Body of European Regulators for Electronic Communications

BEREC

BoR (16) 38

BEREC Report on the Public Consultation of the Report "Enabling the Internet of Things"

January 2016

Introduction

On 5 October 2015, the draft report on “Enabling the Internet of Things” was published. The stakeholders were invited to submit their comments until 6 November 2015.

In total BEREC received 21 submissions from the following stakeholders, one of them confidential (in alphabetic order):

- AT&T
- CEPT
- CISCO
- Confidential Stakeholder
- EENA
- ETNO
- GEMALTO
- GOF
- GSMA
- INTUG
- MoquiThings
- Numericable SFR
- PosteMobile
- PT Portugal
- Mr. Jukka Rannila
- Telefónica
- Telekom Austria
- TIM
- TRANSATEL
- Verizon
- Vodafone

The contribution of the confidential stakeholder is used in this report, whereas the name of the stakeholder is replaced by “confidential stakeholder”. Moreover, BEREC received one submission after the deadline. This submission has been read carefully, but it has not been taken into account when reaching the BEREC conclusions.

BEREC welcomes all contributions and thanks all stakeholders for their submissions. The contributions received from stakeholders will be published on the BEREC website unless they are confidential.[1]

This report has the objective to provide an overview of the received contributions and to present BEREC’s view on them. The report is structured following the six questions raised in the draft report and includes a section with general comments.

[1] See http://berec.europa.eu/

Question 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?

Use of existing national and/or ITU numbering resources

Nine of the commenting stakeholders (AT&T, ETNO, GSMA, PT Portugal, Telefónica, Telecom Italia, Telekom Austria, Verizon, Vodafone) are explicitly in favor of a use of existing numbering resources, namely an extra-territorial use of national numbers and/or use of global International Telecommunications Union (ITU) numbers:

- Seven stakeholders replied that the extra-territorial use of both national E.164 and E.212 numbers and also the use of global ITU numbering resources should be considered complementary options in the numbering toolbox for the provision of IoT services (AT&T, ETNO, GSMA, PT Portugal, Telefónica, Verizon, Vodafone). Both solutions are already used today. None of these models should be mandated, promoted, imposed or prevented by regulation (AT&T).
- One stakeholder regards the extra-territorial use of national numbers as the preferred solution without mentioning the use of ITU numbering resources. However, the permission of extra-territorial use of national numbers by individual countries – which is envisaged by individual countries like Belgium and Germany – is not deemed to be helpful but, since rules on extra-territorial use of numbers are not meaningful if they are not reciprocal, an internationally harmonized approach is favored (GSMA).
- That an internationally harmonized approach with regard to extra-territorial use of national numbers is preferable or even essential was also stressed by other stakeholders (ETNO, GSMA, Telefónica, Verizon). Extra-territorial use of International Mobile Subscriber Identities (IMSIs) should not be restricted within the EU (Verizon). Even if a common approach followed by all individual European regulators is encouraged, European regulators are called upon to further negotiate at international level to create a similar harmonization at international level (ETNO).
- One stakeholder states that national numbering plans are working worldwide-wide and does not see the need for any intervention at European or global level (Telekom Austria)
- One stakeholder (Telecom Italia) is of the opinion that the extra-territorial use of E.164 numbers should be in principle excluded because of the lack of a real need and the impacts on issues like traceability, numbering misuses, frauds, etc., and that the use of global ITU E.164 numbers should be preferred in the case of services provided in more countries.

In essence, the preference for both solutions are based on reasoning that a fragmented distribution model, involving a separate SIM/IMSI per country and integration with each national mobile network operator platform would lead to higher costs and inefficient work streams and distribution chains (AT&T).

European numbering scheme

Arguments against a European numbering scheme

Many of these stakeholders (AT&T, ETNO, GSMA, PT Portugal, Telefónica, Vodafone) as well as one additional stakeholder (Numericable/SFR) explicitly state that they are not in favor of a European numbering scheme.

- Since IoT services tend to be global and businesses deploying IoT solutions most often require global distribution coverage and the provision of consistent global services, a European –hence regionally limited – solution would not represent an advantage (GSMA, PT Portugal).
- Creating an EU administrative boundary would not fulfil market requirements; there are situations in which international customers preferred an offer based on a standard numbering structure rather than an “imposed national ad-hoc IoT structure (Telefónica).
- A European numbering scheme is deemed to be not strictly necessary due to the following reasons: scalability disruption, alternative solutions available, no significant improvements foreseen, high deployment costs (Telefónica, similarly ETNO and GSMA).
- A compelling case for the introduction of a European M2M numbering scheme as a third option besides existing alternatives is not seen (AT&T).
- Rather, adding complexity could hamper the IoT ecosystem growth in Europe (Numericable/SFR).

However, one stakeholder would support a system of pan-EU authorization for IoT based on a national numbering allocation system, even if a requirement for a new pan-EU number range for IoT is not seen in view of the existing solutions (Vodafone).

