

Report

Enabling the Internet of Things

12 February 2016

Table of Contents

| | |
|---|----|
| Executive Summary | 3 |
| 1. Introduction..... | 4 |
| 2. Ensuring adequate resources for IoT services | 10 |
| 2.1. Spectrum | 10 |
| 2.1.1. The different spectrum requirements for the IoT..... | 10 |
| 2.1.2. Current availability of spectrum that can address the needs for M2M connectivity . | 11 |
| 2.1.3. Meeting future demand for spectrum..... | 12 |
| 2.2. Identifiers | 14 |
| 2.2.1. Numbers | 14 |
| 2.2.1.1. Type of numbers to be used for IoT services..... | 14 |
| 2.2.1.2. Right to request numbers (in particular E.212 (MNC))..... | 15 |
| 2.2.1.3. Scarcity of number resources..... | 16 |
| 2.2.1.4. Extra-territorial use of numbers | 16 |
| 2.2.2. IP addresses | 17 |
| 3. IoT services in the context of the EU Telecommunications Framework..... | 19 |
| 3.1. Applicability of the electronic communications regulatory framework | 19 |
| 3.1.1. Remuneration | 20 |
| 3.1.2. Conveyance of signals | 21 |
| 3.2. Roaming | 23 |
| 3.2.1. General applicability of the Roaming Regulation..... | 23 |
| 3.2.2. Permanent roaming in the context of the Roaming Regulation..... | 25 |
| 3.2.3. Current functioning of the market | 27 |
| 3.2.4. Use of international/global E.212 | 28 |
| 3.2.5. Concerns for the future | 28 |
| 3.3. Switching / lock-in issue..... | 30 |
| 3.3.1. MNC assignment for IoT users..... | 30 |
| 3.3.2. OTA provisioning | 31 |
| 3.3.3. Evolution of the regulatory framework with regard to switching | 32 |
| 3.4. Network security | 33 |
| 4. Areas where NRAs can have a coordinating function..... | 34 |
| 4.1. Privacy..... | 35 |
| 4.2. Standardisation..... | 39 |
| Annex 1: The IoT value chain – Examples..... | 43 |
| 1. Business Applications | 43 |
| 2. Industrial Applications | 44 |
| Annex 2: List of BEREC IoT stakeholder interviews | 45 |

Executive Summary

Within the ongoing review and DSM process it should be assessed whether and, if so, to what extent the existing rules which were primarily construed for voice telephony do also fit to Machine-to-Machine (M2M) communications or not.

In view of the Digital Single Market (DSM) review, BEREC considers that, in general, no special treatment of IoT services and/or M2M communication is necessary, except for the following areas:

- Roaming;
- Switching;
- Number portability.

With regard to privacy, BEREC sees the need for a careful evolution – but not an entire overhaul – of the existing EU data protection rules.

This assessment does not preclude that within the DSM review further areas for amendments of the regulatory framework taking into account the peculiarities of IoT services and/or M2M communication might be identified.

No need for a European numbering scheme for M2M communication has been identified.

A more detailed summary regarding the topics of this report can be found at the end of each chapter.

1. Introduction

During the last 20 years, the Internet has changed the way in which we work, communicate and trade. We are now on the cusp of another industrial revolution that will have a significant, positive impact on a wide range of industry sectors, including energy, transport, manufacturing and health. It is described by terms such as “Machine-to-Machine Communication” (M2M) or – the somewhat different notion of – “Internet of Things” (IoT) and involves a large number of devices communicating with one another primarily across the Internet using fixed and wireless access networks. In this report, the terms M2M and IoT are used as synonyms.

The market for IoT services is expected to grow significantly. In a recently published report by the EC, it is expected that the IoT market in Europe will expand with yearly growth rates over 20% in value between 2013 and 2020. The number of IoT connections within the EU28 is expected to increase from approximately 1.8 billion in 2013 (the base year) to almost 6 billion in 2020. IoT revenues in the EU28 will increase from more than €307 billion in 2013 to more than €1,181 billion in 2020, including hardware, software and services. The IoT growth will involve all the Member States, but those with higher accumulated IT investments and advanced telecom networks will grow faster.¹ With this growth comes the potential to deliver significant benefits to consumers, businesses and society, through improvements in inter alia transport, healthcare and the environment.

In the recent years, NRAs have primarily been contacted by stakeholders on issues regarding mobile network based IoT solutions. In addition, stakeholders were mostly concerned with questions involving numbering, roaming and switching between service providers.² Therefore this report assesses these topics in more detail. However, it has to be stressed that many IoT services exist or may be developed which are based on another kind of connectivity (including fixed and another kind of wireless connectivity) than mobile connectivity. In fact, recent data show that only a minor fraction of M2M connections will be based on cellular technologies which means that some of the IoT devices may require a SIM card, but most of the IoT devices will not. This is backed by the following market projections:

| | 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)

This means that any possible regulation with regard to cellular connectivity would only apply to a small subset of the market.

Purpose/aim, scope and limitation

¹ “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination”, Study prepared by IDC and TXT for the European Commission, 13 May 2015, cf. <http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>, p. 26-27.

² Cf. Annex 2 for stakeholder interviews during the year 2014 as well as Consultation Report.

This document gives BEREC's survey and assessment of the state of play on IoT services with the perspective of fostering an environment that will result in sustainable competition, interoperability of electronic communications services and consumer benefits. It is aimed at presenting the most common characteristics of IoT services and assessing whether IoT services might require special treatment with regard to current and potential future regulatory issues. Some suggestions by BEREC addressed to NRAs – where possible – are included on how to deal with them.

The scope of this report, the detailed topics contained within it and suggestions for how areas of work may be taken forward will in part be constrained by the specific duties that fall to the various NRAs. Consequently, the report deals only to a certain extent with issues which, depending on the country, are not or not entirely within the NRAs' remit (such as privacy and standardisation).

Terminology

IoT services are in varying phases of development and take various shapes, hence there is not yet a common understanding or definition of what IoT services and devices really are. Please note that the notion "service" is used throughout the entire document, including this chapter, to explain the service provided in the IoT value chain but not in the meaning of the definitions laid down in the ITU Radio Regulations³. In the latter context, the notion "IoT application" would be more appropriate. Moreover, the notion "M2M communication" is used in order to describe the (technical) connection between an IoT device and a data center, between two devices or the like, which is underlying an IoT service.

In a 2010 paper on convergent services, BEREC described M2M as "*a generic concept that indicates the exchange of information in data format between two remote machines, through a mobile or fixed network, without human intervention.*"⁴ In a recently published report by the EC, the following definition of IoT is used: "*The Internet of Things enables objects sharing information with other objects/members in the network, recognizing events and changes so to react autonomously in an appropriate manner. The IoT therefore builds on communication between things (machines, buildings, cars, animals, etc.) that leads to action and value creation*".⁵

Similarly, some stakeholders only regard such automated exchange between machines as M2M communication where no human beings are involved.⁶ However, according to other

³ The ITU Radio Regulations contains the complete texts as adopted and revised by the World Radiocommunication Conference, cf. <https://www.itu.int/pub/R-REG-RR> and http://www.itu.int/dms_pub/itu-s/oth/02/02/S02020000244501PDFE.PDF.

⁴ BEREC, Report on convergent services, BoR (10) 65, December 2010, p. 6.

⁵ "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", Study prepared by IDC and TXT for the European Commission, 13 May 2015, cf. <http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>.

⁶ GSMA Intelligence, From concept to delivery: the M2M market today, p. 5: "The GSMA Intelligence M2M connections data used in this report refers exclusively to a SIM connection that enables mobile data transmission between machines. It does not count SIMs used in computing devices in consumer electronics such as smartphones, dongles, tablets, e-readers, routers and hotspots". However, in its submission to the draft BEREC Report "Enabling the Internet of Things", GSMA also includes autonomous communication between connected devices and appliances "with limited human intervention" as M2M communication, cf. p. 4. For a similar definition, see ETSI (ETSI TR 102 725 V1.1.1, Machine-to-Machine communications (M2M); Definitions): "physical

definitions, limited human intervention may be part of M2M communication.⁷ In this case, services which can be remotely controlled, such as via smartphones or tablets, may also be examples of IoT services, e.g. remote control of air conditioning and heating systems or the remote (un)locking of cars. However, this does not imply a general statement on the qualification of a service as IoT service with regard to all cases where an app on a smartphone or tablet is involved.

For the purposes of this report, it is not necessary to determine in detail which definition is most appropriate. Fixing a definition of M2M communications or IoT services only makes a crucial difference if obligations explicitly depend on that distinction. In this regard, we note that the definition which includes “limited” human intervention is less clear-cut than the definition which excludes it, since it has to be determined on a case-by-case basis whether such intervention still is “limited”. However, also vague expressions can be interpreted by NRAs and the courts, but if one decided to apply such definition the merits of doing so should outweigh the legal uncertainty attached to it.

By contrast, other publications focus on the terms IoT and/or “Internet of Everything”⁸ (IoE) when referring to the devices and services described in this report. The IoT describes the interconnection of large numbers of everyday devices to provide a range of new and innovative services.⁹ Sometimes, the terms M2M and IoT are used to describe the same services and types of connections.¹⁰

Characteristics

Current IoT services broadly share some of the following characteristics:

- Fully automatic communication of data from remote devices (or with limited human intervention).
- Relatively simple devices, that can either be static (e.g. smart meters) or mobile (e.g. IoT devices integrated in connected cars).
- Low volume traffic, often with sporadic or irregular patterns. However, IoT services have already emerged and/or might emerge in the future that transmit data in greater volumes,

telecommunication based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure”.

⁷ ECC Report 153, Numbering and Addressing in Machine-to-Machine (M2M) Communications, November 2010, p. 5, section 1: “M2M is a communication technology where data can be transferred in an automated way with little or no human interaction between devices and applications.”; OECD, Machine-to-Machine Communications: Connecting billions of devices, DSTI/ICCP/CISP(2011)4/FINAL, 30 January 2012, p. 7. Moreover, this report does not make any statement on eCall services for which a special regulation applies, cf. regulation (EU) No 305/2013.

⁸ This notion was first used by Cisco, cf. <http://www.cisco.com/c/r/en/us/internet-of-everything-ioe/index.html> and <http://blogs.cisco.com/tag/internet-of-everything>.

⁹ Ofcom, Promoting investment and innovation in the Internet of Things, 27 January 2015, p. 9. See also ITU-T Y.2060, where IoT is described as “[a] global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies”.

¹⁰ In fact the Art. 29 Data Protection Working Party describes IoT as “an infrastructure in which billions of sensors embedded in common, everyday devices – “things” as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.” Cf. Opinion 8/2014 on the Recent Developments on the Internet of Things, p. 4.

especially if demand for video-based services increases (e.g. automatic analysis of surveillance video streams, alarm systems).

- IoT services require connectivity, but connectivity accounts for a relatively low proportion of the overall revenue opportunity in the IoT value chain.¹¹
- Many IoT services are provided via devices designed and produced for the world market and for usage based on global mobility.
- Many IoT devices are designed to have a lifetime of many years and may be installed within equipment or infrastructure that itself has a long lifetime. Therefore, the cost of replacement may be relatively high.
- In most cases, the business model is B2B, even if devices may be aimed at consumers (B2B2C). The business model is usually not B2C.¹²

There are different ways in which IoT services could be implemented:

- Different connectivity technologies may be used and, in the case of wireless services, different spectrum bands may be used (cf. below in 2.1.).
- IoT services may use different protocols to deliver their data. They may be based on the IP protocol but could also use SMS, USSD and/or automatic calls.
- An IoT device is addressed via an identifier (e.g. number(s), IP-address), cf. below in 2.2.). However, not all IoT devices need global identifiers (e.g. those that are not connected to public networks).

Main areas of current and/or future IoT services, including M2M communications, are: automotive¹³, E-health services¹⁴, smart metering/smart grids¹⁵, smart home, smart cities¹⁶, industry/automation and agriculture.¹⁷ Examples are set out in figure 1 below.

¹¹ Source: GSMA report: Analysis – “From concept to delivery: the M2M market today“ February 2014, p. 12 (http://www.gsma.com/connectedliving/wp-content/uploads/2014/02/M2M-report_GSMAi.pdf).

¹² Hence, IoT services are changing the relationship between connectivity providers and end-users: the connectivity providers are losing the direct relationship with the end-user (typical B2C model), which becomes, instead, in many cases the prerogative of the IoT user.

¹³ Smart cars: A wide range of car sensors can send automatic status updates to the manufacturer’s system to report on damages, making sure that garages are informed in time and the necessary replacement parts are in stock.

¹⁴ Vital signs are recorded by smart wearable devices which inform – via an e-health gateway – connected parties, such as nursing services and doctors, if a patient forgot to take pills or even on life-threatening situations.

¹⁵ Producers and consumers of energy (electricity, gas) are connected via M2M communication to ensure an optimised flow of energy without possible negative or positive peaks in consumption, which otherwise are likely to happen due to new forms of energy production (i.e. renewable energy).

¹⁶ Public services such as lightning, waste management or the administration of parking areas can be offered at a lower cost rate when devices such as street lamps, garbage cans, parking lots, navigation systems and cars are connected to each other.

¹⁷ Sensors for moisture or nutrients placed in the soil inform automatic watering and manuring devices to provide a growth process at the best possible rate.

