Body of European Regulators
for Electronic Communications
BEREC

BoR (16) 81

BEREC views on *Internet of Things* & *Machine to machine* communications

Francesco Sciacchitano (AGCOM)

OCECPR Stakeholder Meeting , 12 April 2016

Nicosia, Cyprus

Plan of the presentation

- **Description of the IoT phenomenon** - *15 minutes*
  - Market penetration of IoT services
  - Identification of the main features

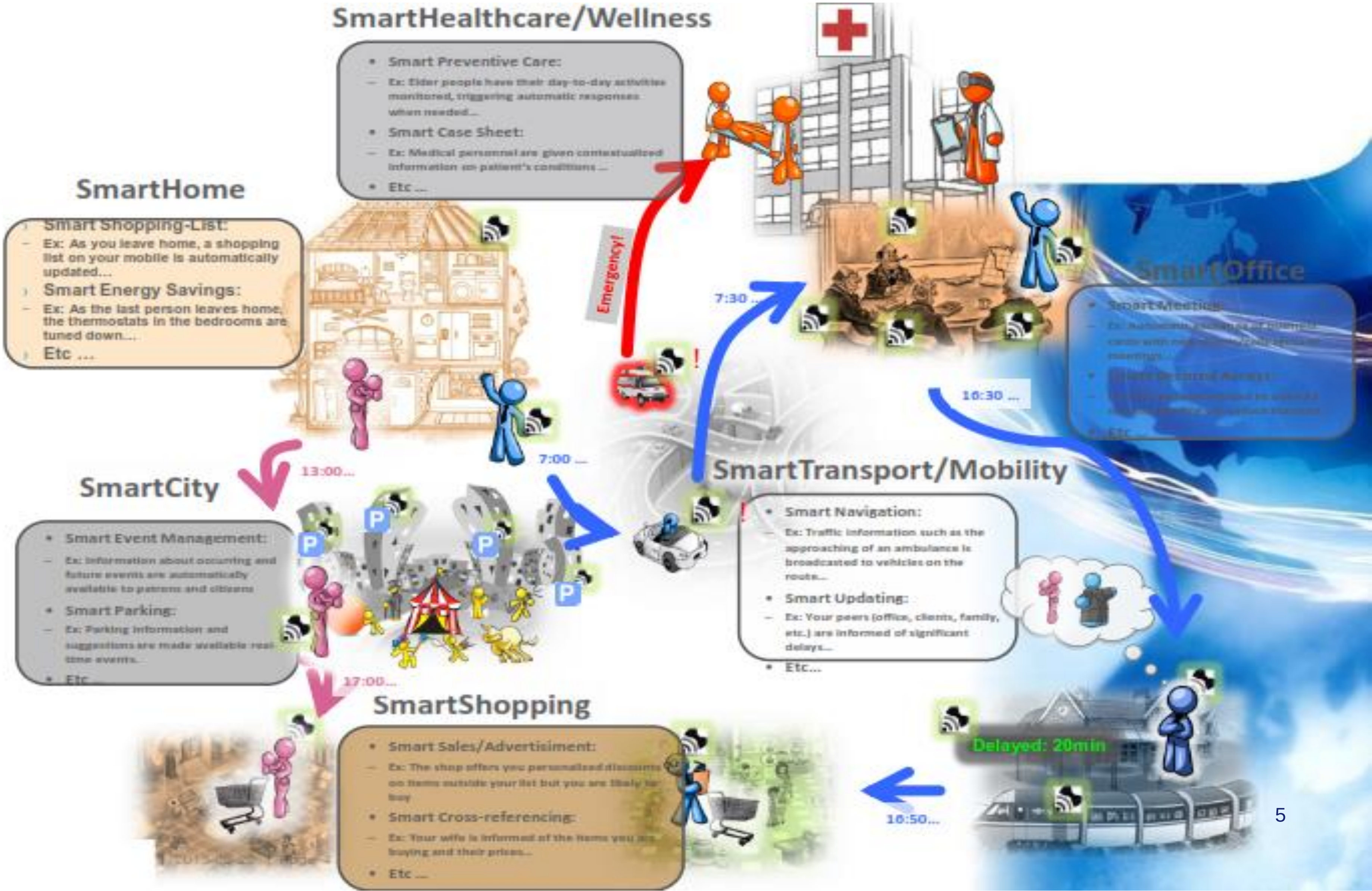
- **Main regulatory issues discussed by BEREC** – *15 minutes*
  - Regulatory framework
  - Scarce resources (spectrum & numbers)
  - Competition issues: vertical integration & lock-in
  - International roaming
  - Applicability of consumer protection tools (portability)
  - Privacy & security of the networks

