Pedro Seixas
ITU Expert

As an expert telecommunications regulation advisor, with over 25 years of consultancy experience, provides guidance and recommendations to Governments, National Regulatory Authorities (NRAs) and operators, as well as to regional and international bodies on telecommunications policy and regulation, including regulatory and policy frameworks, access and interconnection, construction of cost models and conduct of public consultation to set call termination rates, fixed, mobile and cable landing station cost modeling, tariff regulations, process design for defining telecommunications markets, determining dominance and establishing appropriate remedies, and mobile and fixed licensing.

His telecommunications regulation consulting activities, in recent years, specialized in bringing leading-edge regulatory expertise to developing economies in Africa, Asia, South America and the Middle East and have also covered a wide range of other specific issues associated with regulation such as convergence, sharing of infrastructure, ex-post regulation, competition, broadband and more recent issues arising from the emergence of new players in the industry such as application service providers (initially called over-the-top) and Net Neutrality discussions.. Several projects included the NRAs staff training on the use of cost models and ex-ante and ex-post regulatory case studies.

Internet of Things regulatory aspects

AREGNET Workshop on IoT & M2M

Manama, Kingdom of Bahrein
1 October 2018

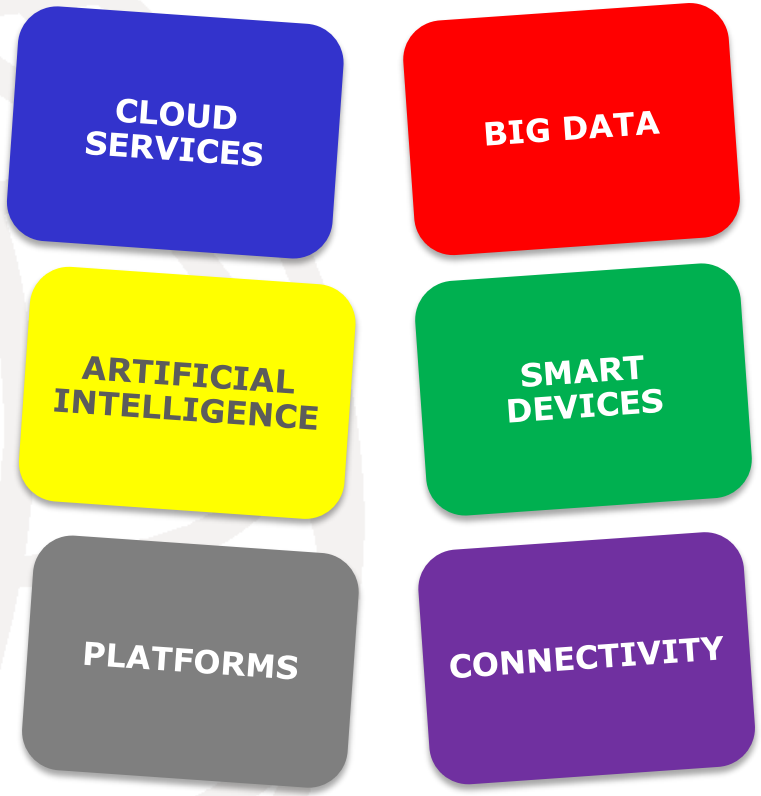
Pedro Seixas, ITU Expert

Agenda

- What is IoT?
- How and by whom is IoT used?
- What are the social and economic benefits and costs of IoT?
- What regulatory concerns does IoT arouse?
- How can policy and regulation help?

The world is getting SMART

- Internet of Things (IoT)* and M2M do not come alone
- National Regulatory Authorities (NRAs): either forbearing on regulation or use of targeted regulatory interventions in order to enable IoT



*A wider scope definition encompasses the Internet of Everything (IoE), which includes big data analysis, cloud services, and sensors and actuators that, in combination, can efficiently run autonomous machines and intelligent systems.

Connected "things": a very significant growth

- Experts estimate an exponential growth of the number of connected objects, up to 2020:
  - IDATE = 80 Billion
  - CISCO = 50 Billion
  - Gartner = 26 Billion
  - Ericsson (2023) = 31.4 Billion
- Impact on mobile is small: the majority stands still with no sim.