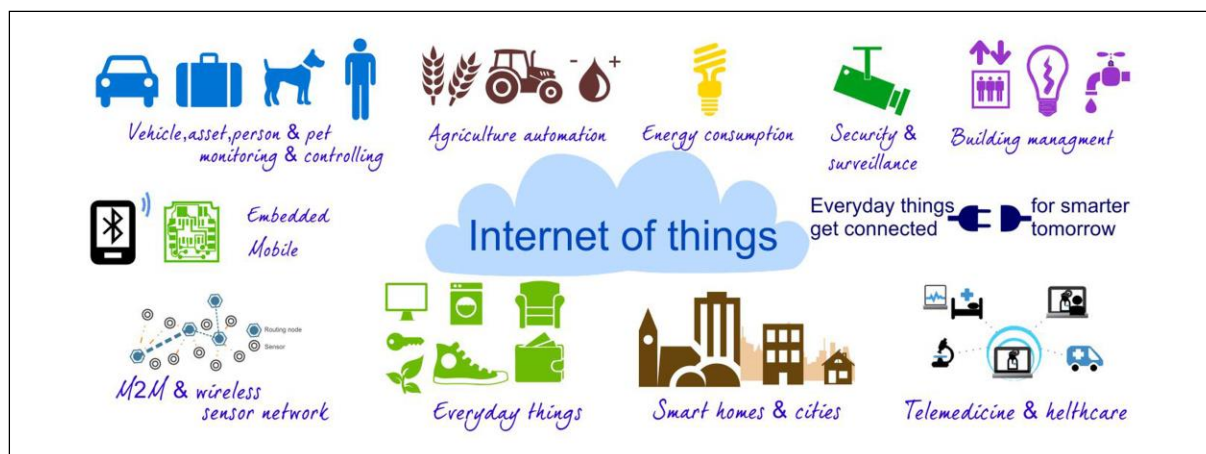


Figure 1: Areas of application of M2M communications¹⁸

Typical examples of the IoT value chain

A market player may have several roles and there are many examples of how the IoT value chain may look. For the purpose of this report, the market players in the value chain are understood as follows:

| | |
|-------------------------------|---|
| Connectivity service provider | Provider of an electronic communication service pursuant to Art. 2 lit. c Framework Directive, i.e. basically a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks. |
| IoT service provider: | Provider of an IoT service, which can comprise the provision of an IoT platform and/or other IoT-related IT-services/solutions. |
| IoT user: | Purchaser of an IoT service who incorporates the IoT service as one component in his own products (i.e. connected devices) and/or services (e.g. a car manufacturer, an electricity provider which also includes the provision of a smart meter in its service). |
| End-user: | Customer at the end of the value chain who purchases a connected device and/or utilises a service (including an IoT service and/or IoT device) (e.g. car owner, electricity customer). An end-user may be a private person or a company (e.g. private car owner and/or company with a car fleet). |

One typical – and very simplified – example for an IoT value chain is shown in figure 2: For the sake of simplicity, not all market players are included in the chart.¹⁹ In some cases, the same undertaking or subject may play more than one role at the same time.²⁰

¹⁸ Source: <http://datasciencebe.com/>. Image published under the article “The Thing in Internet of things”, published in <https://inventrom.wordpress.com/>

¹⁹ Not included are e.g. producers of hardware such as sensors and IoT devices.

²⁰ For example, a city planning to connect traffic lights might decide to supply itself with connectivity by building its own wireless network. In such a case the city plays all roles in the value chain.

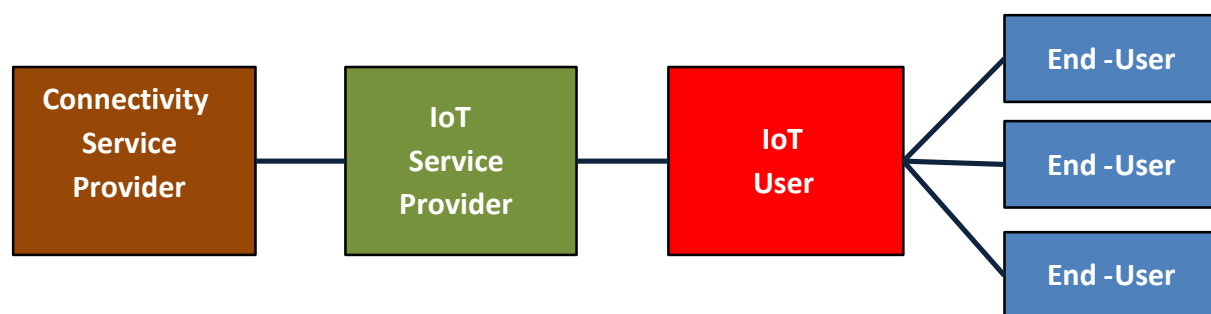


Figure 2: IoT value chain

Usually, the connectivity service providers' customers are the IoT device makers, the IoT service providers or the IoT users, not the end-users (in the sense of this report). Often the connectivity service providers have no relationship with the IoT service providers, and run their business with the hardware manufacturers. The end-user, on the other hand, buys an interconnected device and is not necessarily interested in the communication service as such. The service of the connectivity service provider to the IoT device maker, IoT service provider or IoT user is a wholesale-type of arrangement.

| Industry | Connectivity Service Provider | IoT Service Provider | IoT user | End-user |
|-------------|-------------------------------|----------------------|-------------------------------------|-----------------------|
| Automotive | Connectivity Service Provider | IoT Service Provider | E.g. car manufacturers | Car / car fleet owner |
| E-Health | | | E.g. producers of medical equipment | Patient |
| Electricity | | | E.g. electricity companies | Electricity customer |
| Agriculture | | | E.g. producers of farming equipment | Farmer |

For the IoT user, there are generally two main options to procure the connectivity service and the IoT service.²¹ He can conclude one or two contracts. If he decides to conclude one contract, there are several sub-categories: In the above example, the IoT user purchases the IoT service from the IoT service provider who, in turn, purchases the connectivity from a connectivity service provider. The IoT user may also contract with the connectivity service provider which, in turn, purchases the IoT service as an input product. Alternatively the IoT user may choose to contract with a company which is an integrated connectivity service provider/IoT service provider.²² Moreover, the IoT user may opt for concluding two separate contracts with the connectivity service provider and the IoT service provider. Apart from that, for an IoT service connectivity may be used which is provided according to a contract concluded between an end-user and a connectivity service provider. (i.e. where the IoT service is basically provided as an OTT service). In case of production and distribution of connected devices and/or services

²¹ Apart from that, other options are possible. Moreover, the IoT user may opt not to procure the respective services but to provide them in-house (i.e. as a vertically integrated IoT user).

²² Many of the connectivity service providers – especially if they are incumbents or other bigger players – appear to also offer IoT services, at least at group level.

which include an IoT service or IoT device, the end-user is an entity separate from the IoT user. In case of industrial IoT services, the IoT user usually is at the same time also the end-user. These described examples for IoT value chains are presented in Annex 1.

For IoT services to thrive several preconditions need to be fulfilled which relevant authorities (NRAs, European Commission, other authorities, Member States etc.) might help to establish and which are set out in the following sections of the report:

- Firstly, sufficient resources (like spectrum as well as numbers, IP addresses and other identifiers) in order to underpin and support the service (cf. section 2.).
- Secondly, an EU Telecommunications Framework which fits to IoT services (cf. section 3.).
- Thirdly, consumers' acceptance of IoT services, which depends among other things on the information provided to them about the level of privacy, network and data security and interoperability of services, devices and platforms (cf. section 4 on privacy and standardisation as well as 3.4 on network security).

During the consultation of the draft version of this report several questions have been addressed to stakeholders. The consultation responses including BEREC considerations following from them are summarized in the Consultation Report.²³

2. Ensuring adequate resources for IoT services

IoT services will be underpinned by a number of fundamental resources, such as spectrum and telephone numbers or addresses. While technical management of the identifiers of the Internet (IP addresses) comes under the responsibilities of the Internet Corporation for Assigned Names and Numbers (ICANN), in co-operation with the Réseaux IP Européens Network Coordination Centre (RIPE NCC²⁴), the allocation of spectrum and telephone numbers is within the remit of national authorities of the electronic communications sector, who will play an important role in ensuring an adequate supply of these resources to support the development of IoT services.

2.1. Spectrum

IoT services²⁵ may be deployed using a range of communication technologies, both wired and wireless. However, many of these services will require the flexibility or mobility of wireless networks and will, therefore, rely on the availability of spectrum to support their connectivity.

2.1.1. The different spectrum requirements for the IoT

There is no one, single description of the spectrum requirements for IoT services; rather, the spectrum requirements for a given IoT service will be heavily influenced by the specific nature of that service. For example:

²³ BoR (16) 38, BEREC Report on the Public Consultation of the Report “Enabling the Internet of Things”

²⁴ <https://www.ripe.net/> - RIPE NCC is the Regional Internet Registry for Europe, the Middle East and parts of Central Asia. They are in charge of the allocation and register of blocks of Internet number resources to Internet service providers (ISPs) and other organisations in the referred geographical service region. These Internet number resources are mainly in the form of IPv4 and IPv6 address space and Autonomous System Numbers (ASNs).

²⁵ Please note that the notion “service” is used throughout the entire document, including this chapter, to explain the service provided in the IoT value chain but not in the meaning of the definitions laid down in the ITU Radio Regulations. In the latter context, the notion “IoT application” would be more appropriate.

- From a technical perspective, lower frequency spectrum enables wider area coverage and better penetration deep into buildings;
- From an authorisation perspective, licensed spectrum – either for private/professional networks or for public mobile networks (terrestrial systems capable of providing ECS) – assures the reliable delivery of data, compared to unlicensed spectrum; and
- If there is a need for devices to have very long battery life, there may be a requirement to use bespoke and highly optimised technologies which may require their own allocation of spectrum to work efficiently.

More specifically, in many cases, the requirements of a particular IoT service will influence the technologies used to provide it, which, in turn, determine the underlying spectrum requirements. A range of existing and emerging technologies can be used to provide IoT services. They include:

- Personal and local area technologies: Short range connectivity can be provided by conventional, general purpose technologies such as Wi-Fi or Bluetooth. These technologies may be particularly appropriate for consumer IoT services, such as health or fitness trackers. Optimised versions of Bluetooth and Wi-Fi are also emerging;
- Wide area low power technologies: A number of bespoke technologies are being developed and are optimised specifically for certain IoT services. When deployed using sub-1GHz spectrum, these technologies are capable of providing relatively wide area coverage. In addition, their protocols enable them to use either licensed or licence exempt spectrum;
- Mobile technologies: Existing mobile networks, such as GSM, have been used for several years to provide wireless point of sale applications. Various technical enhancements are being proposed which will enable mobile networks to support a wider range of IoT services more efficiently and allowing connectivity service providers to support these services using much of their existing infrastructure. These enhancements include an air interface capable of efficiently supporting IoT services within a 200kHz channel bandwidth called NB-IoT and IoT-optimised variants of the LTE standard used for 4G services. In the longer term, 5G networks will emerge that will efficiently support a range of services, including IoT; and
- Satellite technology²⁶.

2.1.2. Current availability of spectrum that can address the needs for M2M connectivity

The RSPG²⁷ Report on “Strategic Sectoral Spectrum Needs”²⁸ focused on the development of a strategic policy approach to meet spectrum needs for different sectors and in particular for the IoT, including radio frequency identification tags (RFIDs) and M2M. For this sector, the RSPG has identified no requirements that would motivate a harmonised European solution for

²⁶ Satellite technology is used in the logistics sector as well as in the aviation industry, e.g. the Aircraft Communications Addressing and Reporting System (ACARS), a system that automatically sends information by satellite from the airplane to the airline.

²⁷ Radio Spectrum Policy Group: High-level advisory group that assists and advises the European Commission on radio spectrum policy issues, on coordination of policy approaches, on the preparation of multiannual radio spectrum policy programmes and, where appropriate, on harmonised conditions with regard to the availability and efficient use of radio spectrum necessary for the establishment and functioning of the internal market. (Art. 2 Commission Decision of 26 July 2002 establishing a Radio Spectrum Policy Group amended by Commission Decision 2009/978/EU of 16 December 2009).

²⁸ http://www.cept.org/files/9421/RSPG13-540rev2_RSPG_Report_on_Sectoral_needs.pdf

dedicated spectrum for specific services or applications. However, the large predicted growth within some of these analysed sectors contributes to an increased need and demand for capacity and bandwidth, which may be met in the future through a suitably expanded identification of bands under general authorisations (exemption from individual licensing). Moreover, given their related key requirements, the RSPG considers that many of these needs are best to be realised using spectrum below 1 GHz.

The RSPG conclusion was motivated by the high availability of spectrum resources that can be used to address the different needs of different IoT services.

For IoT services using mobile technologies, any frequency band harmonised for terrestrial systems capable of providing electronic communications services can be used. These bands include the 800 MHz, 900 MHz, 1450 MHz, 1800 MHz, 2 GHz, 2.6 GHz and 3.4 – 3.8 GHz bands and in the future also the 700 MHz band.

Furthermore, many of the unlicensed frequency bands used by IoT services are harmonized by the latest update of Commission Decision 2006/771/EC for SRD (short-range devices) and by CEPT ERC Recommendation 70-03 (SRD). It is the case for Wi-Fi²⁹ and Bluetooth bands, and frequencies at 868 MHz used by M2M / Wide area low power. A regular update of this SRD Decision is anticipated in the SRD Decision, based on a permanent Mandate to CEPT as a regular review (next one is expected in 2016) based on the updates to ERC Recommendation 70-03.

Within Europe there are also many PMR/PAMR frequency bands in between 30.01 MHz and 942 MHz that could be used for IoT services.³⁰ These bands have a harmonization through ECC Decisions and ECC Recommendations which are voluntary for Member States to implement. The IoT usage in these bands is normally provided by bespoke networks optimised for a specific application and that do not need interoperability outside their own network.

Against this background the RSPG report also made the conclusion that future spectrum needs for M2M can be addressed via the ETSI-CEPT process.

The RSPG is further assessing the spectrum-related side of M2M in its current work on an “Opinion on the review of the current RSPG and its revision to address the next 5 years period”³¹ and is going to deal with M2M under the frame of its next work programme.

2.1.3. Meeting future demand for spectrum

It is important that NRAs recognise that all delivery mechanisms of and technologies for IoT could be deployed by industry and other stakeholders as the IoT market develops. It is also important to acknowledge that the long lifetime and high replacement costs of many IoT devices could necessitate enduring access to certain spectrum bands over an extended period. NRAs should, therefore, seek to identify and remove possible barriers to the deployment of these technologies wherever feasible. For example, this could involve

- Modifying licence obligations to allow the deployment of IoT-optimised technologies within their existing spectrum allocations;

²⁹ The 5 GHz Wi-Fi band is harmonised by the Commission Decision 2005/513/EC amended by 2007/90/EC and ECC Decision (04)08. The 2.4 GHz Wi-Fi band is harmonised by the SRD regulation.

³⁰ <http://www.efis.dk/>

³¹ Adoption for public consultation expected for the RSPG plenary meeting in October 2015.

- Modifying the usage conditions for specific bands for new use and users on a licensed or licence exempt basis;
- Opening up bands for access on a shared basis.