Arguments in favour of a European numbering scheme

Three stakeholders, all of them MVNOs, regard a European numbering scheme for IoT services as useful:

- One stakeholder replied that the three options (extra-territorial use of national numbers, use of ITU numbers and use of European numbers) should be used complementary (Transatel).
- Another stakeholder weighted the pros and cons of the three solutions without naming one preferred solution. In doing so, he stated that a European numbering scheme, while having the drawbacks of an ITU numbering plan, is "maybe easier to promote than ITU numbers" (MobiquiThings).
- One stakeholder believes that the "long-term solution for numbering related to IoT services is the use of a European numbering scheme" (Poste Mobile). However, in its view such a new numbering scheme would require some time to be implemented. Therefore, a short-term solution is regarded as necessary and the extra-territorial use of national number is deemed to be the only one that could allow market players to continue offering IoT services.

Flexible approach towards the different solutions

The working group "Numbering and Networks" of the Electronic Communications Committee (ECC) of CEPT cautioned against expressing preferences for any of the three solutions as different IoT applications have different characteristics and will inevitably require different solutions. A certain degree is regarded as unavoidable by CEPT but the long term objective is to provide sufficient, sustainable and scalable numbering and addressing solutions to facilitate competition and to encourage innovation in the IoT sector while ensuring greater transparency in the use of these resources internationally. It is also deemed to be important that the burden of providing numbering and addressing resources does not fall disproportionately on the national numbering plans of one, or a few, European countries.

BEREC considers that the use of existing numbering resources - the extraterritorial use of numbers and the use of global ITU numbers - seems to be a reasonable approach for the development of the part of the IoT market relying on numbers as identifiers, while the introduction of a European numbering scheme does not seem to carry significant benefits which would justify the costs required to implement such a scheme.

The results of the consultation support the BEREC considerations, given that

- **only three stakeholders (MVNOs) have a mildly positive towards the European numbering scheme, but do not mention specific arguments for that;**
- **the large majority of the stakeholders who commented on this topic does not see a need for a European numbering scheme, specifying that it does not provide any additional value, in particular because of its geographic limitation, its costs of implementation and the lack of use cases.**

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

Fourteen of the commenting stakeholders were mostly in favor of permanent roaming, stating that it was a widespread solution to offer IoT services in Europe and also on a worldwide level.

Permanent roaming an efficient and established solution

- Eleven stakeholders refer to permanent roaming as a key factor for the success of IoT services and that it is a sign of IoT services being global services (AT&T, ETNO, GSMA, MobiquiThings, Numericable/SFR, PT Portugal, Telecom Italia, Telefónica, Transatel, Verizon, Vodafone).
- One stakeholder (AT&T) emphasizes that this established, efficient and well-functioning international IoT roaming framework has been helpful for large and small manufacturers alike as they can use a distinct platform.
- Other stakeholders state that using permanent roaming as a basis for IoT services is not a problem (Telekom Austria) or mentioned that it is and will be used to achieve better coverage as a substitute for national roaming (Poste Mobile).
- The wholesale roaming market is regarded as working efficiently (Telekom Austria), and making use of already existing roaming agreements is based on the need for scalable and efficient solutions to offer IoT services on a global basis (AT&T, ETNO, GSMA, Telefónica). A major MNO (Vodafone) states that it has roaming agreements for IoT with at least one operator in each Member State, which promotes sustainable competition, efficient investment and innovation. Four operators (AT&T, Telecom Italia, Telekom Austria, Vodafone) add that all MNOs should be interested in such roaming agreements as they will profit from handling as much traffic as possible in their networks.
- Another stakeholder (MobiquiThings) warns that permanent roaming restrictions would dramatically penalize tier 2 MNOs and MVNOs in their ability to match the capabilities of tier one and multi-country MNOs (MNOs with affiliates in many countries).

Roaming Regulation not applicable to IoT

- With regard to the European Roaming Regulation ten stakeholders (AT&T, ETNO, GSMA, Numericable/SFR, Poste Mobile, PT Portugal, Telecom Italia, Telefónica, Vodafone, confidential stakeholder) are of the opinion that IoT services and the underlying connectivity part are not and should not be within the scope of the Regulation. Most of these stakeholders mention e.g. that the Regulation is a consumer protection instrument (GSMA), intended to protect end-users when travelling within the Union (PT Portugal), favoring travelling EU customers (Poste Mobile) or that end-user specific problems such as “bill shock” cannot arise in case of IoT services (AT&T).
- One stakeholder (confidential stakeholder) is aware of the BEREC guidelines according to which IoT services are in general subject to the Roaming Regulation but considers this a mere formal assumption based on Art. 15 (4) of the Roaming Regulation.
- The different nature of IoT services in comparison to traditional end-user services is also highlighted by referring to IoT users as resembling a “closed user group” (AT&T,

GSMA Telecom Italia) where open-ended Internet connectivity or traditional any-to-any voice communications are not provided (AT&T) and are not the primary purpose of the service (Telecom Italia). In such a case, customers are generally not end-users but businesses requiring global distribution coverage and managed services (GSMA).