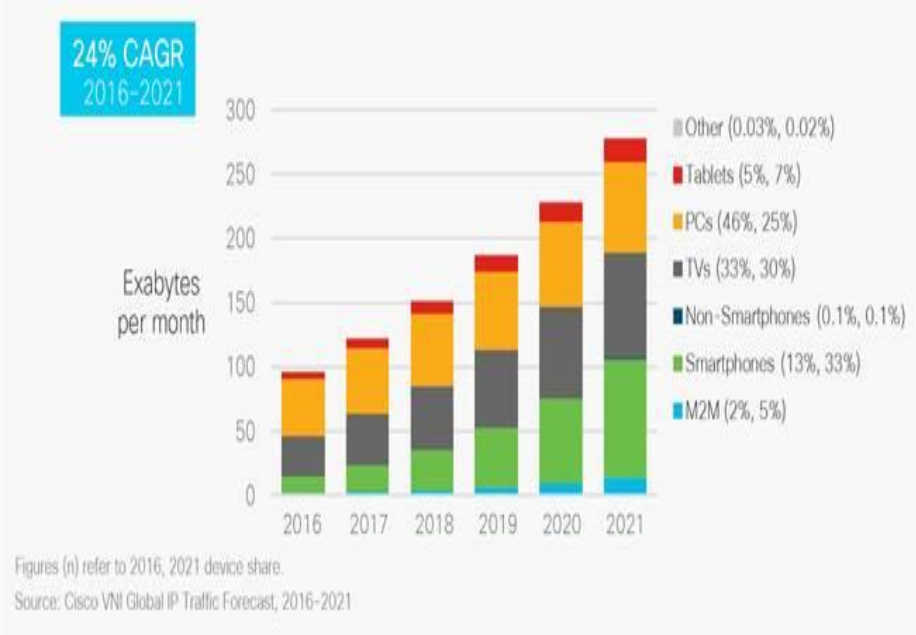
Connected devices evolution (Billions)

IoT	2017	2023	CAGR
Wide-area IoT	0.8	4.1	30%
Of which Cellular IoT	0.7	3.5	30%
Short-range IoT	6.2	15.7	17%
Other devices			
PC/laptop/tablet	1.6	1.7	0%
Mobile phones	7. 5	8.6	2%
Fixed phones	1.4	1.3	0%
Total devices	**17. 5**	**31.4**	**11%**

Source: Ericsson, (2018)

However impact in Internet traffic is not substantial

- Internet traffic growth is driven by video
- Predicted M2M traffic in the Internet is not substantial



Source: Cisco (2018)

How to define IoT?