An in-depth picture of the current situation of the spectrum usage in Europe³² - not limited to IoT services - is provided by the CEPT via the ECO Frequency Information System (EFIS). This is the tool to fulfill EC Decision 2007/344/EC on the harmonised availability of information regarding spectrum use in Europe and the ECC Decision ECC/DEC/(01)03 on EFIS.³³

In order to determine the likely future demand for spectrum for IoT services, it is necessary to form a view on the likely size and shape of the market. In Europe alone, a study prepared for the EU Commission recently expected IoT connections across EU 28 to exceed 6 billion units by 2020.³⁴ Given the significant number of likely devices, it will be important to ensure that there is sufficient spectrum to support the full range of IoT services. It is noted that Member States have developed different national solutions.³⁵

Other current or emerging spectrum options for deploying IoT services include:

- *White spaces*: Applications could be deployed in the gaps between the transmissions of other systems, in spectrum that would otherwise remain unused. One example is the use of gaps between the transmission of digital terrestrial TV services below 1GHz; and
- *700MHz*: There is a proposal to use at national level the duplex gap and guard bands³⁶ of 700MHz which has been identified for future mobile broadband use.

In the longer term and as the market develops, the spectrum requirements for IoT services may change and it is therefore important for NRAs to monitor market developments and spectrum use and, if necessary, take steps to make additional spectrum bands available for

³² For 48 European CEPT countries, including the EU Member States.

³³ <http://www.efis.dk>

³⁴ "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", Study prepared by IDC and TXT for the European Commission, 13 May 2015, cf. <http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>, p. 24

³⁵ Furthermore, by way of an example, a study for Ofcom in 2014 assessed the likely size of the IoT market in the UK for a range of applications and identified likely requirements for spectrum, cf. M2M Application Characteristics and their Implications for Spectrum, report for Ofcom, April 2014, <http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2014/M2MSpectrum>. The study noted that the number of IoT devices is likely to be very large, growing to in excess of 360 million in the UK alone by 2022. However, given that many IoT services only transmit small amounts of data, the study concluded that, in the short to medium term, the UK's existing allocations of spectrum would be sufficient to meet demand. In the UK, Ofcom has been proactive in identifying and making available spectrum bands that could be used for a range of services, including IoT. In particular, the 870-876MHz and 915-921MHz bands are available on a licence exempt basis and the 870-873MHz sub-band can also be used by higher power network relay points, which could be used to create meshed network architectures for IoT services. In France, ARCEP has launched, in 2014, a public consultation on the use of open spectrum aiming to deepen forward-planning on the future use of and need for open spectrum, particular in view of the upcoming development of the IoT. The feedback from market players served to underscore the importance and multiplicity of the issues that are bound up with the IoT. Frequencies, and particularly the identification of unlicensed spectrum, are key to the development of innovative applications. In the Netherlands, a frequency band previously allocated for personal mobile communications has been identified for M2M use. The frequencies around 450MHz will be used to support the country's smart meter programme.

³⁶ The duplex gap is the portion of unused spectrum between the bands allocated for the uplink and downlink transmissions of a frequency division duplex (FDD) system. The duplex gap reduces the likelihood of uplink and downlink transmissions interfering with each other. The guard band is the portion of unused spectrum between two neighbouring allocations, typically used by different technologies, e.g. cellular and television systems. Leaving the guard band unused reduces the likelihood of these different systems interfering with each other. Use of the duplex or guard bands could be possible under certain conditions, such as very low transmission power.

IoT services. This could involve making new bands available, liberalising the use of existing bands or opening up bands for access on a shared basis.

A range of technology options are likely to be used to deploy IoT services. Given the variation in maturity in the evolution of the IoT market across Member States, NRAs should monitor market developments and spectrum use. For the benefit of harmonization, industry is invited to make use of the established processes via ETSI and CEPT if it identifies the demand for additional spectrum. Based on these harmonized European Standards and frequencies, NRAs are invited, where appropriate, to make spectrum available to support these applications.

2.2. Identifiers

Possible issues regarding scarcity of identifiers may only be applicable to public networks. Consequently, the analysis in this section is restricted to the following possible identifiers for IoT devices: telephone numbers (cf. 2.2.1) and IP addresses (cf. 2.2.2.). Other identifiers, such as MAC addresses or names – even if they are relevant for many IoT services³⁷ – do not appear to have any significant limitation in their use if they are used outside public networks (e.g. “behind” an identifier which is the gateway to the public network). If low power wide area networks (LPWAN) technologies develop, specific issues with regard to identifiers might come up, in particular if it is a public network.³⁸ At this early stage of emergence of these technologies, this specific topic is not developed here.

2.2.1. Numbers

With regard to numbering, the following issues are discussed in the IoT context:

- Type of numbers to be used for IoT services;
- Right to request numbers, in particular mobile network codes (MNC) for services using mobile networks;
- Scarcity of numbers;
- Extra-territorial use of numbers.

2.2.1.1. Type of numbers to be used for IoT services

The first issue relates to what kinds of identifiers are useful to identify IoT devices at the network level in a public network and how this might change in the future. The potential number of IoT devices is large and increasing. Accordingly, there will be a need for a large amount of device identifiers.

³⁷ Such identifiers may be used in IoT devices which are not - or not directly – connected to a network termination point, e.g. in private networks (e.g. IoT industry applications) or networks connected via a gateway to the public network (e.g. smart home applications), or meshed networks (e.g. car-2-car communication).

³⁸ LPWAN technologies are generally based on technology specific device identifiers. In case these networks develop, an efficient allocation process of these identifiers might have to be set up to answer the needs of operators and their customers, which may in time deserve some attention.

At network level in a public network, in general, the following national and international telephone number could be used for the addressing in IoT services:

- National E.164 numbers;
- International/global E.164 numbers (CC³⁹ 882/883) assigned by the ITU;
- National E.212 IMSI (International Mobile Subscriber Identity);
- International/global E.212 IMSI with MNCs under MCC⁴⁰ 901 assigned by the ITU.

At network level, no other public addresses seem to be used for the time being.

In particular, since the early stages of the development of IoT services, the approach by connectivity service providers and IoT service providers has been the use of existing ranges of national E.164 numbers (especially mobile numbers) and E.212. This is because of their relative ease of implementation into existing network infrastructures. It is very likely that in the short to medium term – and perhaps even in the long term – E.164 and/or E.212 identifiers will be used for addressing IoT devices, even after an increased use of IPv6 addresses.

Numbering issues related to IoT have been discussed (and are still being discussed) by CEPT ECC WG NaN. In this regard, reference is made in particular to ECC Report 153 on “Numbering and Addressing in Machine-to-Machine (M2M) Communications”.⁴¹

In case of mobile subscriptions using public mobile networks, E.212 IMSIs and E.164 numbers are typically used.

2.2.1.2. Right to request numbers (in particular E.212 (MNC))

With the current national regulations, in various countries, the assignment of MNCs is limited to MNOs and, in some countries, to certain mobile virtual network operators (MVNOs). mainly due to an harmonization compromise within ITU-T (Recommendation ITU-T E.212, Annex B). This means that many countries do not allow the assignment of MNCs to IoT users. Such an assignment might lower barriers to competition in the market if IoT users have the technical and economic capacities required to operate their own MNC (i.e. become assignee of an MNC) and to insource the respective activities in order to effectively switch from one connectivity service provider to another (see for the associated lock-in problem below in section 3.3.), which however might, at best, only concern the largest fleets of IoT devices.

As CEPT has pointed out, the presence of new market players for IoT suggests that NRAs should consider adopting greater flexibility in assigning MNCs. However, if new rules broaden the circle of possible assignees of MNCs, possibly including IoT users, the number of available MNCs in the respective country may decrease and lead to scarcity (see also 2.2.1.3. below).

Hence, each NRA should undertake measures to administer and allocate MNCs in a way that does not lead to scarcity.

Another solution to cope with the lock-in problem could be the promotion of SIM cards whose profiles can be uploaded and updated Over-The-Air (OTA), cf. also below in 3.3.2. Above all, this solution is likely to facilitate the change of connectivity service provider.

³⁹ Country Code (CC).

⁴⁰ Mobile Country Code (MCC).

⁴¹ Published in November 2010; in the following: ECC Report 153.

2.2.1.3. Scarcity of number resources

The availability of sufficient numbers (both E.164 and E.212) has to be ensured.

At present and under the current numbering plans, the possible scarcity of E.164 resources does not appear to be the main obstacle to the development of IoT. However, this potential issue should be carefully analysed and solved by each NRA at national level, if needed (e.g. by opening up a dedicated M2M numbering range or otherwise increase the resources dedicated to E.164 mobile numbers). Although, the introduction of new numbering ranges could introduce delay in their use.

With regard to E.212 resources, sufficient IMSIs (i.e. individual E.212 number resources) are available.⁴² However, there is the risk of scarcity of E.212 resources (MNCs) due to the fact that, in most cases, only 100 MNCs are available per mobile country code (MCC).⁴³ In particular, scarcity could become an issue if the E.212 resource assignment rules are relaxed in order to take into account the presence of new players in the IoT market (the IoT users) that could take advantage from being assigned their own MNC. Possible solutions which try to reconcile the aim of promoting competition and preventing number scarcity are discussed in the ECC Report 212, "Evolution in the use of E.212 Mobile Network Codes".⁴⁴

2.2.1.4. Extra-territorial use of numbers

Based on feedback received from stakeholders, the majority appears to favour an extra-territorial use of national E.164 and E.212 numbers to support IoT services which are incorporated in products which are manufactured for the world-market. In many countries, it is currently unclear whether such an extra-territorial use of numbers is permissible in the IoT context. In any analysis of this issue it should be assured that public policy objectives (such as public security, national sovereignty etc.) are not compromised. An internationally harmonised approach could be desirable. In this context, reference is made to ECC Report 194 "Extra-Territorial Use of E.164 Numbers".⁴⁵

A complementary solution appears to be the use of global resources assigned by ITU (i.e. ITU-T Country Code 882/883 for E.164 numbers and MNCs under MCC 901 for E.212 ones). This could be useful in case of IoT services and connected devices that are distributed internationally but additional complications and costs may arise in the case of using global resources (e.g. conclusion of new roaming agreements, testing). Also, requesting ITU

⁴² Under one MNC, 10 billion International Mobile Subscriber Identities (IMSI) are available (provided that the Mobile Subscriber Identification (MSIN) is 10-digit).

⁴³ Although the ITU-T Recommendation E.212 foresees the use of 2 or 3 digits for this field, actually in most countries only 2 digits are used.

⁴⁴ Published on 9 April 2014; in the following: "ECC Report 212".

⁴⁵ Published on 25 April 2013; in the following: "ECC Report 194". The ECC concludes that as a general rule the extra-territorial use of E.164 numbers should not be allowed because the negative effects listed in this Report outweigh the perceived benefits.

As a consequence:

- A country should in general refuse the assignment of E.164 numbers belonging to its numbering plan to be used outside of its territory on a permanent basis.
- A country should in general not allow the use of E.164 numbers belonging to another country's numbering plan in its territory on a permanent basis.
- Extra-territorial use of numbers should only be permitted in exceptional cases which have been defined by an ECC Decision. Possible candidates are some nomadic voice services and some M2M services.

resources might prove a hurdle for some companies (in particular in view of the high membership fee). Promotion of the use of global resources might help to overcome these issues. It is noted that several MNOs and full MVNOs have already become assignees of an MNC under MCC 901.⁴⁶ Further assessment over time of the evolution of applications and services based on the use of such global resources may prove useful.

The European Commission recently suggested the use of a European numbering scheme for M2M services.⁴⁷ From a cost-benefit perspective, BEREC believes that the introduction of a European numbering scheme does not seem to carry any significant benefits which would justify the deployment costs of setting up such a solution.⁴⁸

Instead, BEREC considers that the use of existing numbering resources - the extraterritorial use of numbers and the use of ITU numbers - seems to be a reasonable approach.

2.2.2. IP addresses

In addition to telephone numbers, IP addressing will be very important as an complementary addressing resource for IoT services.

- Where devices are connected via fixed line or WLAN, IP addresses are used already today.
- If it becomes possible in public mobile networks to address devices directly via IP addresses, i.e. without the use of E.164 numbers, also mobile M2M communication could be gradually converted and the use of E.164 numbers could be discontinued. However, at present it cannot be foreseen whether such fundamental changes will become reality.

The hitherto commonly used IPv4 address format supports a relatively limited number⁴⁹ of globally addressable devices; however, many connected devices may be located behind one IPv4 address using Network Address Translation (NAT). Given the expected growth of IoT services, and the number of Internet connected devices generally, this limited address space could quickly be exhausted.

The IPv6 standard has a significantly larger address space⁵⁰ and can support a considerably higher number of devices. Connectivity providers have recognised the importance of this migration for the growth of new services and are in the process of upgrading their networks to

⁴⁶ A list over the current assignments of MNCs under the shared MCC 901 can be found at http://www.itu.int/net/ITU-T/inrdb/e212_901.aspx. Assignees include international MNOs such as AT&T, Vodafone, Deutsche Telekom, Telecom Italia, Orange and Telenor.

⁴⁷ Roberto Viola, "Machine to machine connectivity in a Digital Single Market", published in the blog "Digital Agenda for Europe", 04/09/2015, cf. <http://ec.europa.eu/digital-agenda/en/blog/machine-machine-connectivity-digital-single-market>; European Commission, COCOM15-13, 30 September 2015, "Machine-to-machine (M2M) connectivity in a digital single market: Challenges for numbering policy resulting from M2M development in Europe".

⁴⁸ This is in particular due to the geographic limitation of a European numbering scheme, its costs of implementation and the lack of truly European use cases. Even if eCall might be a use case which is geographically limited to the EU, the introduction of European numbers would not be in time with regard to the entry into force of the obligation to offer eCall, taking into account the time required for opening up of such numbering ranges (including reaching a political consent, agreeing on respective rules governing such numbering ranges as well as the implementation in the networks). For more details cf. Consultation Report, answer to Question 1, as well as COCOM Minutes of 14 October 2015, p. 15-20 for Member States' submissions.

⁴⁹ An IPv4 address consists of 32 Bit. Hence, 2^{32} (4,294,967,296) addresses are theoretically available, even if in practice a certain amount is reserved for other purposes than public network addresses.