- Consequently seven stakeholders (AT&T, ETNO, GSMA, Numericable/SFR, PT Portugal, Telecom Italia, Telefónica) suggest that permanent roaming for IoT services should be subject to commercial agreements on a voluntary basis which would give flexibility to select the most adequate commercial model agreement (PT Portugal). Such commercial agreements can also take into account specific needs when it comes to billing of IoT services.
- Two stakeholders (GSMA, Telecom Italia) mention that better and more innovative billing regimes could be developed which is not possible with the billing regime stipulated by the Roaming Regulation, which only foresees a model of traffic-oriented remuneration. However, as IoT services typically cause a very limited amount of traffic at periodic intervals and sometimes only signaling, IoT contracts usually include a fixed fee for the service and a variable amount for traffic (Telecom Italia). In this regard, BEREC's assumption that the Roaming Regulation does not cause any access and pricing issues related to IoT is not shared (Telecom Italia).
- A precondition for such flexible and innovative IoT billing models, however, are identifiers to detect M2M traffic (PT Portugal); the GSMA's M2M Roaming Principles are in place and allow for the identification, measuring and distinguishing of roaming traffic from traditional traffic (AT&T).

<u>Permanent roaming part of a wholesale access obligation?</u>

- A wholesale access obligation, which permanent roaming could be a part of, is explicitly rejected by two stakeholders, who do not see the need for this request without prior evidence for the industry failing to address market needs (GSMA, Telecom Italia).

<u>Permanent roaming to be banned</u>

- In contrast to these comments, one stakeholder (confidential stakeholder) asks for IoT services based on permanent roaming to be banned from the EU – irrespective of the applicability of the Regulation to IoT services – because they circumvent national regulation for Mobile Number Portability (MNP) due to missing international MNP rules. Furthermore this stakeholder sees jurisdictional problems when it comes to solving disputes. The same stakeholder suggests limiting national roaming to IoT data services and only if there is evidence that no distortion is caused. An obligation for manufacturers to provide at least dual SIM slots is seen as a solution to override permanent roaming and to stimulate competition. Compared to this position another stakeholder (MobiquiThings) warns that permanent roaming restrictions would dramatically penalize tier 2 MNOs and MVNOs in their ability to match the capabilities of tier one and multi-country MNOs (MNOs with affiliates in many countries).

<u>National Roaming</u>

- One stakeholder (Poste Mobile) basically regards national roaming agreements as an instrument to increase coverage. Still, there could be issues because no operator would want to provide national roaming to its competitors, due to antitrust reasons or

because – in the case of MVNOs – their wholesale contracts could forbid national roaming. Consequently, this stakeholder calls upon NRAs to require operators to offer national roaming agreements in the case of IoT services; a suggestion – although by means of *supporting* national roaming agreements rather than by an *obligation* – which is also mentioned by a stakeholder who sees some difficulties for national operators, e.g. MVNOs, to compete with international operators (Transatel).

- This view is not shared by other stakeholders (Verizon) who do not see any limitations in concluding national roaming agreements or any need for regulatory intervention.
- Some stakeholders do not agree with BEREC's characterization of permanent roaming as a response to the absence of national roaming but rather as a sign of the global nature of IoT business models (AT&T, Telecom Italia). Still, in some cases domestic operators might face distortions due to the competition of foreign networks. Such cases should be dealt with on a national level (Telecom Italia).

BEREC acknowledges that many stakeholders refer to permanent roaming as a key factor for the success of certain IoT business models being used. At the same time it can also be seen as a sign that these IoT services have global reach.
BEREC considers that, when the IoT connected device is used on the basis of permanent roaming, and it is not travelling at all (scenario 3 of the Report), the Roaming III Regulation amended by the TSM Regulation (Roaming Regulation) would not apply, meaning that agreements concerning permanent roaming could be commercially negotiated. On the contrary, the applicability of the Roaming Regulation to IoT connected devices which travel periodically should be dealt with on a case-by-case basis.
BEREC acknowledges that the use of permanent roaming might in some instances be used to bypass the absence of national roaming: in other words, in some national markets the roaming operator exploits a competitive advantage over national operators being able to exploit the coverage of all existing networks, that visited networks would not be able to exploit because of the absence of national roaming. This might create competition distortions.
It remains to be seen if operators will address this by relying on the provisions set out in the new Art. 3 of the Roaming Regulation.

Question 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?

Is switching really an issue?