BEREC work on IoT / M2M

- 2010: BEREC paper on convergent services (description of M2M)
- 2013/2014: stakeholder interviews, internal report
- 2015 (M2M within EWG NGN): IoT/M2M draft report
  - Presentation of the report at the Stakeholders' forum
  - Public consultation
  - Presentation of the report at the BEREC Plenary
  - Publication on the BEREC Website: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

PART 1: Description of the IoT phenomenon

a) Market penetration of IoT services
b) Identification of the main features



SmartHealthcare/Wellness

- Smart Preventive Care:
  - Ex: Elder people have their day-to-day activities monitored, triggering automatic responses when needed...
- Smart Case Sheet:
  - Ex: Medical personnel are given contextualized information on patient's conditions ...
- Etc ...

SmartHome

- Smart Shopping-List:
  - Ex: As you leave home, a shopping list on your mobile is automatically updated...
- Smart Energy Savings:
  - Ex: As the last person leaves home, the thermostats in the bedrooms are tuned down....
- Etc ...

SmartOffice

- Smart Meetings:
  - Ex: Automatic exchange of business cards with [illegible] meetings
- [illegible]
  - [illegible]
- Etc

SmartCity

- Smart Event Management:
  - Ex: Information about occurring and future events are automatically available to patrons and citizens
- Smart Parking:
  - Ex: Parking information and suggestions are made available real-time events...
- Etc ...