⁵⁰ An IPv6 address consists of 128 Bit. Hence, 2^{128} (340,282,366,920,938,463,463,374,607,431,768, 211,456 \approx $3,4 \cdot 10^{38}$) addresses are theoretically available, even if in practice a certain amount is reserved for other purposes than public network addresses.

support IPv6. However, it is expected that IPv4 and IPv6 will exist alongside for quite some time although use of IPv6 has seen substantial growth over the last few years.

Within the EU, 66% of local internet registries (LIRs) have already taken steps⁵¹ to support IPv6 and over 27% of networks⁵² within the EU support IPv6. For a global IoT market, device manufacturers will consider the breadth of IPv6 deployment before beginning development of IPv6-only devices. This has the effect of the late movers in IPv6 deployment affecting the IoT manufacturers' decision process.

There might also be a substantial overlap period where both IPv6 – and IPv4 – addresses and E.164 numbers are in use. There are some estimations from stakeholders that it will take five to ten years for IPv6 to become widely available.⁵³ However, the issue of new E.164 numbers could begin to be phased out when IPv6 addresses becomes widely available and then only for those devices that do not have any requirement for traditional voice or SMS services. When mobility is a necessary characteristic of the service, E.212 resources probably will continue to be needed.

The Réseaux IP Européens Network Coordination Centre (RIPE NCC) is the Regional Internet Registry (RIR) for i.a. Europe. It is competent for the allocation and registration of Internet number resources. However, some Member States are competent with regard to some related aspects.⁵⁴

The identifiers used for IoT services in public networks are: E.164 and E.212 (IMSI) numbers as well as IPv4 and IPv6 addresses. In the short and medium term – and perhaps even in the long term – classical telecommunications numbers (E.164 and E.212) will continue to be one solution to identify IoT devices. In the longer term, the use of IPv6 addresses might become the preferred solution.

Many of the numbering issues NRAs currently have to tackle – and which are primarily dealt by CEPT and/or ITU on an international level – concern IoT services based on mobile connectivity:

Firstly, the alleged scarcity of E.164 numbers does not seem to be a barrier or a problem to be solved to foster the development of IoT. Anyway, the issue of possible scarcity of E.164 numbering resources should be analysed and solved by NRAs at national level, e.g. introducing a new numbering range for IoT services or increasing the mobile number resources.

Secondly, the current national regulation in several countries does not allow IoT users to be assignees of MNCs although this may be a way to ease change of connectivity provider – besides over-the-air provisioning of SIM – without having to physically swap the SIM (cf. section 3.3.). On this issue CEPT suggests the relaxation of the assignment criteria. Still, broadening the circle of assignees might lead to a scarcity of E.212 MNC resources since in many countries only 100 MNCs are available. A flexible approach at national level on how to solve this issue might be appropriate.

⁵¹ RIPE Network Co-ordination Centre statistics as of 7 May 2015, defined as having a „ripeness“ rating greater than 0, <http://ripeness.ripe.net/pies.html>

⁵² RIPE Network Co-ordination Centre statistics as of 7 May 2015, http://v6asns.ripe.net/v/6?s=_EU

⁵³ <http://stakeholders.ofcom.org.uk/consultations/iot/?showResponses=true>

⁵⁴ For example, in the UK Ofcom has a duty to report to the Government on the state of the telecommunications infrastructure and, in recent years, this has involved reporting on the state of IPv4 address availability and migration of networks to IPv6.

Thirdly, the permissibility of the extra-territorial use of national E.164 and E.212 numbers and/or the actual possibility to develop IoT solutions based on global resources appear to be key for IoT services to be economically viable. Still, it must be ensured that public interests like security, national sovereignty etc. are not compromised. BEREC considers that the use of existing numbering resources, the extraterritorial use of numbers and the use of ITU numbers, seems to be a reasonable approach, while the introduction of a European numbering scheme does not seem to carry any significant benefits which would justify the deployment costs of setting up such a solution.

With regard to IP addressing, the IPv4 addressing structure provides an insufficient number of publicly routable addresses to provide a distinct address to every Internet device or service (however, many connected devices may be located behind one IPv4 address), in particular in view of the expected growth of the market. Therefore migration to IPv6 appears to be advisable to enable the accessibility of connected devices from the public network.

3. IoT services in the context of the EU Telecommunications Framework

Stakeholders have raised several questions on the applicability of certain obligations of the EU Telecommunications Framework to IoT services. This concerns above all obligations deriving from qualifying a service as electronic communication service (ECS) (cf. section 3.1.), obligations deriving from the Roaming Regulation (cf. section 3.2.) as well as a possible right to switch connectivity provider (cf. section 3.3.). NRAs can contribute to identifying and eliminating and/or reducing legal uncertainty and possible barriers to the development of IoT services in this regard. In addition, the rules concerning network security, which also apply to M2M communications, are relevant in the context of the EU Telecommunications Framework (cf. section 3.4.).

3.1. Applicability of the electronic communications regulatory framework

The applicability of the current regulatory framework depends on whether the respective service in the IoT value chain is qualified as an ECS according to Art. 2 lit. c Framework Directive.⁵⁵

The definition of ECS and the applicable regulatory framework will be an important issue in the upcoming review process of the EU telecom rules. These issues will have an impact on a wide number of topics, e.g. M2M and Over-the-top (OTT) services.⁵⁶ In this light, assessing whether

⁵⁵ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.04.2002, p. 33, as amended by Directive 2009/140/EC, OJ L 337, 18.12.2009, p. 37, and Regulation 544/2009, OJ L 167, 29.6.2009, p. 12.

⁵⁶ The definition and scope of the so-called "OTTs" is currently a key issue in a separate BEREC working group.

a given service in the IoT value chain is an ECS will have repercussions on other subjects, and vice-versa. Hence, a consistent approach is of the essence.

If a service is considered an ECS, the full-fledged regulatory set of rules applies including the notification obligation⁵⁷ as well as telco-specific rules on consumer protection⁵⁸, data protection⁵⁹ and network security.⁶⁰ Hence, it needs to be assessed as a first step if – and if so, at which level – an ECS has been identified in the IoT value chain.

According to Art. 2 lit. c Framework Directive, an ECS is “a service normally provided for remuneration which consists **wholly or mainly** in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks”.

According to this definition, there are three basic criteria for the finding of an ECS:

- Firstly, that the service normally is provided for remuneration.
- Secondly, that the service consists wholly or mainly in the conveyance of signals on electronic communications networks.⁶¹
- Thirdly, that the service consists in the transmission of content (and not in the production of content).

The analysis of the interpretation of these criteria is focused on the first two, the third being a “negative” one, that excludes services providing content but does not indicate which services are qualified as ECS.

3.1.1. Remuneration

The criterion “normally provided for remuneration” mirrors Article 57 of the Treaty of the Functioning of the European Union (hereinafter: TFEU) that establishes that services subject to the Treaty are the ones normally provided for remuneration. Due to the similarity of concepts the ECJ case law issued within the scope of Article 57 TFEU is relevant.⁶² In this case law the concept remuneration has been interpreted by the ECJ in very broad terms and includes any benefit that constitutes consideration for the service. Connectivity services within the M2M value chain normally are provided for remuneration.

⁵⁷ According to Art. 3 para 2 Authorisation Directive 2002/20/EC, amended by Directive 2009/140/EC, the provision of an ECS is only subject to a general authorization. The undertaking concerned may be required to submit a notification but may not be required to obtain an explicit decision or any other administrative act by the national regulatory authority before exercising the rights stemming from the authorisation.

⁵⁸ Cf. above all Art. 20, 21, 22 Universal Service Directive 2002/22/EC as amended by Directive 2009/136/EC.

⁵⁹ Directive on privacy and electronic communication 2002/58/EC as amended by Directive 2009/136/EC. Cf. in more detail below 4.1.

⁶⁰ Cf. Art. 13a of Framework Directive (2002/21/EC as modified by 2009/140/EC). Cf. in more detail below 3.4.

⁶¹ ECJ, judgement of 7 November 2013, C-518/11, para. 38, 41 - *UPC Nederland*; judgement of 30 April 2014, C-475/12, para. 36 41- *UPC DTH*, which both concern broadcasting, namely the transmission of radio and television programmes.

⁶² See, for instance, C- 263/86 - *Belgium v. Humbel*, C-180/98 - *Pavlov* or C-206/98 - *Commission v. Belgium*.

3.1.2. Conveyance of signals

The second element can be sub-divided in a two-step test, namely (i) whether signals on electronic communications are conveyed, and (ii) whether the service consists wholly or mainly in this conveyance of signals.

In this regard, it is of no relevance for the finding of an ECS whether the transmission of signals is by means of an infrastructure that does not belong to the respective service provider.⁶³ All that matters in that regard is that the service provider is responsible vis-à-vis the end-users for transmission of the signal which ensures that they are supplied with the service to which they have subscribed.⁶⁴ Hence, not only connectivity service providers with their own network infrastructure but also resellers – whose service wholly or mainly consists in reselling connectivity and who call on the service of, and systems belonging to, third parties – can provide an ECS.

The fact that various transmission technologies are used for M2M communication (cf. 2.1 above) does not affect the assessment whether the respective service represents an ECS or not.⁶⁵

From the above, the following can be concluded with regard to services provided in the IoT value chain:

Services in the IoT value chain generally depend on a connectivity service as an input product but connectivity accounts for a relatively low proportion of the overall revenue opportunity in the IoT value chain.⁶⁶ Hence, in many cases it is decisive whether the respective service in the IoT value chain consists “wholly or mainly” in the conveyance of signals on electronic communication networks. This criterion leaves room for interpretation. Due to the variety of IoT services, this assessment may often only be possible on a case-by-case basis. This assessment may be made by an NRA, whose decision, however, may be subject to review by national courts and finally the ECJ.

It is helpful to assess the respective service (contract) in the value chain⁶⁷ in order to determine whether it can be qualified as an ECS.

Within the IoT value chain, the connectivity service provider who provides connectivity over a public network for remuneration⁶⁸ is generally a provider of an ECS.

⁶³ C. f. Cf. ECJ, judgement of 30 April 2014, C-475/12 – *UPC DTH*, para. 43, 44.

⁶⁴ Cf. ECJ, judgement of 30 April 2014, C-475/12 – *UPC DTH*, para. 43.

⁶⁵ As is apparent from Art. 2 lit. a Framework Directive – which defines the notion of electronic communication networks – and Art. 2 lit. c Framework Directive, the fact that the conveyance of signals on electronics communications networks is effected by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and television broadcasting or cable television networks, is not decisive for the purpose of the interpretation of ECS, cf. along these lines ECJ, judgement of 30 April 2014, C-475/12 – *UPC DTH*, para. 41 with explicit mentioning of cable and satellite infrastructure.

⁶⁶ „*From concept to delivery: the M2M market today*“, February 2014. GSMA Intelligence.

⁶⁷ Cf. figure 2 in the introduction as well as in Annex 1.

⁶⁸ A different assessment might be possible, in particular if the connectivity is sold in-house (i.e. vertically integrated companies or public institutions) and/or via private networks.

With regard to the IoT user (e.g. car manufacturer, electricity provider), the following categories might be helpful.⁶⁹

- Typically, an IoT user who includes connectivity as an input product into his products or services does not seem to provide an ECS when selling a connected device or “smart” service⁷⁰ (unless he wholly or mainly resells connectivity to his customers). In this case, the IoT user is similar to a producer and/or vendor of terminal equipment.
- Vice-versa, a reselling situation – and hence ECS – may be found at the level of the IoT user when the IoT user is contractually liable vis-à-vis the end-user for the provision of connectivity and this constitutes a whole or main part of what is sold.

However, since there are so many different types of packages including connectivity and since business models are just beginning to evolve, it has to be carefully assessed, also taking into account the spirit and purpose of the law, in which situations an IoT user may be qualified as a provider of an ECS.

To conclude, in those cases where market players are not regarded as providers of an ECS, they are not obliged under the respective national laws to notify their activities to NRAs of the countries where they are active. In those cases where these market players are providers of ECS, reference is made to BEREC’s general approach towards a possible relaxation of the notification obligation.⁷¹ To date, with regard to the notification obligation no special treatment of an ECS contained in the IoT value chain appears necessary.

Within the ongoing review and DSM process the aim of fostering effective competition in the IoT industry for the benefit of the society and citizens should be considered. When doing so, it should be assessed whether and, if so, to what extent the existing rules which were primarily construed for voice telephony do also fit to M2M communications or not. Moreover, the regulatory costs (i.e. time, manpower, costs) connected to the adherence to telecommunication rules should be taken into account. In addition, one should be aware that qualifying IoT users as ECS providers might lead to a rise in the number of notifiable market players. It should be carefully examined during the review whether this shall be the purpose of the regulatory framework. Finally, this should be balanced against possible benefits for end-users. In particular, protection stemming from such regulation might increase trust and, in turn, willingness to use IoT services.

At national level, stakeholders sought clarification from NRAs with regard to the applicable EU regulatory framework (e.g. notification regime) in the IoT value chain. This, in turn, mainly depends on the finding of an electronic communication service (ECS) according to Art. 2 lit. c Framework Directive.

Under the present regulatory framework, the connectivity service provider who provides connectivity over a public network for remuneration is generally the

⁶⁹ Please note that this guidance is not a statement of law and is without prejudice to the interpretation of the notion of ECS by the ECJ.

⁷⁰ This holds in particular true if the connectivity is a secondary or free element of the final product or service that could be considered as self-provision in order to provide an added value service, like, in the case of manufacturing cars, to monitor remotely the car.

⁷¹ See for example BoR (14) 50, BEREC views on the European Parliament first reading legislative resolution on the European Commission’s proposal for a Connected Continent Regulation; BoR (13) 142 BEREC views on the proposal for a Regulation “laying down measures to complete the European single market for electronic communications and to achieve a Connected Continent” on a proposed single EU notification and authorisation.

provider of an ECS in the IoT value chain; he is responsible vis-à-vis NRAs for the compliance with the obligations deriving from the EU regulatory framework. In contrast, the IoT user (e.g. car manufacturer, provider of energy including smart meter) typically does not seem to provide an ECS. According to such an approach, IoT users would not be subject to the rules of the EU regulatory framework. However, there would be a finding of an ECS if the IoT user wholly or mainly resells connectivity to the end-user. Overall, since there are so many different types of packages including connectivity and since business models are just beginning to evolve, it has to be carefully assessed by NRAs in which situations an IoT user may – or may not be – be qualified as a provider of an ECS.