Three of the commenting stakeholders express the view that switching between connectivity service providers is or might not an issue in the IoT sector since the connectivity component, while being a precondition for the provision of IoT services, is not the key component and appears to generate only a small value in the IoT market. (GSMA, Numericable/SFR, PT Portugal)

No need for a regulatory intervention

Four stakeholders believe that there is no need for regulatory intervention either since there is already a solution available on the market (Telekom Austria) or since IoT users in B2B and B2B2C markets are most often businesses with sufficient countervailing power to negotiate appropriate contractual terms. (GSMA, Telefónica, similarly Poste Mobile)

OTA provisioning of SIM

Arguments in favor of OTA provisioning of SIM

Nine stakeholders are in favor of, and/or do actively contribute to the development and evolution of the OTA solution (AT&T, ETNO, Gemalto, GSMA, Poste Mobile, Telecom Italia, Telefónica, Telekom Austria, Vodafone):

- The market has already led to available switching solutions; the technical solution is now mature and ready to be implemented by SIM manufacturers and operators. (GSMA, Poste Mobile, Telekom Austria)
- One stakeholder describes the current state and the advantages of an OTA solution, in particular with regard to globally marketed connected devices at the example of an IoT automotive use case. One of the main advantages is the download of a national profile which also helps to overcome the issue of extra-territorial use of numbers, for example when new devices are deployed across multiple regions and OTA provisioning allows for provisioning at a later stage. (Gemalto; similarly Numericable/SFR which, however, states that both solutions have yet to be further defined and experimented)
- The OTA provisioning of SIM cards is regarded as the long term solution to facilitate switching between operators once a contract has expired. (Poste Mobile)
- The industry approach developed within the GSMA is regarded as the best option placed, best suited and timely approach. It has been commercially driven by telcos and other player. This approach is also being developed at international level and at standardization fora. (Telefónica)
- The OTA capability has been evolving since the first release of the GSMA specification and, while further work is required to fully enable the functionality, the latest version 3.0 of the specification, which became available in October 2015, does allow full, interoperable OTA provisioning between different carriers. (AT&T, GSMA, Vodafone). Moreover, a GSMA White Paper identifies and defines potential approaches which would enable an MNO to re-programme a SIM of a customer of

another MNO. (GSMA). Further, it is envisaged to develop an Independent Entity that will monitor and manage the process of switching operators. Such self-regulation by industry consists of a timely and reliable provisioning of profile changes with a guaranteed performance, a contractual regime, a messaging mechanism that records transactions as well as a code of practice (Vodafone)

- OTA provisioning also accommodates changes to profiles of different MNOs over the life span of a product, enabling opportunities for greater choice by IoT manufacturers as well as enabling customers to retain control and leverage over their communications spend. (AT&T, Vodafone)
- The costs are greatly reduced when using OTA provisioning of SIM compared to manual SIM swaps. (Vodafone)
- Only for IoT services which have difficulties or impossibility (e.g. embedded SIM) to change the physical SIM when changing the mobile operator, it is necessary to reconfigure the SIM remotely. (ETNO)

Concerns regarding OTA provisioning of SIM

Three stakeholders raise concerns regarding the OTA solution:

- Since OTA provisioning of SIM is at an early stage and raises complex issues regarding security and standardization that would oblige MNOs to undertake significant implementation costs, a clear regulatory environment would be needed prior to the implementation of an OTA provisioning of SIM solution. (PT Portugal)
- It would need to be proven if the OTA process effectively lowers switching costs and improves the flexibility of the IoT market in a non-discriminatory way. OTA techniques shall be designed in order to grant that: full competition among parties is guaranteed, the mobile operator will be the direct user interface for the switching process (no third party intermediation and direct relation among user and SIM configurator), and encryption and authentication processes shall be fully defined and grant an appropriate level of safeguards to all customers. Moreover, OTA provisioning should be limited in two ways: Firstly, it should be limited to a subset of IoT services, i.e. B2B, while B2C and B2B2C should still relay on physical SIM entitling final customers to easily and more clearly choose its connectivity provider. A generalized introduction of OTA provisioning would likely to destroy the industry of SIM production and development. Secondly, it should be limited to IoT services and not be extended to person-to-person services since otherwise this would open the market for connectivity “brokers” and the MNO would be reduced to a wholesale provider of access to mobile networks without any interest to provide services integrated on their network. OTA introduction in the market shall only be allowed when it has been fully standardized at international, or at least at EU level, in order to avoid that proprietary solutions could create a walled garden where only few players can “play their own games” to the detriment of a full scale competition reducing consumer benefit (confidential stakeholder).
- The OTA solution is not perfect because some of the SIMs cannot be reprogrammed. It is limited to those SIMs that are under OTA coverage, and there are always devices that are not reachable, particularly in the IoT context (were SIMs could be hidden in a connectivity module or a machine). (Transatel)

MNC assignment to IoT users

Arguments in favor of MNC assignment to IoT users

Only one stakeholder (Transatel) expressed a preference for an "MNC solution" (i.e. assignment of own MNCs to IoT users), for the following reasons:

- It has been demonstrated from the MVNO environment that an MNC assignment to non-MNO market players authorizes switching from an operator to another operator "overnight and for a massive consumer base". (Transatel)
- There is no problem of scarcity because it is possible to use a shared MNC that are unlimited (the IoT service provider can use a technical and neutral enabler that owns its own MNC and distributes a dedicated MNC to IoT service providers. (Transatel)
- The operational costs of the migration seem to be very limited; the real cost is the technical implementation the new agreement with the new mobile network provider, which is itself really limited in an international roaming context. (Transatel)
- The IoT service provider does not need to acquire its own (costly to manage) mobile network infrastructure while operating its MNC because it can use a technical and neutral enabler which can provide a customized solution to the customer. (Transatel)

Concerns regarding MNC assignment to IoT users

Four stakeholders expressed doubts and/or concerns with regard to the solution of assigning MNC directly to IoT users (Poste Mobile, PT Portugal, Verizon), or even state that there is no need for a direct MNC assignment to IoT users (Telefónica):

- This stance is often based on the grounds of amount of MNCs as well as size of the individual MNC (which contains 10 billion IMSI): The number of MNC available per country (MCC) is limited (usually 100 per country/MCC). (Poste Mobile) MNC assignment to any IoT user, independently of the size of the companies' projects, could lead to a tremendous waste of IMSIs with increased costs to all mobile operators. (ETNO, PT Portugal) There would be the need to enforce, monitor and control the management of a scarce resource. (Telefónica)
- In several instances, this approach is motivated by the reasoning that MNC should only be available to authorized providers than can demonstrate a need for these resources (ETNO, Telecom Italia) Slightly different, one stakeholder would like to limit MNC assignment to providers of electronic communication services at least as long as the current EU framework for electronic communication services addresses numerous compliance and reporting obligations for electronic communication service (ECS) providers.(Verizon)
- Other stakeholders see increased complexities, unnecessary implementation costs as well as security and fraud risks associated to misuse. The regulatory approach could not beat the industry-driven (OTA-) approach in terms of time and costs. (Telefónica; similarly GSMA with regard to solutions based on shared MNC/HLR proxy)
- Moreover, service continuity should be assured as this measure could potentially disrupt a consolidated and well-established model and could destabilize a worldwide-system already in place. (Telefónica, similarly ETNO)
- Moreover, while evaluating the scarcity of MNCs, if assigned to IoT service platforms, it shall also be considered that a specific, additional MNC for IoT services shall be

provided to each EU mobile operator to handle M2M traffic in a more efficient way (confidential stakeholder).

- There was no evidence of a sustained demand for MNC assignment to IoT users. (Vodafone)
- Two stakeholders requested that certain rules apply and/or certain aspects are solved if MNC are assigned to IoT users: Various technical, security and operational questions would need to be addressed, including what infrastructure requirements would apply to the IoT user, how would switching operate and with what risks, and what would be the impact on MNC resources. (AT&T)
- In order to ensure equitable treatment of all market players, IoT users should be subject to similar numbering obligations as those applicable to the assignment and use of such numbers by MNOs and MVNOs. This would effectively mean that the IoT user would need to become a provider of electronic communication services or electronic communications networks. (AT&T) Similarly, it is requested that, being an MVNO, the IoT platform service provider must comply with all the obligations related to customer handling (safeguard privacy and related consumer rights) and network integrity (being currently unknown which network equipment it will manage) (confidential stakeholder).

Flexible approach

The working group “Numbering and Networks” of the Electronic Communications Committee (ECC) of CEPT cautioned against expressing preferences for a specific solution. Reference is made to the answers to Question 1 where their answer is summarized in more detail.

Approach assuring the end customer’s choice

One stakeholder expressed the view that it must be assured that the final customer is able to choose its final connectivity service provider. Moreover, the task of regulation should be to prevent the establishment of solutions that allow collapsing of distinct figures in the value chain in a single turn-key provider This would de facto limit the possibility of choice for the end customer and competition between the parties involved (confidential stakeholder).

BEREC acknowledges that according to the majority of commenting stakeholders there seem to be more challenges in the assignment of MNCs to IoT users than in the adoption of the OTA option.

BEREC understands that there seem to be pros and contras for both methods which can co-exist, certainly in a market as IoT, which is very diverse in terms of applications and market actors. The assignment of MNCs to IoT users may introduce challenges in the administration of MNCs and carry the risk of scarcity of MNCs while the OTA switching process is appealing under the condition that it is designed in an open, transparent and non-discriminatory manner in order to avoid competition problems and ensure the needed security measures. NRAs could have good reasons to consider introducing more flexibility in MNC assignment and also to become active in the OTA provisioning of SIM if connectivity service providers do not introduce it themselves in a timely manner. Overall, BEREC sees the need for flexible solutions at national level.

Question 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?

Thirteen stakeholders commented on the question if Art. 13a of the Framework Directive should be amended.

No need for changes

- Two stakeholders (Numericable/SFR, Telekom Austria) state that there is no need to change the Framework Directive with respect to IoT, whereas one of them (Telekom Austria) is generally in favor of reduced sector-specific regulation.