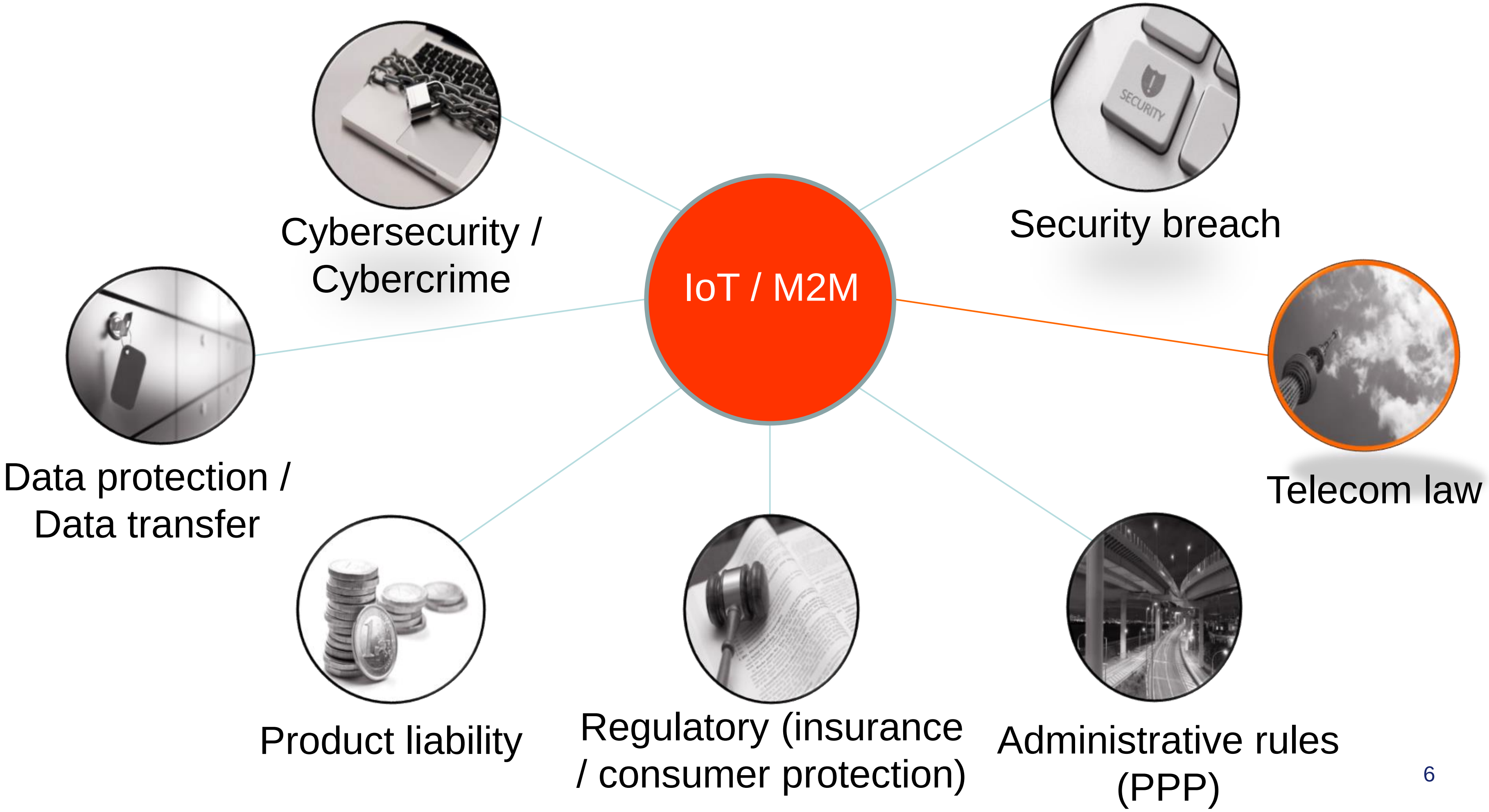
SmartTransport/Mobility

- Smart Navigation:
  - Ex: Traffic information such as the approaching of an ambulance is broadcasted to vehicles on the route...
- Smart Updating:
  - Ex: Your peers (office, clients, family, etc.) are informed of significant delays...
- Etc...

SmartShopping

- Smart Sales/Advertisiment:
  - Ex: The shop offers you personalized discounts on items outside your list but you are likely to buy
- Smart Cross-referencing:
  - Ex: Your wife is informed of the items you are buying and their prices...
- Etc ...

Legal issues related to IoT



IoT / M2M

Cybersecurity / Cybercrime

Security breach

Data protection / Data transfer

Telecom law

Product liability

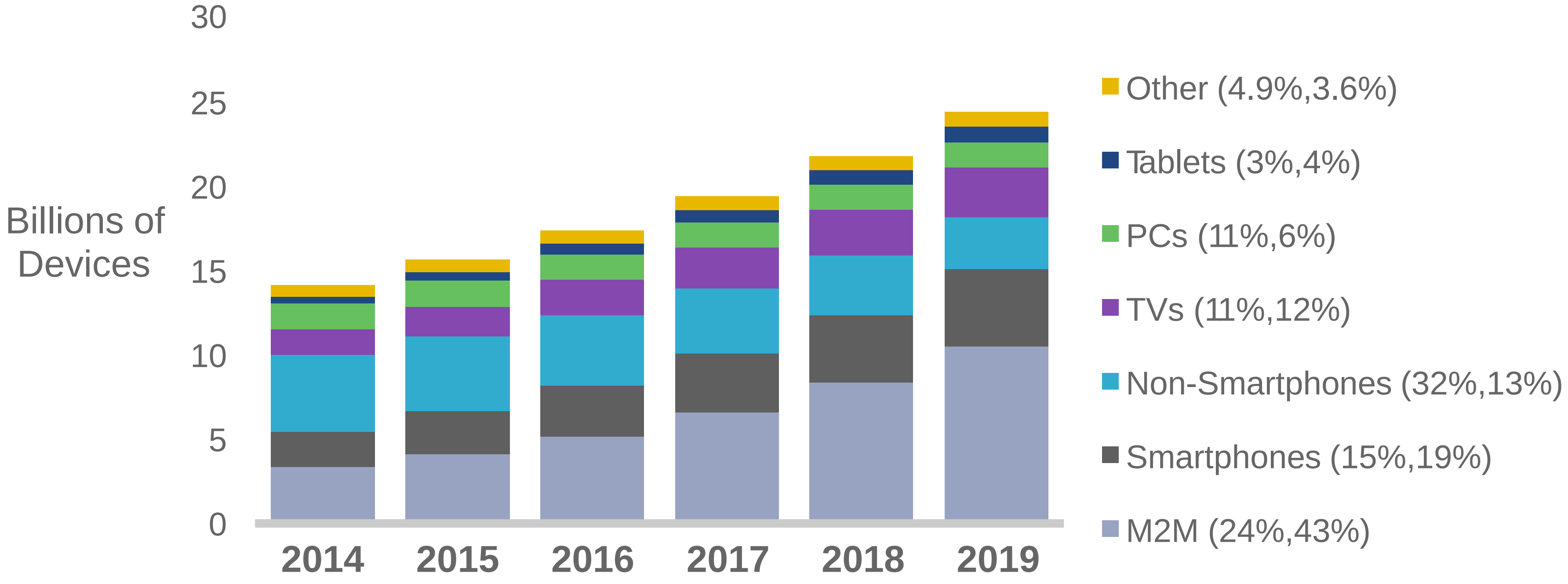
Regulatory (insurance / consumer protection)