Within the ongoing review and DSM process it should be assessed whether and, if so, to what extent the existing rules which were primarily construed for voice telephony do also fit to M2M communications or not. Also possible regulatory costs and/or the possible number of notifiable market players should be taken into account and be balanced against possible benefits for end-users.

3.2. Roaming

Depending on the particular business model, the underlying connectivity service linked to IoT services, which is incorporated into IoT services as an input product, can be provided by mobile public communications networks. In such a case, the connectivity can be provided via international roaming or via domestic networks. Furthermore, according to the business models being developed, roaming can function on a permanent or a transitory basis. Examples of this fact can be found in some of the business models set out in the introduction, such as connected cars, agriculture measuring devices or smart meters that are distributed worldwide, or devices as e-readers which may cross borders.

The key issues regarding the regulatory situation of IoT services when based on mobile connectivity involving international roaming are in particular

- whether these types of services are under the scope of the Roaming Regulation and, furthermore,
- whether the Roaming Regulation applies when the connectivity is provided based on permanent roaming.

This whole section deals with roaming for the case of mobile public communication networks (2G/3G/4G) for which roaming occurs at present.

In case new technologies such as low power wide area networks develop, they will also become subject to roaming services between different network operators of the same technology. Such agreements are already incorporated between e.g. Sigfox network operators or Lora network operators. This type of connectivity is not covered here, but may in time require attention in order to ensure that appropriate conditions are met for such roaming services.

3.2.1. General applicability of the Roaming Regulation

The purpose of the Regulation (EU) No 531/2013 of the European Parliament and of the Council of 13 June 2013 on roaming on public mobile communication networks within the

Union⁷² (Roaming III Regulation) as amended by Regulation (EU) No. 2120/2015 of 25 November 2015⁷³ (TSM Regulation) (hereinafter Roaming Regulation) as stated in Art. 1, is to introduce “*a common approach to ensuring that users of public mobile communications networks, when travelling within the Union, do not pay excessive prices for Union-wide roaming services in comparison with competitive national prices (....)*”.

Under the Roaming Regulation “*Union-wide roaming*” means, in the context of data roaming services, “*the use of a mobile device by a roaming customer (....) to use packet switched data communications, while in a Member State other than that in which the network of the domestic provider is located (...)*” (Art. 2 f). In addition, a “*regulated data roaming service*” is defined in the Regulation as a “*a roaming service enabling the use of a packet switched data communications by a roaming customer by means of his mobile device while it is connected to a visited network*” (Art. 2 m).

According to these definitions, the Roaming Regulation only applies to mobile connectivity-based applications or devices that are connected to a visited network, meaning a mobile communication network situated in a Member State other than that of the roaming customer’s domestic provider (definition provided by Art. 2 e of the Regulation).

At the wholesale level roaming services are provided on the basis of commercial agreements.

The Roaming Regulation, when applicable (cf. scenarios below), establishes two types of limits to the commercial terms that might be agreed:

- a) Price caps for regulated roaming services which cannot be exceeded by commercial agreements. The Regulation establishes maximum wholesale and retail charges for data, voice or SMS traffic on roaming.⁷⁴
- b) A general roaming access right, meaning that mobile network operators shall meet all reasonable requests for wholesale roaming access.⁷⁵ The guarantee of this right applies to every mobile operator notwithstanding the existence of any commercial agreement. However, this general right is not unlimited. Mobile network operators may refuse access (only) on the basis of objective criteria.⁷⁶

In a first step, it is analyzed whether the commercial relationships established between mobile operators to provide IoT services are subject to those two limits.

Regarding the general applicability of the Roaming Regulation to IoT services, neither Art. 1 of the Roaming Regulation dealing with its scope nor the definitions laid down in Art. 2 of the Roaming Regulation explicitly refer to IoT services. However, as set out previously, a connectivity service is always underlying an IoT service. When that connectivity service

⁷² Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union, OJ 2012, L 172/10; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:172:0010:0035:EN:PDF>

⁷³ Regulation (EU) No. 2120/2015 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ 2015, L 310/1.

⁷⁴ Art. 7, 8, 9, 10, 12, 13 of the Roaming III Regulation

⁷⁵ Art. 3, para. 1, of the Roaming III Regulation.

⁷⁶ Art. 3, para. 2, of the Roaming III Regulation.

consists of public mobile connectivity for a a roaming device, this service will fall within the scope of the roaming regulatory framework, regardless of the parties affected by the connectivity contractual obligations.

At present, it derives from Art. 15 (4) of the Roaming Regulation⁷⁷ underpinned by some specific references included in the BEREC guidelines on Roaming Regulation (BoR (16) 34)⁷⁸ that the European roaming regulatory framework applies in general to the mobile connectivity in IoT services.

Therefore the main regulatory measures regarding roaming are generally considered applicable to the mobile connectivity service underlying IoT services, implying that any IoT service provider/mobile operator benefits from the roaming access right as well as from the price caps. Mobile network operators on the other hand benefit from the right to refuse access requests on the basis of objective criteria (cf. above).

3.2.2. Permanent roaming in the context of the Roaming Regulation

A number of IoT services relying on mobile connectivity are provided on the basis of permanent roaming for different reasons:

- When the connected device is sold outside the country of production but uses a SIM with an IMSI of the country of production (e.g. cars, e-readers).
- In order to achieve better coverage (e.g. for smart meters).⁷⁹

Prior to its amendment in November 2015 by the TSM Regulation, the Roaming III Regulation was legally not clear with regard to permanent roaming in the IoT context, neither with regard to

- (i) The admissibility of permanent roaming as such nor with regard to
- (ii) The question whether the Roaming III Regulation applies to permanent roaming.

⁷⁷ Paragraphs 2 and 3 shall not apply to machine-to-machine devices that use mobile data communication", which means IoT devices that use mobile data communication are excluded from the application of the obligations related to price information and cut-off limits imposed to retail data roaming services. This permits the reverse conclusion that the remaining provisions under that Regulation are in general applicable to IoT services (*argumentum e contrario*).

⁷⁸ Paragraph 66 of the "BEREC Guidelines on Roaming Regulation (excluding articles 3, 4 and 5 on wholesale access and separate sale of services)" (BoR (16) 34) indicates that "Pursuant to Article 15(4) the transparency provisions do not apply to machine-to-machine devices that use mobile data communication"; and, in addition, the executive summary, no. 8 of the same Guidelines also refers to M2M communication ("Finally the BEREC guidelines cover various general issues such as charges for voicemail messages, charges in currencies other than the Euro, scope of regulated roaming call, scope of regulated data roaming, inadvertent roaming, value added services, machine-to-machine communication (M2M) and geographical scope of the Regulation"). Guideline no. 8 of the "BEREC Guidelines on Roaming Regulation (Articles 4 and 5 on separate sale of roaming services)" establishes that "There are no restrictions in the regulation, which exclude M2M services from the regulation, therefore decoupling does apply to these services based on public communications network as defined in Article 2(d) of the Framework Directive".

⁷⁹ In principle, this goal can also be achieved via national roaming. However, there is no regulated access right for national roaming and it is often not used in practice, while there is an wholesale access right for international roaming. The latter solution implies that the device is connected via the best network at prices below the caps. For the party requesting access, this saves transaction costs and the need to negotiate access on the basis of national roaming. Overall, the need to achieve best possible coverage leads to arbitrage. In this case, permanent roaming in the context of M2M is very similar to the remaining scenario or to any situation of parallel import/trade.

The Roaming III Regulation made no explicit reference to permanent roaming (no statement to allow or exclude it). In this regard, it only refers to the terminology “*when travelling within the Union*” (cf. Art. 1 (1) of the Roaming III Regulation⁸⁰) as well as the definition of “*Union-wide roaming*” (cf. above). Hence, the question whether permanent roaming is within the scope of the Roaming Regulation, depended mainly on an interpretation of the notions “*travelling*” and “*mobile device*”.

The TSM Regulation - which in principle will be applicable as of 30 April 2016 - has amended the Roaming III Regulation. Among others, the revised text explicitly mentions permanent roaming. The “reference offer [which roaming providers have to publish] may include conditions to prevent permanent roaming or anomalous or abusive use of wholesale roaming access for purposes other than the provision of regulated roaming services to roaming providers’ customers while the latter are periodically travelling within the Union” (cf. replaced Art. 3 (6) of the Roaming Regulation). The reference offer concerning wholesale roaming access may therefore include general conditions denying/prohibiting permanent roaming schemes. Furthermore, roaming providers may apply a “‘fair use policy’ to the consumption of the regulated retail roaming services provided at the applicable domestic retail price level, in order to prevent abusive or anomalous usage of regulated retail roaming services by roaming customers, such as use of such services by roaming customers in another Member State than that of their domestic provider for purposes other than periodic travel” (cf. new Art. 6b of the Roaming Regulation).⁸¹

From these provisions, the following conclusions can be drawn:

- Firstly, a distinction between, on the one hand, roaming during “periodic travel” and, on the other hand, “permanent roaming” is made.
- Secondly, according to the amendments to the Roaming III Regulation for Art. 3, network operators may include in the reference offers conditions to prevent permanent roaming or anomalous or abusive use of wholesale roaming access for purposes other than provision of regulated roaming services and therefore refuse access for IoT services based on permanent roaming schemes. In other words, it implies that the wholesale access obligation for such services does not apply for permanent roaming scenarios, but this does not prevent that operators may offer permanent roaming services on a commercial basis.

In general⁸², it is noted that the provisions do not differentiate between person-to-person communications and M2M communications (i.e. they do not foresee any special treatment for M2M communications).

In light of the currently applicable roaming regulatory framework, BEREC concludes that – especially in the light of the fast developing nature and diversity/solutions of IoT services/business models as well as different permanent roaming scenarios – that there might

⁸⁰ According to Art. 1 of the Roaming III Regulation, “[t]his Regulation introduces a common approach to ensuring that users of public mobile communications networks, when travelling within the Union, do not pay excessive prices for Union-wide roaming services in comparison with competitive national prices, when making calls and receiving calls, when sending and receiving SMS messages and when using packet switched data communication services, (...)”.

⁸¹ Finally, the Commission shall in their review of the wholesale roaming market “take into account the need to prevent permanent roaming or anomalous or abusive use of wholesale roaming access for purposes other than the provision of regulated roaming services to roaming providers’ customers while the latter are periodically travelling within the Union” (cf. new Art 19 of the Roaming Regulation).

⁸² Except for Art. 15 para 4 (exemptions for M2M as regards transparency and safeguard mechanisms for retail data roaming services).

be IoT services using permanent roaming where the scope and application of the Roaming Regulation is indeed questionable. Against this background a case-by-case evaluation and legal interpretation should be envisaged taking into consideration the specific (technical) details and parameters of the respective IoT service in light of the purpose of the Roaming Regulation. When applying such case-by-case analysis, the following typical IoT roaming scenarios can be distinguished:

- Scenario 1:** The connected device is travelling periodically (e.g. a car used for a leisure trip).
- Scenario 2:** The connected device is used most of the time on the basis of permanent roaming, but the object is moving either within one country or across borders (e.g. a car which is sold abroad).
- Scenario 3:** The connected device (e.g. smart meter, sensors) is used on the basis of permanent roaming but is not travelling at all, often with a long period of usage. Furthermore it is questionable whether in this case the connected device can be called a mobile device at all, since it is not used in a mobile fashion.

In scenario 1, there is no permanent roaming and the Roaming Regulation is applicable also to IoT devices. In scenario 3, BEREC considers that IoT connected devices used on permanent roaming and not travelling at all should not be considered in the scope of the Roaming Regulation (i.e. the Roaming Regulation should not apply to them, while agreements concerning permanent roaming could still be commercially negotiated). In scenario 2, it is less clear whether the Roaming Regulation applies or not. However, it lies in the nature of a case-by-case approach that it does not provide safe harbours.

Therefore, in order to ensure legal certainty to all players involved, further clarification in the Roaming Regulation and/or in a Commission Communication as to permanent roaming in the IoT context might be helpful.

3.2.3. Current functioning of the market

Irrespective of the question of the applicability of the Roaming Regulation to permanent roaming in the IoT context, BEREC notes the following on the basis of the available data, including the BEREC Report on the wholesale roaming market BoR (16) 33:

- The majority of operators have for the time being not implemented any measures to discourage permanent roaming.⁸³
- The majority of operators do not apply specific prices or conditions for M2M traffic.⁸⁴
- Moreover, it is likely that IoT roaming charges are below the regulated price caps.⁸⁵

⁸³ Cf. BEREC Report on the wholesale roaming market, BoR (16) 33. However, around 20 percent of the responding MNOs have some kind of mechanism in their wholesale roaming agreement to discourage permanent roaming.

⁸⁴Information gathered for the BEREC Report on the wholesale roaming market (BoR (16) 33) shows that the majority of operators do not apply specific prices or conditions for M2M traffic while a few operators have special conditions and rates for M2M traffic. If commercially negotiated wholesale roaming tariffs are applied for M2M traffic, this M2M traffic has to be identified. According to GSMA, connectivity providers use specific MNC or MNC ranges for M2M traffic whereby M2M traffic can be identified among them. GSMA has referred to a specific Annex on Transparency where this is laid down which, however, has not been disclosed to BEREC.

⁸⁵ This is inter alia supported by the fact that average EEA wholesale data prices were below the price cap in Q2 and Q4/2014, cf. International Roaming BEREC Benchmark Data Report April-September 2014, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4922-international-roaming-berec-benchmark-data-report-april-8211-september-2014.

However, it is noted that 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 gains a competitive advantage over national operators being able to exploit the coverage of all existing networks that visited networks would not be able to gain 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.

3.2.4. Use of international/global E.212

Currently, some operators use MNCs under the shared MCC 901 to offer transnational services by way of permanent roaming. The use of this specific code which is not linked to any country permits to better identify and limit the service in the context of roaming access agreements. The visited network is able to better estimate the number of visited SIM permanently roaming on its network and their consumption.