Existing rules applicable for whole IoT service chain

- Six stakeholders (AT&T, ETNO, GSMA, PT Portugal, Telecom Italia, Telefónica,) rather think that the already existing rules should be extended to all parties involved in the provision of IoT services (e.g. manufacturers, operators, application providers, system integrators), taking into account that security measures can only be as effective as the weakest link in the IoT value chain. One of them (AT&T) stresses that it is even disproportionate to impose additional security obligations on one part of the ecosystem only. From a global player's point of view, another operator (Verizon) rather sees a need for a consistent approach on a global level.
- Three stakeholders (Verizon, Vodafone, confidential stakeholder) stress that those IoT services which are based on an ECS are already subject to regulation and thus must fulfill high security standards. In this context three stakeholders (Cisco, Telefónica, Verizon) mention the draft Network and Information Security (NIS) Directive which is supposed to be adopted in early 2016 at the latest. The Directive includes a definition of network and information services which would cover the IoT networks in question. Consequently all kinds of IoT services would be obliged to fulfill a high level of security without changes in the Framework Directive.

Industry self-regulation better than regulatory measures

- In this regard two operators (AT&T, Vodafone) refer to already existing initiatives, many of which are industry led. These initiatives often cover several parts of the IoT value chain and address security concerns by means of standards (e.g. One M2M), standardisation methodologies (Mandate 530) and industry guidelines (GSMA IoT security guidelines).
- One stakeholder (Verizon) comments that industry self-regulation is regarded as being fare more effective than top-down sector-specific regulatory measures. Especially as the IoT market is fully competitive, there are strong incentives for industry stakeholders to provide high levels of security and safety, a position which also shared by another stakeholder (Telefónica). Those stakeholders which are not able to fulfill these levels will not be able to survive on the market.

Security level depending on criticality of a service

- One stakeholder (PosteMobile) sees the need for a balanced approach. On the one hand the existing rules already cover most of the IoT services, as e.g. the underlying connectivity part is regarded as a critical infrastructure. Thus a high level of security

must be ensured. On the other hand some modifications should be considered taking into account the different level of “criticalness” of the several IoT services: For less critical services an implementation of deep security protection is not necessary. Also the low cost of the equipment should be considered which not always allow for strong security measures.

BEREC acknowledges that the appropriate security level depending on the specific IoT service in the respective value chains should be applied by all the parties involved because the security measures are as effective as the weakest link in the respective IoT value chains.

Question 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?

On a general level all of the fourteen stakeholders, who answered this question, are in favor of a technology-neutral way of handling privacy issues regarding IoT services. In this context the future General Data Protection Regulation (GDPR) is often quoted as an appropriate tool to address such issues, rather than sector-specific provisions.

No IoT specific rules

- Two stakeholders do not see the need for IoT specific rules and regulatory intervention (Telekom Austria) and ask for same protection rules irrespective of sector and location (PT Portugal) without suggesting any specific modifications or amendments.
- The view that no IoT specific rules should be adopted, but rather general privacy rules should be implemented, is shared by ten stakeholders (AT&T, Cisco, ETNO, GSMA, Numericable/SFR, Poste Mobile, Telecom Italia, Telefónica, Verizon, Vodafone). To achieve this goal, most of these stakeholders suggest to delete the current ePrivacy directive and to incorporate its provisions into the GDPR, such as the definitions of "communication" and "electronic mail" and the clauses on confidentiality of communications and unsolicited communications (ETNO, GSMA). In this regard three stakeholders (ETNO, GSMA, Telecom Italia) point out that a parallel application of the ePrivacy Directive and of the GDPR would lead to confusion for both IoT operators and for consumers on which rule has to be applied and what their privacy will be treated like respectively. With just one Regulation in place, such problems can be avoided and legal certainty can be achieved.

GDPR a good solution

- Two stakeholders (Poste Mobile, Verizon) see an advantage in the legal nature of the future GDPR in contrast to the existing ePrivacy Directive. As the Directive had to be transposed into national legislation, Member States had some discretion resulting in 28 national regimes. In comparison to this, a Regulation is applied directly and reflects the pan-European (and even global) nature of most IoT services.
- Nine stakeholders (AT&T, ETNO, GSMA, Numericable/SFR, PT Portugal, Telecom Italia, Verizon Vodafone, confidential stakeholder) welcome the approach of the GDPR as it would cover not only telecom operators but – in a technology-neutral way – all kind of IoT services irrelevant of the system which is used to realize them. Two stakeholders (ETNO, GSMA) suggest that in addition the Telecoms Package could be amended for telecoms specific clauses and definitions, e.g. integrating the definition of "user", or the clauses on itemized billing, presentation and restriction of calling and connected line identification or technical features and standardisation. Specific obligations for telecom providers, such as traffic data, location data or specific data breach notification regime should be deleted.

