Telefónica´s contribution to the public consultation on BEREC Draft Report on Enabling the Internet of Things

Introduction

- It´s extremely risky to draw any conclusion without a clear definition of both, IoT and M2M. There are many statements included in the document that indistinctly apply to both concepts when they are not exactly the same.
- As there are no clear distinction between concepts, throughout the document it seems that "IoT = M2M = cellular". This approach is not service/technology neutral and will focus all regulatory concerns on mobile, whereas the IoT value chain is extraordinary broader and more complex than the mobile industry, including other kind of wireless access.
- Both IoT and M2M are global markets by nature and it´s difficult to fit them, from an administrative perspective just to an EU-wide regulation. As there are no geographical boundaries in the IoT and M2M market a regulatory jurisdictional issue will appear due to absence of global regulator. Therefore better worldwide coordination is desired amongst policy makers.
- There is no need for early intervention due to market characteristics (nascent industry, different from traditional voice and data services…etc.). An early intervention could become a competitive disadvantage to EU companies subject to regulatory constraints if compared to other regions or markets and start an unlevel-playing field for European operators.
- There is no need for a regulatory ad hoc regulatory framework for IoT or M2M services.

Spectrum

- There is a need for adequate spectrum resources availability but no specific spectrum resources should be allocated directly to M2M use. The service and technology neutrality principle should prevail and not be breached.
- In the medium term, IMT spectrum is capable to cope with M2M services demand and market requirements. If more spectrum is needed it should be identified through well established procedures (ETSI/CEPT/WRC) and allocated to mobile use.

1. ***How do you evaluate the three options mentioned above (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?

- IoT and M2M services are global by nature. Creating an EU administrative boundary will not fulfil market requirements. Imposing numbering structure, as already occurred in some countries, could become a competitive disadvantage as operators face commercial situations in which international customers preferred an offer based on a standard numbering structure rather than an imposed national ad-hoc m2m numbering structure.
- Numbering resources scarcity for IoT or M2M services are not foreseen. There are no specific cases up to date.
- Don´t turn "early regulatory intervention" into a competitive disadvantage for EU providers. Harmonisation should be pursued at global level by means of better coordination.
- Extraterritorial use of E164/E212 and global ITU numbering resources are relevant and complementary pieces of the numbering toolbox. ITU numbering resources are already relevant and any concerns have been reported.
- Extraterritorial use is harmonised numbering resources is highly desirable but not at regional level. The EU numbering scheme should be "optional" as it is not strictly necessary due to the following reasons:
    - Scalability disruption
    - Alternative solutions available
    - No significant improvements foreseen
    - High deployment costs

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

- The global market for M2M/IoT services is extraordinarily competitive.
- Permanent roaming is a widespread solution that´s is key to take momentum on both IoT and M2M markets. Both are currently in a very positive commercial dynamics that could not be missed, especially as a result of too early regulatory intervention.
- Permanent roaming takes advantage of mobile services scale and efficient solutions. It reflects the truly global nature of IoT and M2M services that currently is well functioning.
- Permanent roaming should be dealt at bilateral commercial level amongst operators. Currently, the provisioning relies on bilateral agreed commercial negotiations worldwide.

We should take into account that intervention at the EU market will create a jurisdictional issue as the worldwide regulatory balance will be disrupted. Reciprocity should be guaranteed between EU and non-EU players to maintain a level playing field.

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?***

No need for MNC direct assignment

- No observable problems identified and no clear benefits foreseen
- Increased complexities, unnecessary implementation costs as well as security and fraud risks associated to misuse.
- Need to enforce, monitor and control the management of a scarce resource such as numbering. NRA should make sure that public interests and objectives are fulfilled.
- Service continuity should be assured as this measure could potentially disrupt a consolidated and well-established model. It could destabilize a worldwide system already in place.
- Already numbering alternatives in place (E-164/E-212 and ITU)
- If done, only after thorough impact assessment. We foresee potential impact.
- IPv6 numbering could be slowed down and negatively impacted.

Switching

- Countervailing power is extremely high in both B2B and B2B2C markets; therefore there is a competitive pressure to solve competitive concerns at connectivity level.
- The same "competition concerns" should be examined across the value chain and with alternative access solutions, in a holistic approach, making sure there is a level playing field.
- Industry approach developed within the GSMA as referred in the consultation document is the best option placed, best suited and timely approach. It has been commercially driven by telcos and other players. The regulatory approach could not beat this approach in terms of time and costs. This approach is also being developed at international level and at standardisation fora

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?***

- Security is vital to build trust and consumer confidence. This is not a regulatory concern but a critical commercial requirement to develop a nascent market such as IoT and M2M.
- Robust security measures are required across the whole IoT value chain. Remit to current art. 13a and future NIS provisions if applicable when required. No need for specific IoT/M2M regulatory framework.
- Security "by design" is key to ensure a confident and resilient IoT/M2M ecosystem as these services are very sensitive. (i.e consumption).

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?***

- We need to rely on horizontal law as much as we can to achieve a consistent application across the value chain in a service/technology neutrality manner. Need to delete ePrivacy Directive and rely on the ongoing GDPR provisions.
- We support industry measures that identify and mitigate privacy risks. Future proof Self Regulation/Code of Conducts should be use for fine tuning provisions, including fostering collaboration among different industries.
- Given the different impacts to the privacy of individuals associated to IoT projects (from smart agriculture, fleet management, smart cities or e-health projects), privacy issues must be sorted out based on Privacy Impact Assessments (PIAs) in the light of the applicable horizontal privacy regulation where the appropriate technical, contractual and legal measures should be considered to tackle the identified privacy challenges. In this respect, the new General Data Protection Regulation supports this risk based approach to face the upcoming privacy issues in new technology-driven projects like IoT.
- Privacy "by design" is key to ensure a confident and resilient IoT/M2M ecosystem as these services are very sensitive (i.e consumption).

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?***

- Standards policy should reflect the global nature of IoT services, fostering interoperability and scaling up of services.

- Increased support and promotion of interoperable specifications and standards.

- Focus on timely solutions that reduce deployment costs and complexities. First option should always be commercially driven approaches that focus on implementation. Smart Cities are Living labs for Internet of Things applications. Public Administrations should foster open standards by adopting an “open by default” approach for smart cities platforms and by improving common or standardized data formats for open data. An open platform is defined as one that allows external agents to interact with it, via public interfaces (non-proprietary APIs), and that ideally have been defined by a reputed agency. Ecosystems are generated around a platform and applications that rely on it. Open platforms promote easy to connect and build, support horizontal infrastructure that enables all kind of applications (openness), portability (avoiding lock in and fostering increasing scale), and interoperability by default. An example could be Smart Cities’ FIWARE platform developed as part of the Future Internet initiative FI-PPP (Future Internet Private Partnership Programme) launched by the European Commission in collaboration with the industry.