3.2.5. Concerns for the future

Even if there seem to be no explicit access and pricing issues related to M2M connectivity with regard to the Roaming Regulation and apart from a need for further clarification with regard to permanent roaming in the IoT context, BEREC still sees some concerns in the future for the development of the part of the IoT market relying on cellular network connectivity and numbers as identifiers:

Firstly, the question whether the Roaming Regulation – and hence the access right – does apply might be of relevance at a later point in time. It cannot yet be foreseen how the markets will develop: Once the principle of “*Roam like at home*” (RLAH) is applied and roaming charges are significantly decreased or abolished, after a revision of the wholesale regulation the MNOs might adopt measures to prevent permanent roaming. Hence, there is the risk that access issues will occur in the future. However, any conclusion regarding this matter would be premature and will need to be revised in light of the Commission’s planned wholesale roaming market review.

Secondly, any possible further revision and/or clarification of the Roaming Regulation should explicitly take into account the specific IoT context. The rationale for roaming underlying person-to-person communication relates to consumer protection arguments which do not apply to M2M communication underlying an IoT service.⁸⁶ A number of IoT services are currently provided on the basis of permanent roaming.⁸⁷ Considering that IoT is a global market, which goes beyond European borders, BEREC notes that permanent roaming – while

⁸⁶ Cf. Art 1 (1) of the Roaming Regulation: “*This Regulation introduces a common approach to ensuring that users of public mobile communications networks, when travelling within the Union, do not pay excessive prices for Union-wide roaming services in comparison with competitive national prices, when making calls and receiving calls, when sending and receiving SMS messages and when using packet switched data communication services, thereby contributing to the smooth functioning of the internal market while achieving a high level of consumer protection, fostering competition and transparency in the market and offering both incentives for innovation and consumer choice.*” and Consideration 20 of the Roaming Regulation III: “*A common, harmonised approach should be employed for ensuring that users of terrestrial public mobile communication networks when travelling within the Union do not pay excessive prices for Union-wide roaming services, thereby enhancing competition concerning roaming services between roaming providers, achieving a high level of consumer protection and preserving both incentives for innovation and consumer choice. [...]*”.

⁸⁷ For the provision of many IoT services, the absence of permanent roaming possibilities would be a significant hassle, making impossible to use roaming aggregators and significantly increasing transaction costs.

not being justifiable by consumer protection – might facilitate the development of such a market. Against this background, the right of operators to refuse permanent roaming or to provide it on the basis of economically unattractive conditions should be followed carefully, taking into account the particularities of IoT communications. It might also be worthwhile to consider an access right for IoT permanent roaming.

In the context of the review of the wholesale roaming market to be finalized by the Commission in mid-2016, it might be worthwhile for the legislator to address the issues presented above in the interest of establishing increased legal certainty.

The IoT sector has evolved to be a transnational market of services where a significant part of the devices supporting those services are conceived for global mobility, not only under the basis of temporary mobility but to be marketed globally on a permanent roaming basis. In this context, the possibility and the economic terms under which such connections can be provided are fundamental for the development of the sector. Permanent roaming appears to be a key factor for the success of certain IoT business models being used.

Whether the Roaming Regulation is applicable to permanent roaming in the IoT context, depends mainly on the elements “periodically travelling in the Union” and “mobile device”. BEREC considers that IoT connected devices used on permanent roaming and not travelling at all should not be considered in the scope of the Roaming Regulation (i.e. the Roaming Regulation should not apply to them, while agreements concerning permanent roaming could still be commercially negotiated). In particular, Regulation No. 2120/2015 concerning amendments to the Roaming III Regulation explicitly mentions permanent roaming; the new provisions suggest that operators may include conditions in the wholesale reference offers to prevent permanent roaming and therefore even refuse access under regulated conditions for such requests. However, it is noted that these provisions do not differentiate between person-to-person communication and M2M communication (i.e. they do not foresee any special treatment for M2M communications). Against this background a case-by-case evaluation and legal interpretation should be envisaged taking into consideration the specific (technical) details and parameters of the respective IoT service in light of the purpose of the Roaming Regulation. However, any case-by-case approach carries legal uncertainty. Therefore, further clarification in the Roaming Regulation and/or in a Commission Communication with regard to permanent roaming in the IoT context might be helpful.

Debates concerning obligation to grant or a right to refuse access might occur in the future if RLAH applies. Any possible further revision and/or clarification of the Roaming Regulation should take into account the specific IoT context. Considering that IoT services might be a global market which goes beyond European borders, BEREC notes that permanent roaming is currently used for the provision of a number of IoT services and might facilitate the creation of such a market. Apart from that, the rationale for permanent roaming differs in the case of, on the one hand, person-to-person communication and, on the other hand, M2M communication. In the context of the review of the wholesale roaming market to be finalized by the Commission in mid-2016, it might be worthwhile to consider an access right for IoT permanent roaming.

3.3. Switching / lock-in issue

The potential solutions to the switching/lock-in problem which are presented in this section refer to IoT services which are provided on the basis of connectivity (via SIM) over public mobile networks only.

Even if number portability might not be an issue for IoT users and/or end-users who do not need to communicate, or even be aware of a possible phone number associated to their IoT devices, switching the connectivity service provider can be identified as an issue regarding the development of IoT services and the functioning of the market.

At present, switching connectivity service provider requires a hardware modification of the IoT device (such as the replacement of the connectivity module or, when possible, the replacement of the SIM card), but the cost of dispatching technicians for each IoT device might outweigh the expected gains of the switch, especially for extensive deployments of equipment. As a result, it could negatively impact the incentives for a IoT user to switch to another connectivity service provider.

If switching costs are important for a competitive IoT environment, IoT users should carefully evaluate pro and cons of the offered connectivity technologies, taking into account the drawbacks related to possible lock-in due to proprietary solutions or spectrum licences (such as Low Power Wide Area Network, wired data network) because switching connectivity service provider may in many cases require switching the connectivity technology and replacing the related hardware.

From this point of view, cellular networks based on 3GPP standards (GSM, UMTS and LTE) may be able to meet IoT users' expectations as two main solutions have been investigated by the industry to solve this issue:

- MNC assignment to IoT users such as utility companies (gas, water, electricity), car makers (see also 2.2.1.2. above);
- OTA provisioning of SIM.

3.3.1. MNC assignment for IoT users

On the one hand, if IoT users become entitled to be assignees of MNCs, they could contract with connectivity service providers, like any MVNO with its own MNC, for the deployment of their services. IoT users would become Private Virtual Networks Operators (PVNO). Even if one assumed that assignment rules were modified by ITU-T according to a CEPT contribution proposal in order to allow national numbering plans to make available such assignments (which does not seem to happen quickly), this solution still raises questions regarding the technical and economic conditions required to operate its own MNC and effectively switch from one connectivity service provider to another:

- What infrastructure should the IoT user own by himself? If the IoT user needs to rely on a technical enabler he mandates to operate its MNC on a shared mobile network infrastructure, he will still have a lock-in problem with his technical enabler.
- Would the IoT user need to become an ECS?
- What is the switching process? Has it already been tested under real conditions? An effective transition from a service provider to another would require that all contracts and routing are changed during a specific period of time.

- What are the operational costs of switching connectivity service provider and the related risks on the security and the availability of the wireless connectivity provided to IoT devices as the IoT user might be responsible for operating highly sensitive core network equipment ?
- Will MNCs become scarcer if assigned to IoT users in greater numbers? This indeed seems to be a relevant problem, since in most cases only 100 IMSI-blocks (MNCs) can be assigned to each country or, more precisely, to each mobile country code (MCC). Even if it is possible for a country to apply for a new MCC at ITU, these resources are not unlimited⁸⁸.

3.3.2. OTA provisioning

The GSMA⁸⁹ has specified a mechanism for the remote provisioning and management of embedded SIM, allowing OTA provisioning of an initial connectivity service provider subscription, and the subsequent change of subscription from one connectivity service provider to another. This mechanism has been designed to answer IoT needs where SIM may not easily be changed manually.

For the moment, it seems that this mechanism has only been partially implemented for certain end-users (and mainly within closed co-operations among MNOs). At present, remotely programming the SIM appears to be technically feasible, although so far there seems to be no evidence of a specific procedure that has been agreed between MNOs

- which would allow for switching a large number of devices at the same time or within a short time period, because not all devices might be connected at the same time; and
- which would enable an MNO to re-programme a SIM of a customer of another MNO (in case of a customer's wish to switch to another MNO) and which in addition provides for a non-discriminatory, open and transparent access as well as a solution for security issues.

This partial implementation of the GSMA mechanism is not fully effective for lowering switching costs. Connectivity service providers may be reluctant to go further as they fear losing control over the SIM in the event of OTA provisioning of a new profile.

However, OTA provisioning seems to be promising for effective provider change and not to be bound by the problems previously identified for the other switching solution, the assignment of MNCs to IoT users. OTA specification is quite recent (having been published by the GSMA in October 2014) and it is reasonable to expect that further implementation, including of switching features, may take place in the coming months. A technical specification by ETSI is expected for Q2/2016.

In any case, if OTA provisioning does not enable switching between connectivity service providers within a reasonable time period, it might be considered to adopt a statutory obligation to introduce OTA provisioning at a certain point in time or at least regulatory mechanisms or incentives to foster OTA provisioning. Such an obligation could prescribe that the switching process via OTA has to occur in a synchronized manner (so that all connected devices of a M2M customer are switched to the new connectivity provider at the same time and/or within a

⁸⁸ See Consultation report, p. This concern has been raised by many stakeholders in their answers to the public consultation launched by BEREC.

⁸⁹ <http://www.gsma.com/connectedliving/embedded-sim/>

short time frame) and it might also encourage the sector to find an agreement on a global open standard for switching operator through OTA provisioning.

3.3.3. Evolution of the regulatory framework with regard to switching

As explained above, there is no mature solution to mitigate the lock-in problem related to switching between connectivity service providers of M2M services yet. Both solutions have advantages and drawbacks as explained above. BEREC expects that at least one solution might be able to address this issue efficiently within the next few years and, in particular, that OTA provisioning of SIM might be ready for the market in the near future. 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. Overall, BEREC sees the need for flexible solutions at national level.

Depending on the switching solution (e.g. assignment of own MNC, OTA provisioning), without any regulatory incentive the biggest IoT users, such as the automotive industry, may have sufficient buying leverage on connectivity service providers to negotiate their business models. There is a possibility that smaller IoT users would not have access to efficient switching mechanisms.

An evolution of Art. 30 of the Universal Service Directive entitled “Facilitating change of provider” might be appropriate to grant IoT users the right to switch remotely between connectivity service providers, at least with regard to those connectivity service providers whose networks are interoperable with IoT user terminal equipment.

BEREC believes that - in the IoT context - the number portability obligation might not be appropriate in case the E.164 number of the connected device is not known by the IoT user (and/or by the IoT end-user), which usually happens when the device is not designed to send or receive any voice calls or SMS.⁹⁰ Also, it could create unnecessary barriers for new market entries due to costs for participating in the porting process. Furthermore, given that numbers are used extra-territorially in many instances, one would need to create a worldwide number portability process. Such efforts are not proportionate in view of none or very limited portability use cases.⁹¹

If a customer intends to change connectivity service provider, it is currently necessary that the SIM is replaced physically. The costs of doing so might prevent switching the connectivity service provider, thus generating the “lock-in” effect.

Both MNC assignment to IoT users as well as over-the-air provisioning of SIM could mitigate the lock-in issue of the IoT value chain by dropping the cost of dispatching technician to upgrade IoT devices. 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

⁹⁰ For some stakeholder views cf. Consultation Report, answer to Question 3.

⁹¹ A use case for calling numbers used for IoT services might be a wake-up SMS for the machines. However, this might be an old use case.

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.

A new approach might be appropriate, both in view of facilitating a provider switch as well as of the number portability obligation, taking into account 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.

3.4. Network security

With the development and proliferation of IoT services, it becomes increasingly important to ensure secure and reliable communication among connected IoT devices. Different services will have different requirements for security and resilience. Many consumer services will not require a highly resilient network connection since temporary service interruptions will not significantly impact the integrity of the service provided. On the other hand, services that control important processes will require high levels of security and service availability. Such services could also be deployed over private networks, which do not fall under current legislation.

Traditional security approaches used in electronic communications may not be sufficient to address low cost devices used by many IoT services. When previously unconnected devices are turned into connected devices, the security of the devices (through passwords, encryption and software updates) seems to be neglected in many instances. Due to limited resources in terms of energy and computing power, such IoT devices may be vulnerable to cyber-attacks. An increasing number of less secure connected devices, which are exposed to a wider audience, can become a potential privacy and information security target that can have negative effects on consumer perception of security and acceptance of IoT services. In that regard, secure and lightweight protocols that can be used in such low resource environments will be required.

In order to mitigate network connectivity issues, Art. 13a of the Framework Directive (2002/21/EC as modified by 2009/140/EC) has already imposed certain security and integrity obligations on providers of publicly available networks and services, as follows:

- Networks and service providers must take appropriate measures to appropriately manage the risks posed to security of networks and services, in particular these measures shall ensure a level of security appropriate to the risk presented and to prevent and minimize the impact of security incidents on users and interconnected networks.
- Network providers must take all appropriate steps to guarantee the integrity of their networks and thus ensure continuity of supply of services provided over those networks.
- Networks and service providers must notify the competent NRA of a breach of security or loss of integrity which have a significant impact on the operation of networks or services.

NRAs which provided answers to BEREC confirmed that these obligations are in general implemented in their national legislation. The majority of NRAs also have powers to enforce

these obligations.⁹² National legislation of a Member State does not specifically address IoT services. All obligations apply also to IoT services provided that they are considered ECS or to the ECS which is underlying any IoT service.

Moreover, the Commission has set forth a draft directive in order to ensure a high common level of network and information security (NIS) across the EU.⁹³ Taking into account the increasing digitalization of the economy, the original draft directive intended to oblige in particular operators of critical infrastructure (such as energy, transport, banking, stock exchange, healthcare) and key Internet enablers (e-commerce platforms, social networks, etc.) to undertake a NIS risk assessment, implement corresponding measures and to report incidents with a significant impact to the competent authorities. To date, a final compromise text in view to agreement has been reached,⁹⁴ which will need to be adopted by the Council and Parliament in order to enter into force.

National legislation of a Member State (based on Art. 13a Framework Directive) concerning network security does not specifically address IoT services. All obligations apply also to IoT services provided that they are considered ECS or to the ECS which is underlying any IoT service.

However, traditional security approaches used in electronic communications may not be sufficient to address low cost devices used by many IoT services. Due to limited resources in terms of energy and computing power, such IoT devices may be vulnerable to cyber-attacks.