Too strict regulations will hinder IoT growth

- Several stakeholders consider that too strict regulations on privacy could hinder the development of IoT services. Two stakeholders (Cisco, Telecom Italia) point out that the current procedure of "notice and consent" could become a problem as many IoT devices might not have any user interface on which check-box options could be displayed. Furthermore, as IoT services become more and more omnipresent, data subjects could feel overflown by endless "notice and consent" requests. In addition many IoT use cases rely on gathering persona data to work properly and to fulfill the users' expectations. As a solution the inclusion of measures such as pseudonymisation or avoiding the collection of identifiers is suggested.
- In particular one stakeholder (Cisco) is very concerned about the current privacy provisions and rules which are currently under consideration. According to this stakeholder the EU is moving to a too rigid and prescriptive approach to data protection which might harm the EU's global competiveness regarding IoT services. The reasons for such an assumption are, among others, very strict conditions for profiling including impact assessments and prior consultation with data protection authorities, or instability surrounding the Safe Harbor Privacy Principles. By contrast, another stakeholder (confidential stakeholder) considers the current regulatory regime of a case-by-case analysis on profiling with a prior check mechanism by the NRA to work well and suggests that they could also be used for IoT data.

Privacy by Design

- "Privacy by Design" is mentioned by some stakeholders as a possible solution for fulfilling the data subject's rights (Cisco), and four stakeholders (ETNO, GSMA, Telecom Italia, Vodafone) refer to the "Alliance for Internet of Things Innovation" (AIOTI). In this Policy Working Group, set up by the European Commission, the industry can play a strong and proactive role. Its report includes recommendations regarding Privacy by Design, Privacy Engineering methodologies and a Privacy Knowledge Base (Vodafone).

BEREC understands the need to strike a balance between the need for the collection, processing and use of data (which is typical for IoT services to work properly) and the end-users' need for an appropriate level of privacy.
BEREC acknowledges that the challenges raised by the evolution of IoT applications, especially in health related fields or similarly sensitive fields, require specific protection for sensitive data against inappropriate use. These issues are not new, but they become more complicated because of the fact that the IoT value chain includes several parties which could have access to the data of the end-users.
To that end, BEREC seizes the occasion of the upcoming review of the data protection rules to recommend that the new legislative provisions take into account the suggestions highlighted in the BEREC IoT Report.

Question 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?

Sixteen stakeholders commented on the question on standards, and to some extent all of them stressed the relevance of open standards and interoperability for the successful deployment of IoT services.

Open standards are more favorable than regulated (EU-wide) standards

- Ten stakeholders (AT&T, Cisco, ETNO, GSMA, Poste Mobile, Numericable/SFR, PT Portugal, Telecom Italia, Telefónica, Vodafone) are in favor of open standards as they are important to maximize economies of scale. Such standards must, however, reflect the global nature of the IoT services (AT&T, Cisco, ETNO, GSMA, INTUG, Numericable/SFR, PT Portugal, Telecom Italia, Telefónica, Verizon, Vodafone), so a procedure which focuses on only EU-wide or even national standards should not be supported.
- When it comes to the role of regulators, many stakeholders (AT&T, Cisco, ETNO, GSMA, Jukka Rannila, Telecom Italia, Telefónica, Telekom Austria, Verizon) comment that those and other authorities should rather focus on promoting and supporting standard development organizations (SDOs) to foster open standards and interoperability rather than setting EU wide or national standards, taking into account that obligations, e.g. on which technologies should be used, would have a negative impact on the evolution of this rather new market (Verizon).
- The view, that industry-led development of standards is a favorable solution, is supported by seven stakeholders (AT&T, Cisco, GSMA, Jukka Rannila, PT Portugal, Telecom Italia, Telefónica) who mention already existing SDOs and institutions. For example, in 3GPP (LTE-MTC, NBIOT, EC GSM) existing mobile standards are modified and optimized for low data/throughput and power consumption for IoT devices, whereas IETF plays a key role in making sure that protocols will not adversely impact the internet (Cisco). Another stakeholder (AT&T) refers to the GSMA's work on specifications for the embedded SIM to be provisioned over the air as an example of the industry to work together successfully, resulting in a solution which reduces costs, complexity and improves consumer experience. Also other SDOs are mentioned, such as CEN, ETSI, ITU-T, OneM2M (Cisco).

BEREC should play role in setting standards

- On the other hand, one stakeholder (Jukka Rannila) suggests that BEREC should join several SDOs and foundations to play an active role in defining standards. In addition, the regulators could regularly initiate questionnaires to gather the view of experts on specific standards.

Interoperability for communication between different standards

- Being in favor of open standards and interoperability, two stakeholders (Cisco, Jukka Rannila) point out the IoT's nature as a "network of networks" in which interoperability can be realized in different ways. It is not always necessary that each connected

device is able to communicate with another device (e.g. smart meters and bio sensors), and in many cases they use different protocols and infrastructures (although the Internet protocol is becoming a common language for most data communication) (Cisco). Still, with the use of standards, communication between such systems can be guaranteed, e.g. via central systems which can communicate with each other. In this context, another stakeholder (Telefónica) brings up the example of the FIWARE platform for smart cities, which uses non-proprietary APIs which the different external agents can interact with.

