8] More details can be found at this link: http://www.gsma.com/connectedliving/profile-interoperability-now-included-within-gsmas-solution-for-remote-sim-provisioning/

4. **Do you think there is a need to adapt Art.13a of the Framework Directive to address security concerns in the M2M context? If so, which adaptations do you consider to be useful?**

a) The GSMA believes the security is vital to building and maintaining consumer confidence in mobile services to date and will be as critical to the success of IoT connected services that have the potential to support and deliver increasingly sophisticated and security sensitive services.
b) It is important that robust security measures are extended to the whole value chain of the IoT market, including device and chip manufacturers and software vendors, who are equally part of the IoT value chain. Reducing vulnerabilities in devices, applications, and web services to ensure IoT connected services provide end-to-end security should be a priority for all parties.
c) In consideration of the key principles above the GSMA considers that the obligations stemming from art 13a of the Framework Directive should not be amended. It is important however to ensure that these obligations apply, consistently across all IoT providers in a service and technology-neutral way.

5. Do you think there is a need to adapt the Privacy Directive and ePrivacy Directive to address privacy concerns in the M2M context? If so, which adaptions? Do you think that the reform of the Privacy Directive as foreseen in the Council's General Approach of 15 June 2015 on the future General Data Protection Regulation goes in the right direction?

a) The GSMA welcomes BEREC's conclusion that "*the respect and protection of end-users' privacy is a critical success factor for the realisation of the prospects and growth of M2M services*" and agrees with BEREC's assessment that there is no need to deviate from the basic principles of data protection law in the M2M context.

b) Overall, the GSMA believes that the data protection and security practices developed for a given IoT connected service should reflect the overall risk to an individual's privacy and the context in which data about the individual is collected, distributed and used. Any regulatory interventions should be limited to areas where identified risks emerge and existing measures are insufficient to address these.

c) Furthermore, there are initiatives underway which are addressing potential issues associated with privacy and security in the IoT context. One such example is the Alliance for Internet of Things Innovation ('AIOTI'), which has been set up by the European Commission. The GSMA is part of the Policy Working Group, which has made a number of policy recommendations on how industry can address potential privacy challenges associated with IoT, including through the creation of an AIOTI Privacy Knowledge Base that will contain best practice on application of Privacy by Design methodologies.

d) The GSMA believes that the realisation of full benefits of IoT in a data driven economy will rely on the ability to do analytics in the IoT context, which will need to be balanced with relevant security and privacy considerations, including protection of confidentiality of communications, to ensure a trustworthy and sustainable IoT business and technology environment.

e) However, the GSMA believes that the current data protection regulatory framework in Europe (i.e. the sector-specific applicability of the ePrivacy Directive (EPD) as opposed to the general rules within the 'Privacy Directive' (95/46/EC), as outlined in BEREC's consultation, imposes additional obligations on the provider of the 'electronic communications service' (ECS) underlying any IoT connected service in public communication networks, i.e. the connectivity service provider. This inconsistent applicability of the rules – which do not apply to other players in the value chain – creates confusion for European consumers, whose privacy will be treated differently by the various companies accessing their personal data when using an IoT connected service. The playing field must be level and functionally equal services should be subject to equal protections.

f) The GSMA believes that the current framework needs to be updated to achieve legal certainty for European consumers and a level playing field for all IoT players irrespective of sector and geographic location. The best way to achieve this legal certainty is to review the EPD. In such review, it is essential to ensure that the same protection applies to the same services, however they are technologically provided. The rules will have to provide an appropriate protection for confidentiality of communications. The review should ensure it does not overlap with the GDPR, in particular those relating to data breach notifications, and harmonising EU law across

Member States to avoid divergent implementations. To achieve these objectives we provide some recommendations on how certain specific provisions in the EPD could be integrated into the GDPR:

Specific Recommendations on the integration of the ePrivacy Directive into the GDPR

a) In order to achieve legal certainty for citizens and a level playing field for all players irrespective of technology, sector and geographic location, the GSMA proposes that: (a) all relevant overlapping legal provisions on data protection currently in the ePrivacy directive are incorporated into the GDPR; and (b) the Telecoms Package is amended to account for telecoms specific definitions and clauses protecting the confidentiality of communications.