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.

4. Areas where NRAs can have a coordinating function

With regard to areas like privacy, data security and standardisation NRAs competences vary. Some have only limited or no competences at all.

However, NRAs could coordinate with the respective competent authorities, and with other stakeholders in industry, in order to create awareness and foster an innovation-friendly, as well as consumer-friendly, environment.

⁹² Denmark, Italy and Spain have ministries which are directly responsible for their enforcement.

⁹³ Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7.2.2013, COM(2013) 48 final. For an overview over the discussions during the legislative process, cf. <http://data.consilium.europa.eu/doc/document/ST-5257-2015-INIT/en/pdf>.

⁹⁴ Cf. Final compromise text in view of agreement, Interinstitutional file 2013/0027 (COD), 15229/2/15 REV 2, 18 December 2015. The obligations shall now apply to operators of essential services and digital service providers. For an overview of the legislative process, cf. <http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52013PC0048>.

4.1. Privacy

One major issue to consider with regard to the IoT is the protection of privacy and personal data. "Personal data" is defined in Art. 2 of the Privacy Directive (95/46/EC): "*'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". Such private data may be collected in a number of services that are mentioned in Fig. 1 such as smart meters (which transmit data about consumption patterns), health applications (which transmit data about health conditions) etc. The fact that the data is transmitted via M2M communication does not change its qualification as personal data.⁹⁵

The more connected devices there are, the greater amount of personal data will be processed (e.g. collected, stored, digitally analysed, shared) even by an unpredictable and non-controllable amount of people or organisations (e.g. producer of the device, platform administrators, technicians, provider of telecommunication services) and made available via the Internet. Whether it is consumer-driven processing of personal data or business-driven big data processing, the more IoT services and connected devices consumers and businesses are using, the greater the amount of information that needs to be managed and protected. In certain cases, the data holder may not even be aware that his data are collected.⁹⁶ Also, he might lose control over the dissemination of his data.⁹⁷ With such amount of personal data available, it would in principle also be possible to pool the information and to obtain a "profile" of a given person.⁹⁸ If this information is not protected, it can give rise to infringement of privacy.

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.⁹⁹

There seems to be a general understanding among stakeholders involved in the development and implementation of IoT services¹⁰⁰, that the respect and protection of end-users' privacy is a critical success factor for the realisation of the prospects and growth of these services. If users do not trust that their data is being handled appropriately there is a risk that they might restrict or completely opt out of its use and sharing, which could impede the successful development of IoT.

⁹⁵ Cf. similarly Opinion 8/2014 on the on Recent Developments on the Internet of Things, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (in the following: "Art. 29 WG Opinion"), cf. chapter 3.2: "*In the context of the IoT, it is often the case that an individual can be identified based on data that originates from "things". Indeed, such data may allow discerning the life pattern of a specific individual or family [...]*".

⁹⁶ Art. 29 WG Opinion, cf. chapter 2.2.

⁹⁷ Art. 29 WG Opinion, cf. chapter 2.1.

⁹⁸ Art. 29 WG Opinion, cf. chapter 2.4.

⁹⁹ European Parliament, Big Data and smart devices and their impact on privacy, September 2015, [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU\(2015\)536455_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf).

¹⁰⁰ Sources: Ofcom consultation; Telenor Connexion; Gartner; Art 29.

With regard to personal data collected and shared in the context of IoT services, two different sets of rules may apply in EU Member States:

- The general relevant legal framework in the EU to assess privacy and data protection issues is composed of Directive 95/46/EC (Privacy Directive), which is currently under review¹⁰¹;
- The specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC (ePrivacy Directive) applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the Community (cf. Art. 3 ePrivacy Directive).

These directives are transposed in national laws of the Member States aiming at protecting the privacy and integrity of end-users' data.

The jurisdiction and legal competence to enforce compliance with these provisions has been implemented in different ways among Member States. While the general rules of the Privacy Directive falls under the jurisdiction of the national data protection authorities, for the majority of NRAs the legal competence to enforce the provisions of the ePrivacy Directive is shared with the national data protection authorities or national ministries (generally following different related laws transposing the ePrivacy directive into national law).¹⁰²

In contrast to the Privacy Directive (or rather the respective national law) the rules of the ePrivacy Directive are not only applicable to personal data of individuals, but provide for protection of the legitimate interests of subscribers who are legal persons, cf. Art. 1 (2).¹⁰³ The rules applies at least to the market player in the IoT value chain (cf. Fig. 2 and Annex 1) who provides the ECS underlying the IoT service in public communication networks, i.e. the connectivity service provider.

With regard to all other market players processing personal data, the Privacy Directive (or rather the respective national law) is applicable. In an opinion from September 2014¹⁰⁴, the Art. 29 WG tries to identify the role of the different stakeholders involved in the IoT value chain (such as device makers, IoT platform controllers) and to qualify their legal status as data controllers, and thus the national law applicable to the processing which they implement, as well as their respective responsibilities.

In the context of the provision of services in the IoT, all objects that are used to collect and further process the individual's data qualify as "equipment" in the meaning of Art. 4 (1) c)

¹⁰¹ There is an ongoing review of the Privacy Directive (95/46/EC) and a new regulation has been proposed by the EC (cf. <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011>). Cf. for more information: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

¹⁰² This conclusion is based on responses to a questionnaire carried by BEREC during 2015. In total 22 NRA responded to the three questions (1) *Does your national law place (based on EU law) any obligations on providers of electronic communication services and networks with regard to privacy?*; (2) *Does your NRA have any powers to enforce these obligations? If not, which authority is responsible for this?*; and (3) *Is M2M/IoT addressed in any way in these rules?*

¹⁰³ Eg. the rules on security (Art. 4) and confidentiality of the communications (Art 5) as well as the rules on traffic and location data (Art 6 and 9).

¹⁰⁴ Art. 29 WG Opinion, cf. chapter 3.3, chapter 6.2.

Privacy Directive¹⁰⁵ which is one possible requirement for the applicability of the Privacy Directive.¹⁰⁶

The provisions in the ePrivacy Directive particularise and complement the Privacy Directive (cf. Art. 1 (2) ePrivacy Directive). Overall, the following rules contained in the two Directives are of particular interest in the IoT context:

- Purpose limitation¹⁰⁷;
- Information about data processing¹⁰⁸;
- Consent to data processing¹⁰⁹;
- Security measures¹¹⁰;
- Notification obligation of the competent national authority in case of a personal data breach¹¹¹;
- Storing of information in terminal equipment¹¹²;
- Processing of traffic and location data.¹¹³

There are no specific rules in these two directives with regard to IoT services as such, or to M2M communication. Until now, BEREC has not identified a need to deviate from the basic principles of data protection law in the IoT context, i.e. no need for a special treatment of IoT services has yet been considered. However, with regard to certain IoT services it might be worthwhile to consider rules which are more adapted to the IoT environment. For example the methods for giving information, offering a right to refuse or requesting consent could be evaluated in order to make them as user-friendly as possible.¹¹⁴ In this light, there appears to be a need for a careful evolution where appropriate, but not an entire overhaul of the applicable data protection laws with regard to the IoT.

A step in the right direction to modernize the data protection legal regime might be the Council's General Approach of 15 June 2015¹¹⁵ on the future General Data Protection Regulation (GDPR) which aims at strengthening individual rights of citizens and ensuring a high standard

¹⁰⁵ Art. 29 WG Opinion, cf. chapter 3.1. This qualification obviously applies to the devices themselves (step-counters, sleep trackers, "connected" home devices like thermostats, smoke alarms, connected glasses or watches, etc.). It also applies to the users' terminal devices (e.g. smartphones or tablets).

¹⁰⁶ Art. 4 (1) Privacy Directive defines its scope of application, which inter alia is the case when the processing is personal data is carried out in the context of the activities of an establishment of the controller on the territory of the Member State (Art 4 (1) a) Privacy Directive) or when the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community (Art 4 (1) a) Privacy Directive).

¹⁰⁷ Art 6 (1) b) Privacy Directive which states that data can only be collected for specified, explicit and legitimate purposes.

¹⁰⁸ Art. 10, 11 Privacy Directive.

¹⁰⁹ Art 7 a) Privacy Directive.

¹¹⁰ Art. 17 Privacy Directive; Art. 4 (1), (2) ePrivacy Directive.

¹¹¹ Art. 4 (3) ePrivacy Directive.

¹¹² Art. 5 (3) ePrivacy Directive.

¹¹³ Art. 6, Art. 9 ePrivacy Directive.

¹¹⁴ Cf. Art. 29 WG Opinion, cf. chapter 6.1 (p. 22).

¹¹⁵ Council of the EU, Press release 450/15 of 15/06/2015, cf. <http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/>; European Commission, MEMO/15/5170. Full text version: Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach" of 11 June 2015, 9565/15, Interinstitutional File: 2012/0011 (COD).

of protection adapted to the digital era. The reform foresees inter alia easier access to data, a right to data portability which shall make it easier to transfer personal data between service providers, more detailed information and more transparency (e.g. informing about data processing and the privacy policy in clear and plain language), a right to erasure of personal data and “to be forgotten” as well as limits to the use of “profiling”. After a political agreement was reached in the trilogue between the European Parliament, the Council and the European Commission in the end of 2015, it is expected that the new rules will be formally adopted by the Parliament and the Council at the beginning of 2016.

In the same line, there are examples already today of how industry is working on solutions on how to comply with legal obligations and ensuring users’ trust within the IoT context:

- Building privacy concepts into devices and services from the beginning. This so-called “privacy by design” approach requires an early and detailed consideration of a full range of privacy issues and how they relate to and interact with other components of the IoT ecosystem, such as network security, resilience and user interface design.
- Devising simpler terms and conditions for the collection and sharing of data, including the means to obtain informed consent from users via a range of innovative approaches.
- Related to simpler terms and conditions, many respondents supported the development of a common framework to simplify and categorise different levels of data sharing.¹¹⁶

Personal data may be collected by a number of connected devices. The fact that the data is transmitted and shared via M2M communication does not change its qualification as personal data.

BEREC understands the need to strike a balance between the need for 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.

However, BEREC believes that the respect and protection of end-users’ privacy is a critical success factor for the realisation of the prospects and growth of IoT services. If users do not trust that their data is being handled appropriately there is a risk that they might restrict or completely opt out of its use and sharing, which could impede the successful development of IoT.

While the general rules of the Privacy Directive (Directive 95/46/EC) are not sector-specific and apply in general, the rules of the ePrivacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC) apply to the processing of data from both individuals and legal persons in connection with the provision of publicly available electronic communication services in public communication networks in the Community.

There are no specific rules in these two directives with regard to IoT services as such. As to now, BEREC has not identified a need to deviate from the basic principles of data protection law in the IoT context, i.e. no need for a special treatment of IoT services. However, with regard to certain IoT services it might be worthwhile to consider rules which are adapted to the IoT environment. For example, rules on information and consent should be made as user-friendly as possible. A step in the right direction might be the Council’s General Approach of 15 June 2015 on the future

¹¹⁶ Sources: Ofcom (page 14).

General Data Protection Regulation which is expected to lead to a formal adoption of the new rules at the beginning of 2016. Moreover, BEREC acknowledges that the challenges raised by the evolution of IoT applications, especially in health related fields or similarly sensitive fields, require protection for sensitive data against inappropriate use. These issues are not new, but they become more complicated by 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 this Report.

4.2. Standardisation

IoT devices need common, interoperable technical standards if regional or global markets are to yield significant economies of scale. Standardisation can intervene at different levels, such as the application¹¹⁷ and connectivity layers. All along the service chain, a balance shall be struck between openness, interoperability, easiness, innovation and investment.

The potential trade-off between incentivising innovation by allowing proprietary solutions to be developed in a competitive process and increasing interoperability with the help of standardization processes is well-known.

In general, when a new application is introduced into the market, particularly if this application is as innovative as IoT services, partnerships may have an important role as they help the service to spread out and to get regular improvements, thus fostering investments. Interviews conducted by BEREC in 2014 showed that many IoT applications were developed in a vertical way, with specialised and proprietary solutions, often created by partnerships of connectivity service providers, IoT users and IoT service providers (e.g. Global M2M Association, M2M World Alliance, Bridge M2M Alliance).

However, again according to these interviews, the proprietary solutions developed by the aforementioned partnerships and alliances often appear incompatible with each other. This situation may create switching barriers commonly referred to as the “lock-in” problem: the IoT user becomes dependent on a connectivity service provider (or an IoT service provider which is member of a specific alliance) for products and services, and he is unable to use another provider without substantial switching costs, due to the need to change apparatus, remote devices, or to the impossibility to port his data to a new service provider etc.

Where such co-operation with regard to proprietary solutions violates competition rules (such as the prohibition of anti-competitive agreements and/or the abuse of a dominant position laid down in Art. 101 and 102 of the Treaty on the Functioning of the European Union and corresponding national laws) competition authorities would be competent to take appropriate measures. Otherwise, there is little scope for NRAs to intervene.

¹¹⁷ See for instance, Zigbee Alliance, ZigBee Alliance and Thread Group Collaborate to Aid Development of Connected Home Products, zigbee.org, 2 April 2015.

Still, the ease of switching between connectivity service providers as well as IoT service providers is important in order to create a competitive environment for IoT services.

For this reason, some stakeholders highlighted the necessity of standards to abolish switching barriers, solve the lock-in problem and help the future development of IoT services: in fact, the presence of standards could reduce the cost in realising IoT services because research and development costs may be shared. For instance, they can level up security and limit the risk of unsecure proprietary solutions reaching the market.

However, also co-operation with regard to standardisation has to respect competition law. In essence, where participation in standard-setting is unrestricted and the procedure for adopting the standard in question is transparent, standardisation agreements which contain no obligation to comply with the standard and provide access to the standard on fair, reasonable and non-discriminatory terms will normally not restrict competition.¹¹⁸

Among others, ITU-T has carried out standardisation initiatives related to the IoT under the Global Standards Initiative on IoT (IoT-GSI).¹¹⁹ Its goal was to promote “a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale”.¹²⁰ Such an initiative dates back to a report on the Internet of things from 2005.¹²¹ ITU has in the meantime taken more concrete steps in a Recommendation ITU-T Y.2060 from June 2012.¹²² The IoT-GSI concluded its activities in July 2015 and the new ITU-T Study Group 20 “IoT and its applications including smart cities and communities”¹²³ was established. All ongoing activities in the IoT-GSI were transferred to the new SG20.