Problems for IoT due to patents and royalties

- Two stakeholders (Cisco, Vodafone) mention issues which might come along the usage of standards in the context of royalties for patents and the existing IPR (intellectual property right) licensing models. For the implementation of standards sometimes many thousands of patents have to be taken into account and licensed, e.g. in the case of LTE and Wifi. As many devices have a relatively low value and a rather high deployment rate, the current rules on licensing costs are regarded as a discouraging hurdle for the widespread implementation of standards.

Advantages of proprietary standards

- Some benefits of proprietary standards are mentioned by three stakeholders. One of them (confidential stakeholder) prefers open standards, but concedes that a proprietary standard might show higher security and privacy features; nevertheless the advantages of a greater diffusion of know-how and improved competition are seen as more important. Another stakeholder (Vodafone) points out that, despite speaking out for open standards, companies also need to compete through technical and commercial differentiation, and in many cases this can be achieved by using proprietary solutions. As such solutions can lead to innovations and advantages, one must be careful to ensure that companies will still have the possibility to differentiate their offers, avoiding a situation in which too much standardization will block innovation (Telekom Austria).

BEREC acknowledges that the IoT industry is currently driven more by proprietary than by open standards. BEREC understands that in an initial phase of development of the market, the adoption of proprietary standards might have a positive effect for the investments and R&D.
At the same time, BEREC considers it necessary to monitor the market, in particular to prevent any possible anti-competitive effects (such as the "lock-in" effect) and any national fragmentation in the standardization process.

Other remarks

Emergency services

One stakeholder (EENA) comments that the Report should have taken into account the consequences IoT will have for the future of emergency services in Europe. Wearable technology is mentioned as an example where biometric information can be transmitted to the incident manager or the effects eCall will have on the work of emergency services.

No need for completely new approaches

One stakeholder (Verizon) points to the fact that IoT is about new business models rather than representing a completely new technical revolution. Thus only some elements might need some fine-tuning to fit the needs of IoT, rather than re-inventing specific IoT policies.

Unclear definitions

One MNO (Telefónica) comments that it is risky to draw conclusions without clear definitions of IoT and M2M, taking into account that these terms refer to concepts which are not exactly the same. In BEREC's Report, however, many statements are applied to both concepts.

An association (GSMA), however, agrees with BEREC's statement that for the purposes of the Report no detailed definition is necessary. It admits that there is no industry agreement on the definitions for M2M and IoT, referring to its own terms:

> **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.*

M2M ≠cellular

Two MNOs (Telefónica, Vodafone) mention that the Report is not service-/technology-neutral and focuses on cellular services, whereas there are many applications which do not rely on mobile services:

	2014	**2024**
Total global M2M connections	5 billion	27 billion
Of which total global cellular M2M connections	256 million	2.2 billion

Source: Machina Research, M2M Global Forecast and analysis, 2014-2014 (quoted by Vodafone)

Similarly, another stakeholder (GSMA) refers to the fact that only a small fraction of M2M connections will be based on cellular technologies, estimating that by 2019 only 140 million connections will be cellular in the EU. In the same vein, another stakeholder (Cisco) states that “some of the M2M may require a SIM card, but most of the M2M devices will not”.

Spectrum

One stakeholder (Telefónica) suggests not to allocate spectrum to IoT services specifically. While there is a need for adequate spectrum resources, the principle of technology neutrality should be maintained. IMT spectrum is capable to cope with the demand of IoT services on the medium term. Otherwise established procedures are in place to find solutions (ETNO, Telefónica).

Choosing the right spectrum, in particular below 1GHz (higher frequencies are less optimal for IoT services), will be crucial, whereas licensed spectrum will be important for guaranteeing QoS. There might also be a demand for “earmarking” some spectrum for IoT applications without restricting its use to IoT only, e.g. 2x3 MHz in the 700 MHz band, following the results of CEPT ECC Report 242 (GSMA).

The association (GSMA) also refers to 5G as likely being the first cellular technology which will be optimized for IoT from the start. Its implementation will improve signaling and spectrum efficiency, reduce device costs, offer better QoS guarantees, lower latency and extended range.

Number portability

Two stakeholders submit that number portability is not necessary in the IoT context (AT&T, Poste Mobile), taking into account that the nature of IoT services makes phone numbers not relevant. (Poste Mobile) In case of a switch of connectivity service provider, the expectation is that the E.164 number would be changed along with the E.212 number (IMSI) assigned. (AT&T) The requirement of number portability would only increase operational costs and complexity. (Poste Mobile)

BEREC acknowledges that mobile connectivity is only used to a minor degree for IoT communications and that, therefore, any possible regulation in this regard would only apply to a small subset of the market.
BEREC considers that the nature of IoT services, which differs considerably from voice communications services and where in many instances a B2B or B2B2C business model is applied, might require a new approach with regard to the number portability obligation.