b) Specifically, the GSMA recommends the following actions to:
   I. Requirements relating to confidentiality of communications (art 5, EPD) traffic data (art. 6 EPD), and technical features and standardisation (art. 14 EPD) apply to all communications, whether provided by traditional ECS providers, OTT providers or others. Confidentiality of communications is an essential right which requires protection across all services. At the same time the provisions relating to confidentiality of communications and traffic data will need to be carefully reviewed in the context of telecommunications package to ensure that data related innovation is not unduly restricted, especially when such can be done with no or minimal privacy impact.
   II. The requirement relating to directories of subscribers should be reviewed within the context of the universal services obligation within the Telecoms Package. If this obligation to provide directories remains, any privacy requirements should be maintained in the same legislative instrument.
   iii. Delete requirements relating to itemised billing (art. 7 EPD). To the extent that this requirement is still seen as necessary, it should be equally applied to all consumer services.
   iv. Delete the clauses that introduced specific obligations for telecom providers that are no longer justifiable in the current telecom landscape such as: presentation and restriction of calling and connected line identification (art. 8 EPD), exceptions (art. 10 EPD) and automatic call forward forwarding (art. 11 EPD) and others which are now addressed in the proposed Regulation, notably the clauses on location data (art. 9 EPD) and the specific data breach notification regime (art. 4 EPD), including the related Regulation 611/2013 on the notification of data breaches, and delete the definitions that are consequently no longer required (notably 'traffic data', 'location data', 'consent', 'value added service' and 'personal data breach').
   v. Delete clauses that do no longer serve a purpose due to the proposed changes, notably the clauses on the scope and aim of the ePrivacy Directive (art. 1 EPD), (while preserving the objective of protection of Confidentiality of Communications as part of law), the services concerned (art. 3 EPD), the Committee procedure (art. 14a EPD), the application of certain provisions of the Directive (art. 15 EPD), the implementation and enforcement of the ePrivacy Directive (art. 15a EPD), transitional arrangements (art. 16 EPD), transposition (art. 17 EPD), review (art. 18 EPD), repeal (art. 19 EPD), entry into force (art. 20 EPD) and art. 21 (addresses).

c) Regarding the council's General Approach, the GSMA welcomes the proposed General Data Protection Regulation (GDPR). Data protection and privacy are fundamental to building trust and confidence in, and driving the uptake of, new digital and IoT connected services by Europe's citizens.

d) However, The GSMA wants to emphasize that the EU has to create an environment that encourages data driven innovation in Europe. A successful regulation is a key element of a Digital Single Market. Data is the lifeblood, currency and the new "oil" of the Digital Single Market, and much of that data will be personal data. The right balance between values of privacy as a fundamental right and unleashing the potential of digital economy must be struck by the regulation and the Telecoms Package. We believe both of these objectives can be achieved simultaneously.

e) In particular, more emphasis is needed to ensure data related innovation continues to be viable especially when privacy impacts have been minimised through privacy enhancing technologies e.g. appropriate pseudonymisation and other such means.

f) The integration of all European rules related to data protection into one legislative instrument would be beneficial for all stakeholders and increase legal clarity and certainty, as businesses and consumers will only have to look to one legal instrument in order to understand their rights and obligations in respect of the processing of personal data. Moreover, by creating one set of rules all stakeholders will clearly know what is expected from them.

g) The GSMA supports the intention in the GDPR to create a level playing field between all players irrespective of sector or geographic location. Within the M2M and wider contexts, it is important that consumers are able to enjoy consistent privacy standards, irrespective of the technologies, infrastructure, business models and data flows involved and of who provides a service or where a company may be located. However, as long as the ePrivacy Directive coexists with the GDPR this will not be achieved. Telecoms operators (as ECS) will be subject to a dual regulatory regime and restrictions and obligations which do not apply to other internet players. Most notably, they will be subject to different data breach notification regimes and rules on the treatment of location data and traffic data.

h) As the ePrivacy Directive is currently interpreted and applied inconsistently across member states, its continued existence will hamper the harmonisation of data protection and privacy regulation across the EU. Additionally, whilst the GDPR seeks to apply its rules extraterritorially to non-EU-based companies, the ePrivacy Directive does not contain such provisions, resulting in inconsistent privacy experiences for consumers and asymmetry in law.

i) The resolution of these matters is crucial to enabling a level playing field, consumer confidence and to achieving a digital single market and the enablement of innovative IoT connected services. To this end, the GSMA calls for legislators to amend the proposed GDPR as soon as possible to incorporate all relevant data protection rules in a single document (notably a Regulation instead of a Directive).

6. What is the impact of open and proprietary standards on the development of the M2M sector? What are the advantages and disadvantages of open and proprietary standards, taking in account that M2M services may be provided on private or public networks?

a) Regulators should also recognize the truly global, nature of IoT. Globally interoperable services and standards reduce deployment costs and complexity, facilitate scalability, and enable consumers to enjoy intuitive connected experiences.
b) The GSMA has been and is actively working to promote interoperability in defining standards specifically in the IoT segment in 3GPP (LTE –MTC ,NBIOT and EC GSM) with the objective to modify and optimize existing mobile standards to fulfil the specific requirements of low data/throughput and power consumptions typical of the IoT environment.
c) The GSMA believes that the European regulators should support and promote interoperable specifications and standards across the IoT industry and Europe.