Administrative rules (PPP)

A view on the M2M market

Global Connected Device Growth by Type

By 2019, M2M Connections Will be More Than 40% of Total Connections



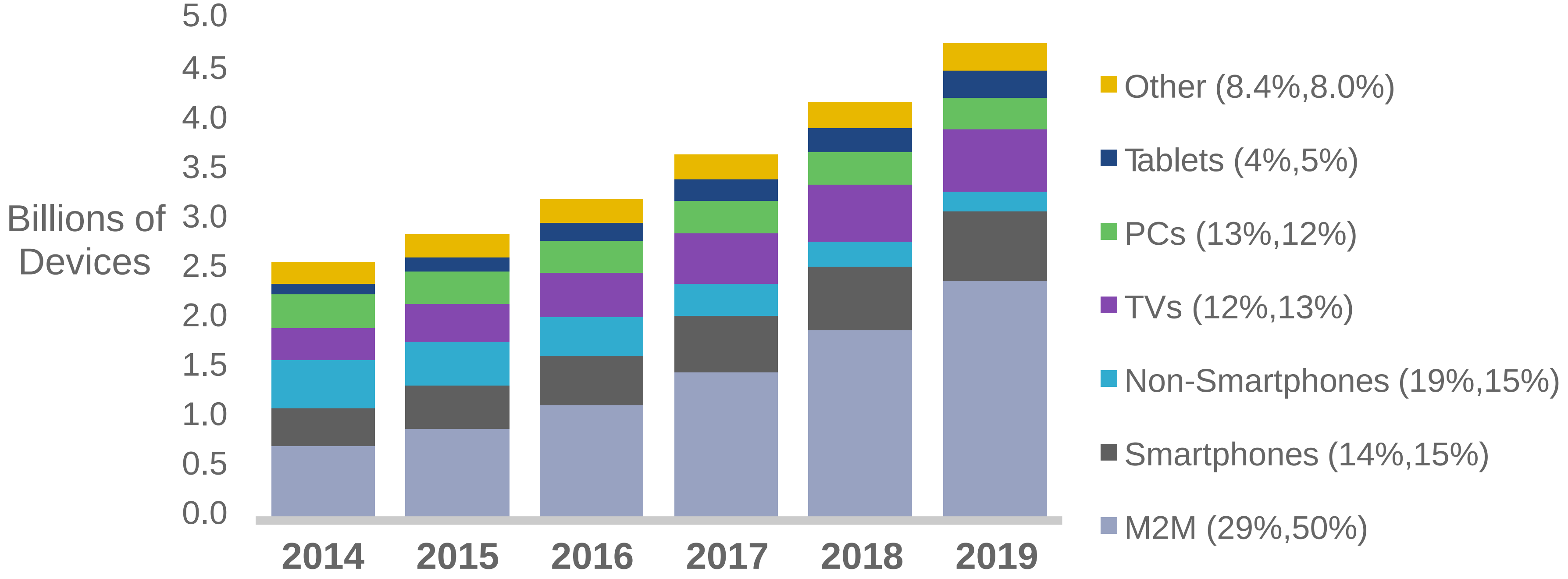
*** Figures (n) refer to 2014, 2019 device share**