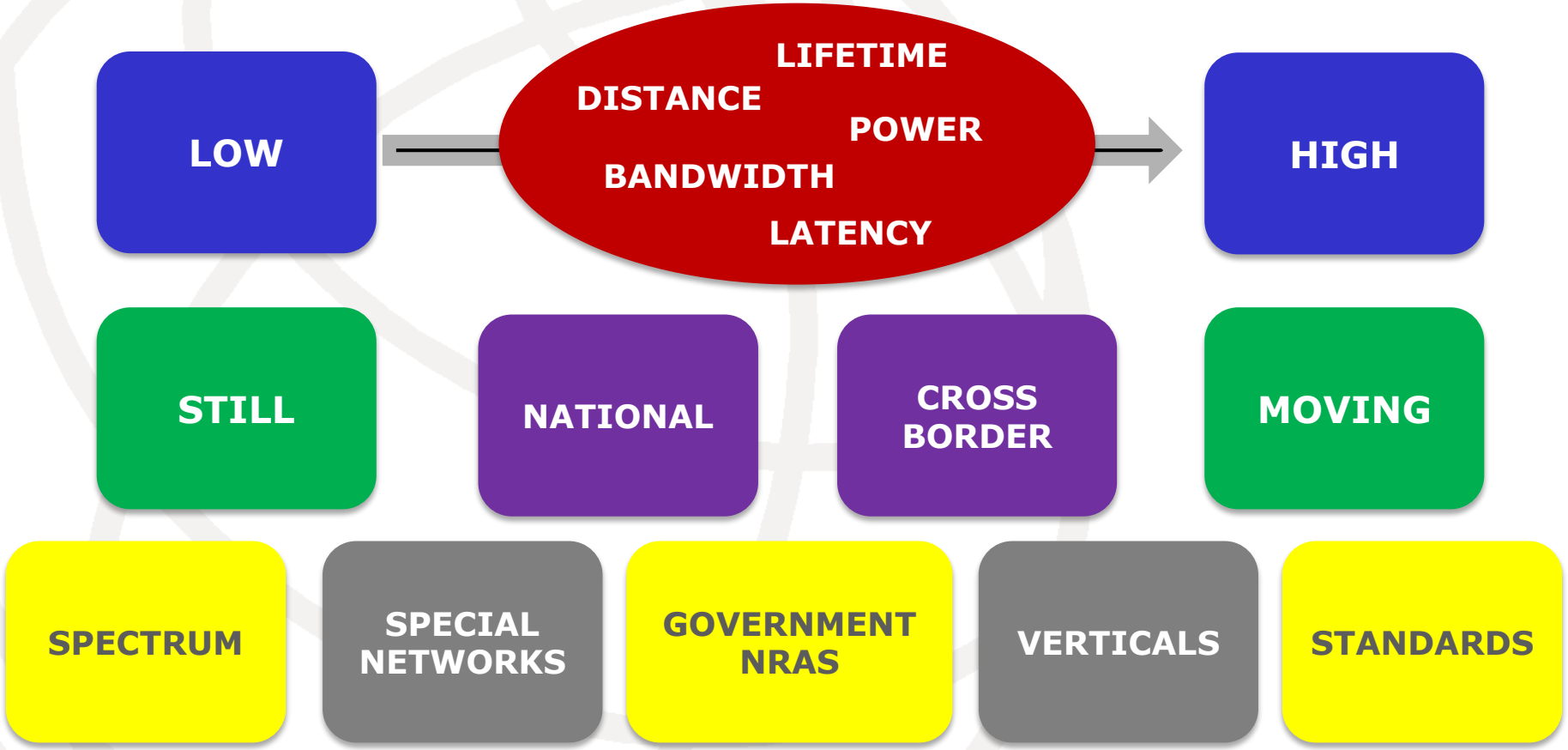
- Many different definitions have been proposed:
  - **A global infrastructure**: "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies".* (ITU, 2012)
  - **Usage**: "*The use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects*" (GSMA, 2014)
  - **A connected group of objects**: "*Dans le cadre de ce rapport, une acception large du terme internet des objets sera retenue, correspondant à un ensemble d'objets physiques connectés qui communiquent via de multiples technologies avec diverses plateformes de traitement de données, en lien avec les vagues du cloud et du big data*'' (ARCEP, 2016)

IoT applications are multi-sectoral

"Users" of IoT	Example purposes for using IoT
Humans	Sensor data provide information to guide people's actions and decisions regarding fitness and health improvement.
Home	Energy management, security, and automation of domestic appliances.
Retailers	Reducing losses due to theft, lowering inventory costs, personalised promotions.
Vehicles	Design, production and maintenance optimisation; self driving vehicles.
Hospitals	Predicting predisposition to disease and likely responsiveness to treatment plans.
Factories	Predictive maintenance, production optimisation, automated quality control