As for standardisations bodies, since 2006, IETF (Internet Engineering Task Force) has also produced a series of standards and protocols designed for the IoT.¹²⁴ Besides, the initiative of ETSI focused on the development of an application-independent ‘horizontal’ service platform seems to be an important step.¹²⁵

Besides, the “OneM2M” initiative was founded in 2012 by seven international standards bodies in order to set up “a common efficient, easily and widely available M2M Service Layer”.¹²⁶ To date, this initiative consists of 202 members (mainly from the industry), associate members (government and regulatory agencies) and partners (standards bodies). Although common

¹¹⁸ Cf. EU Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ 2001, C 11/1, para. 257 et seq., in particular para 280.

¹¹⁹ See the most recent constitution of a new group titled “ITU-T Study Group 20: IoT and its applications, including smart cities and communities”. ITU, *ITU standards to integrate Internet of Things in Smart Cities*, Itu.int, 10 June 2015.

¹²⁰ ITU, *Internet of Things Global Standards Initiative*, itu.int, 2015 (<http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>).

¹²¹ ITU, *ITU Internet reports 2005: Internet of Things, 2005*. See Chapter 4 on “Emerging challenges” and more specifically Chapter 4.2 on “Standardization and Harmonization”. An executive summary is available here: http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

¹²² ITU-T, *Overview of the Internet of things*, Y.2060, June 2012.

¹²³ <http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx>

¹²⁴ See Zhengguo Sheng *et al.*, *A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities*, *Wireless Communications, IEEE*, December 2013, vol. 20, issue 6.

¹²⁵ ETSI, *ETSI M2M Horizontal Platform Strategy*, Etsi.org, 27 May 2014 (http://docbox.etsi.org/Workshop/2014/201405_smartappliancesworkshop/s01_m2mplatforms_koss_arndt.pdf).

¹²⁶ Association of Radio Industries and Businesses (ARIB, Japan), Alliance for Telecommunications Industry Solutions (ATIS, US), China Communications Standards Association (CCSA), European Telecommunications Standards Institute (ETSI) Telecommunications Industry Association (TIA, US), Telecommunications Technology Association (TTA, Korea) and Telecommunication Technology Committee (TTC, Japan).

standards in the application environment also play a significant role, the initiative's objective is not, however, "to standardise the whole environment across networks, applications and devices [but the] interfaces so they are applicable to the entire ecosystem."¹²⁷

Standards play a significant role in the development of IoT technologies as they define openness, interoperability and ultimately competitiveness in the IoT environment. Standardisation bodies are already addressing the issue of standardisation in the IoT environment in a significant manner.

BEREC acknowledges that the IoT industry is currently driven more by proprietary standards 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 possible anti-competitive national fragmentation in the standardization process).

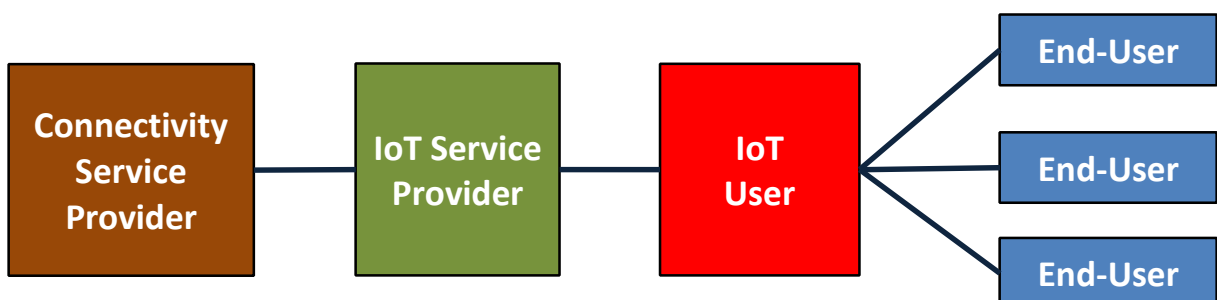
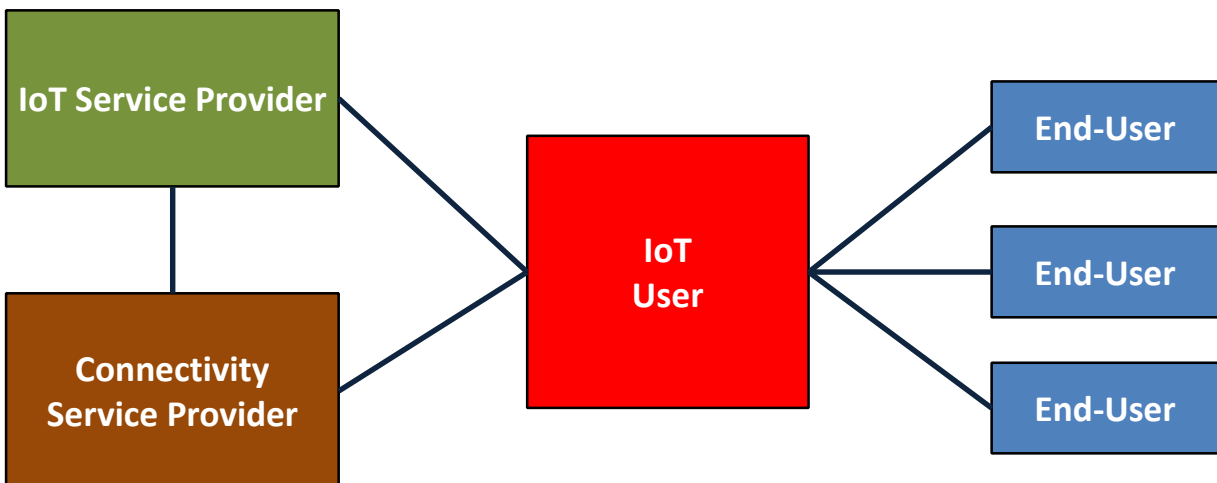
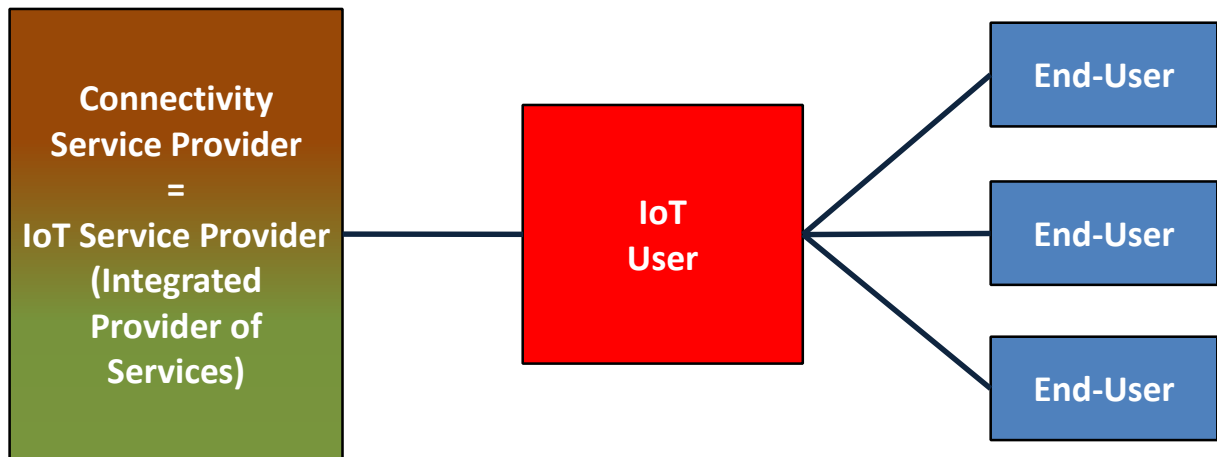
¹²⁷ oneM2M, *The Interoperability Enabler for the Entire M2M and IoT Ecosystem. White paper*, January 2015.

Glossary

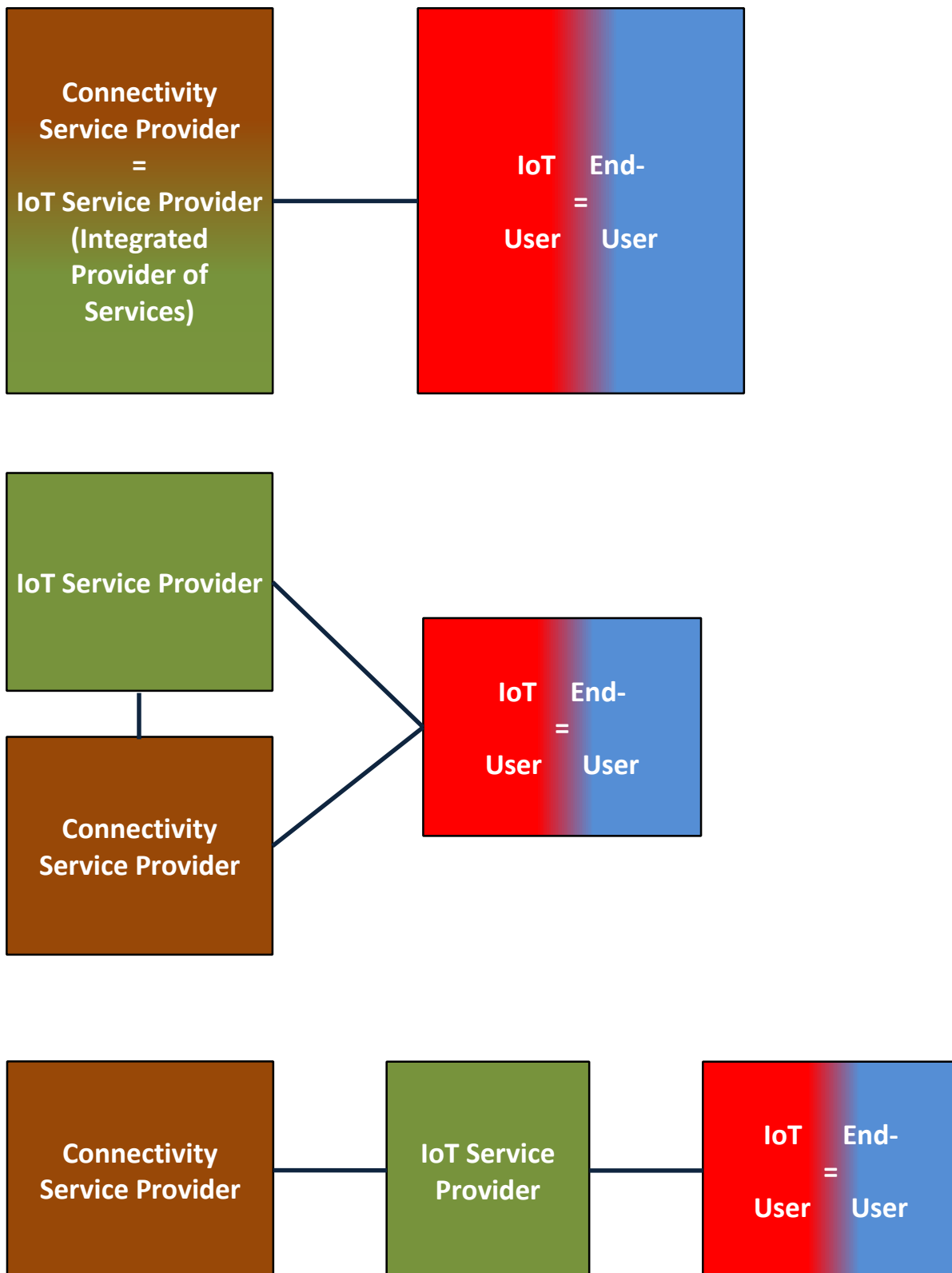
| | |
|--------------------------------|---|
| Connected device | Device/Product in which an M2M device is integrated (e.g. connected car, smart meter). |
| Connectivity service provider: | Provider of an electronic communication service pursuant to Art. 2 lit. c Framework Directive, i.e. basically a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks [...]. |
| E.164 number | A string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in [ITU-T E.164]. The number contains the information necessary to route the call to the end-user or to a point where a service is provided. |
| E.212 number | See IMSI, MCC, MNC and MSIN. |
| End-user: | Customer at the end of the value chain who purchases a connected device (including an M2M service and/or M2M device) (e.g. car owner, electricity customer). An end-user may be a private person or a company (e.g. private car owner and/or company with a car fleet). |
| IMSI | International mobile subscription identity: [ITU-T E.212] „IMSI is a string of decimal digits, up to a maximum length of 15 digits, which identifies a unique subscription. The IMSI consists of three fields: the mobile country code (MCC), the mobile network code (MNC), and the mobile subscription identification number (MSIN)“. |
| IoT service provider: | Provider of an IoT service, which can comprise the provision of an IoT platform and/or other IoT-related IT-services/solutions. |
| IoT user: | Purchaser of an IoT service who incorporates the IoT 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). |
| MCC | Mobile country code: [ITU-T E.212] The MCC is the first field of the IMSI and is three digits in length and identifies a country. The Director of TSB may assign more than one MCC to a country. MCCs in the 90x range are administered by the Director of TSB. |
| MNC | Mobile network code: [ITU-T E.212] The MNC is the second field of the IMSI, it is two or three digits in length and is administered by the respective national numbering plan administrator. The MNC, in combination with the MCC, provides sufficient information to identify the home network. |
| MSIN | Mobile subscription identification number (MSIN): [ITU-T E.212] The MSIN is the third field of the IMSI, it is up to 10 digits in length, and is administered by the relevant operator to identify individual subscriptions. |

Annex 1: The IoT value chain – Examples

1. Business Applications



2. Industrial Applications



Annex 2: List of BEREC IoT stakeholder interviews

| Date | Stakeholder |
|----------------|--|
| 16.06.2014 | CISCO KCL |
| 17.06.2014 | ETNO GEMALTO ITU |
| 26.06.2014 | ECTA GSMA |
| 27.06.2014 | ETSI EURELECTRIC |
| 17.07.2014 | IET |
| 18.07.2014 | ERICSSON ETSI QUALCOMM |
| 26.07.2014 | Volkswagen |
| 29.-30.09.2014 | Aspider AT&T CoopVoce / Postemobile Fastweb Telecom Italia Tele 2 Sverige Vodafone Wind Telecomunicazioni |