Source: Cisco VNI Global IP Traffic Forecast, 2014–2019

A view on the M2M market

Europe Connected Device Growth by Type

By 2019, 50% of Total Connections in Europe Will be M2M



*** Figures (n) refer to 2014, 2019 device share**

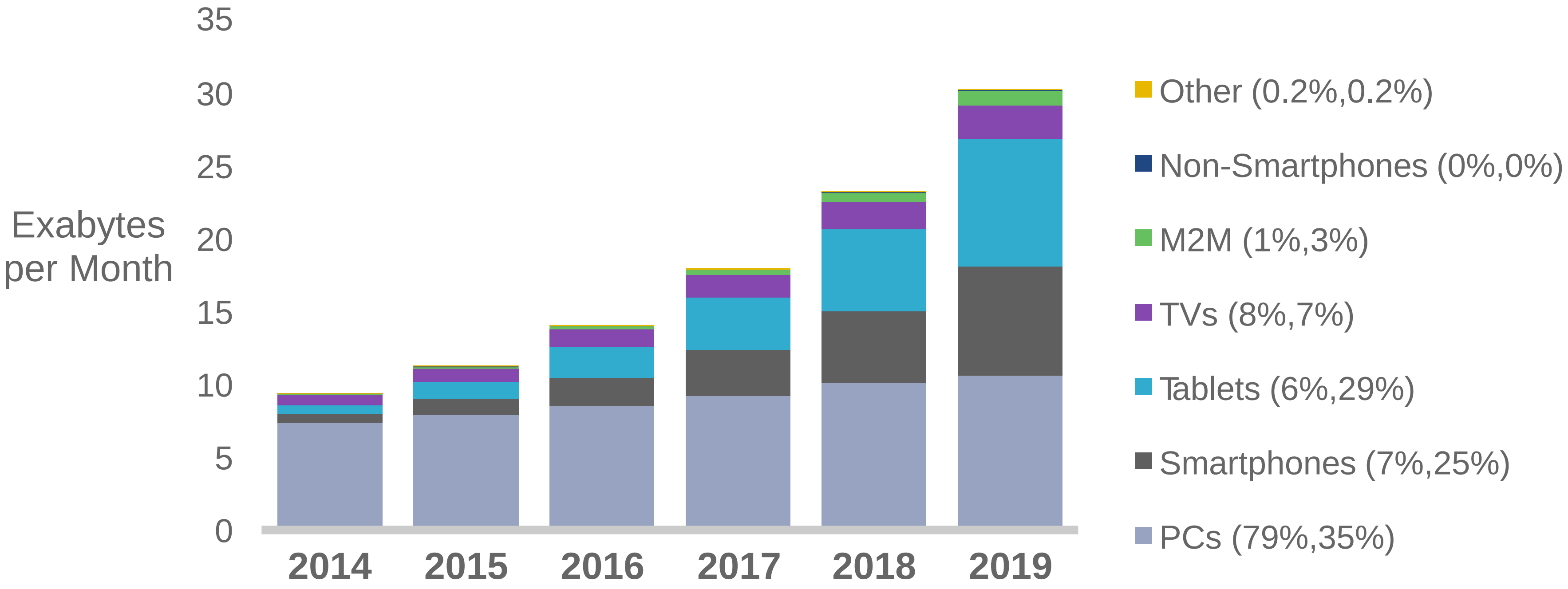
Source: Cisco VNI Global IP Traffic Forecast, 2014–2019

*Note Europe defined as Western Europe + CEE, excluding Ru

A view on the M2M market

Europe Internet Traffic by Device Type

M2M Traffic Only About 3% by 2019



*** Figures (n) refer to 2014, 2019 device share**

Source: Cisco VNI Global IP Traffic Forecast, 2014–2019

*Note Europe defined as Western Eu + CEE, excluding Ru

Main drivers of the sector

1. Connected Car
infotainment, apps, navigation, telematics, e-calls

2. E-health services: Fitness trackers, Smart wearables, Health care gateways, smart pill

3. Smart metering & grids

Automated meter readings

4. Smart cities

Smart lighting, parking, waste management,

5. Transportation: Car Hire, Share, fleet management + pay as you drive insurance

6. Agriculture

Humidity sensors for gardens and fields irrigation

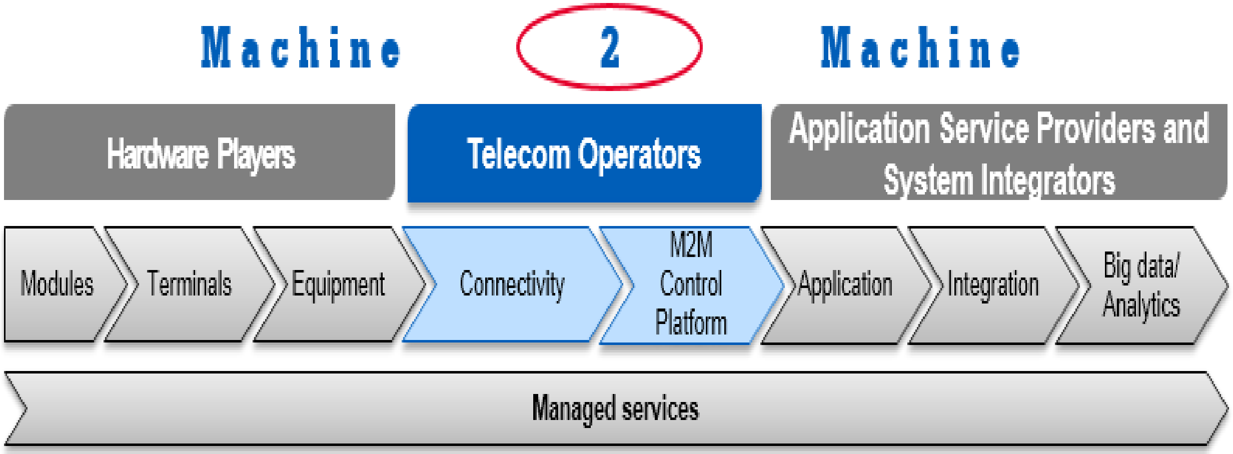
7. Building Automation
Energy savings, efficiencies in building management

8. Security
Private security, enhanced remote monitoring

Characteristics of IoT

- Fully **automatic** (or with limited human intervention) communication of data from remote devices
- M2M **communication patterns** differ from personal communications
- Usually **Low traffic volume**, with sporadic/irregular patterns (**signals**)
- Relatively simple devices (both static and mobile)
- M2M services require **connectivity**, however connectivity accounts for a relatively low proportion of the overall revenue opportunity in the M2M value chain
- Many M2M devices produced for the world-market, hence many M2M services based on **global mobility**
- Many M2M devices designed to have a **long lifetime** (20-30 years)
- Usually the business model is **B2B**, even if devices may be aimed at consumers (B2B2C)

IoT Value chain & business model

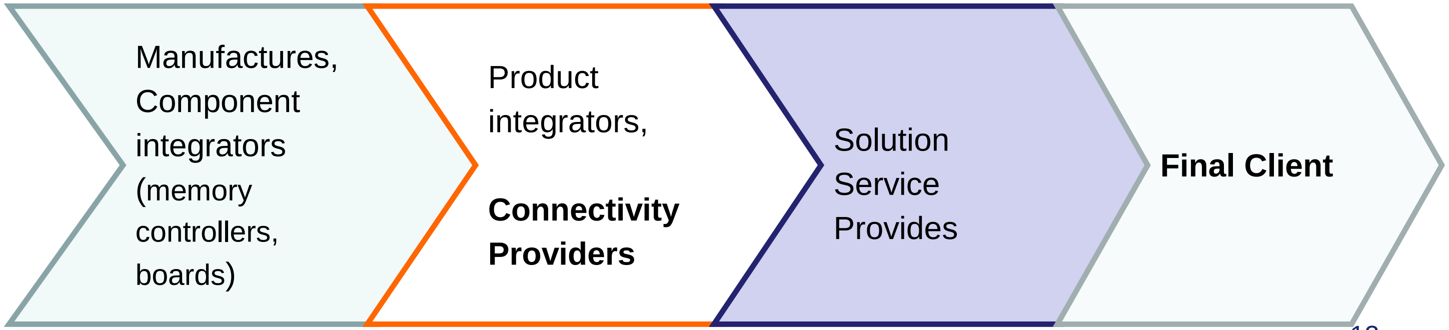


New business model

- Connectivity is only a part of the business
- Telecommunications companies have different strategies: either to provide connectivity only or to provide more integrated services
- Partnerships & alliances

New value chain:

- Usually the consumer is not the end user;
- It's a B2B, not a B2C model
- Global business


Manufactures, Component integrators (memory controllers, boards)

Product integrators,

Connectivity Providers

Solution Service Provides

Final Client

Part 2: Main regulatory issues discussed by BEREC

a) Regulatory framework

b) Scarce resources (spectrum & numbers)

c) Competition issues: vertical integration & lock-in

d) International roaming

e) Applicability of consumer protection tools (portability)

f) Privacy & security of the networks

Regulatory Framework

- Applicable framework (e.g. authorization regime) depends on the applicability of the definition of electronic communication service (ECS)
- 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, […]”*.
- Within the IoT/M2M value chain:
  - ➢ Connectivity service provider = ECS
  - ➢ IoT/M2M-user = typically no ECS, unless reseller
  - ➢ However, careful case-by-case approach since there are so many different types of packages including connectivity and since business models are just beginning to evolve.

DSM review: The definition of ECS might be extended to include a wider range of service providers, maybe with different obligations

Numbers and Identifiers

- 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 M2M services based on mobile connectivity:
  - ➢ E.164 numbers/scarcity: not a problem. National solutions
  - ➢ Migration to IPv6 will solve scarcity issues
  - ➢ Global marketing of connected devices:
    - – Permissibility of **extra-territorial use** of numbers?
    - – Use of international **ITU numbering** resources?
    - – Use of European numbering resources (**ETNS**) not worth the cost…

Spectrum

- No major problems of scarcity of frequencies for mobile applications
- Technology choices may depend on what, how, and how much, spectrum is made available. Availability of White spaces, unlicensed spectrum, IoT narrow-band and shared licenses might have an influence on how IoT evolves.

Switching / “lock-in” issue

- If a customer intends to change connectivity service provider, it is currently necessary that the SIM is replaced physically. In the M2M-context, the costs and the proprietary standards might prevent switching the connectivity service provider (“**lock-in**”).
- Possible solutions:
  - MNC assignment to IoT/M2M-user (i.e. right to apply for own MNC/IMSI range). Forbidden by several Countries
  - Over-the-air (OTA) provisioning of SIM

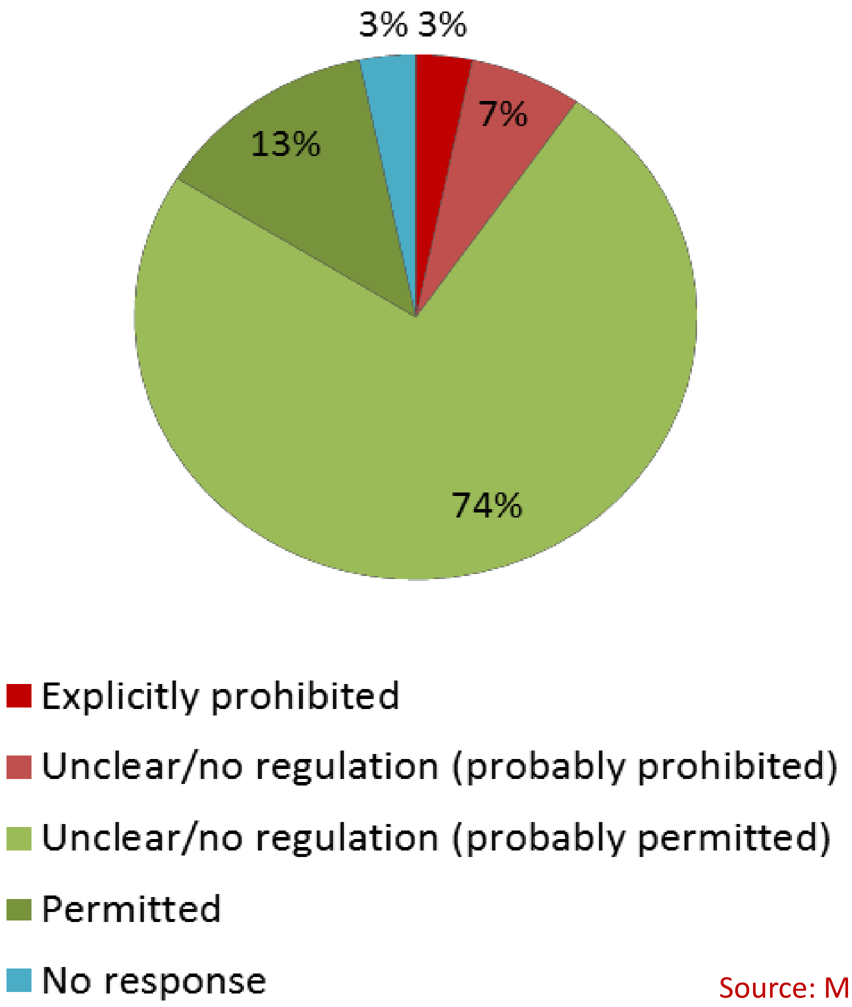
- DSM review: Special treatment required
  - ➢ Regulatory measures to make MNC assignment more flexible
  - ➢ Regulatory measures to foster OTA provisioning of SIM or make it mandatory

Roaming

- 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 temporary.
- Permanent roaming appears to be a key factor for the success of certain IoT business models being used
  - Is permanent roaming formally allowed?
  - Is Roaming regulation applicable in these cases? 3 scenarios
    - 1: Device travelling periodically (car, kindle….)
    - 2: Device travelling abroad most of time (car sold abroad)
    - 3: Device placed abroad permanently (smart meter) Roaming regulation does not apply

- In Europe the TSM modified the **Roaming regulation**: it allows permanent roaming and states that the operators may include conditions in the reference offer to prevent it.

Regulation of permanent roaming around the world



Source: Machina Research 2014

Applicability of consumer protection tools

- Need to strike a balance between the need to protect consumer (with measures that are costly) and the need to foster the development of the IoT: the consumer protection rules should apply:
  - Only if the regulatory framework applies
    - IoT is B2B2C, not B2C
  - Only if there is a real need to protect the consumers
    - No number portability if the consumer does not know the number

- DSM review: adapt the framework to the peculiarities of the IoT

Privacy

- Personal data may be collected by a number of connected devices.
- Who collects the data? Who owns the data? Where is it stored? Does the consumer give consent to the use of the info? How?
- Current legal framework: Privacy Directive (Directive 95/46/EC) and sector-specific ePrivacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC); no specific rules with regard to IoT/M2M.
- 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 rules on information and consent should be made as user-friendly as possible.

- SOLUTION: revision of EU data protection framework under way (**GDPR** - General Data Protection Regulation), aim also to adapt privacy rules to digital era

Network security

- National legislation of a Member State (based on Art. 13a Framework Directive) concerning network security does not specifically address IoT services.
- 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.

- SOLUTION: draft Directive in order to ensure a high common level of network and information security (**NIS**) across the EU

Thank you

Francesco Sciacchitano (AGCOM)

f.sciacchitano@agcom.it