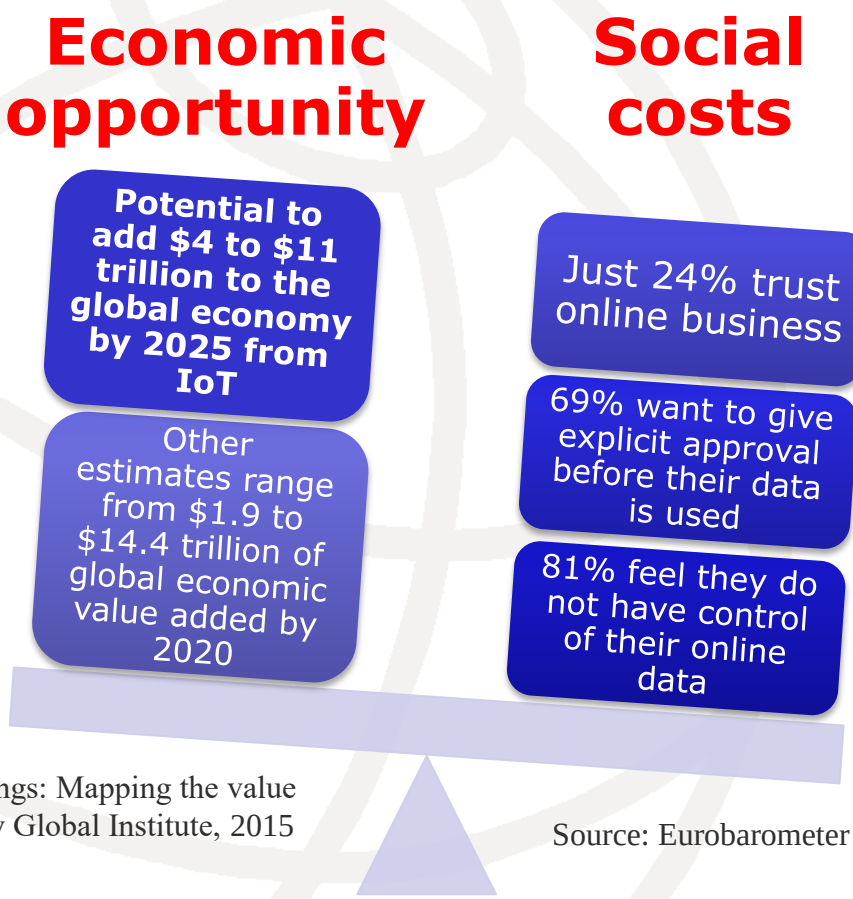
Source: "The Internet of Things: Mapping the value beyond the hype", McKinsey Global Institute, 2015

Higher complexity due to heterogeneous requirements



The IoT conflicting factors

- Predicting and warning
- Personalisation
- Research and development
- Crime prevention
- Innovation
- Manufacturing costs reduction



- Security vulnerabilities
- E-commerce
- Data
- Privacy
- Limited choice
- Political interference

Source: "The Internet of Things: Mapping the value beyond the hype", McKinsey Global Institute, 2015

Source: Eurobarometer (2015)

IoT regulatory issues: global approach vs. national solutions

	National	Cross-border
Technical	▪ Standardisation ▪ Numbering and Adressing ▪ Spectrum ▪ Network and devices security	***Key topics*** ▪ Standardisation ▪ Numbering and Adressing ▪ Spectrum
Legal	▪ Existing national legal framework ▪ Spectrum licensing/ pricing and numbering ▪ Data and privacy ▪ Liability	▪ Extra-territorial use of numbering resources ▪ Permanent roaming ▪ Data flow

Source: Based on recent NRAs Public Consultations specifically addressing IoT or related topics.

Review existing national laws and regulations

- In the short term allow M2M and IoT applications within the existing licensing framework and identify candidate spectrum bands to address estimated future demand. Plan for 5G development.
- If necessary review spectrum licensing and pricing and use of numbering resources.
- Further analyse if standards/interoperability are more than just a technical issue and need legal support.
- Allow next generation networks to expand.

Develop Standards for IoT interoperability

Examples

Organisations	Key activities
ITU-T Global Standards Initiative on IoT (IoT-GSI) 2005 up to July 2015 ITU-T Study Group 20	Standardisation initiatives related to the IoT to promote a unified approach in ITU-T for development of technical standards. ITU has in the meantime taken more concrete steps in ITU-T Y.2060 from June 2012.
IETF (Internet Engineering Task Force)	Elaboration of a series of standards and protocols designed for the IoT.
ETSI (European Telecommunications Standards Institute)	Development of an application-independent 'horizontal' service platform.
OneM2M	Set up widely available M2M Service Layer

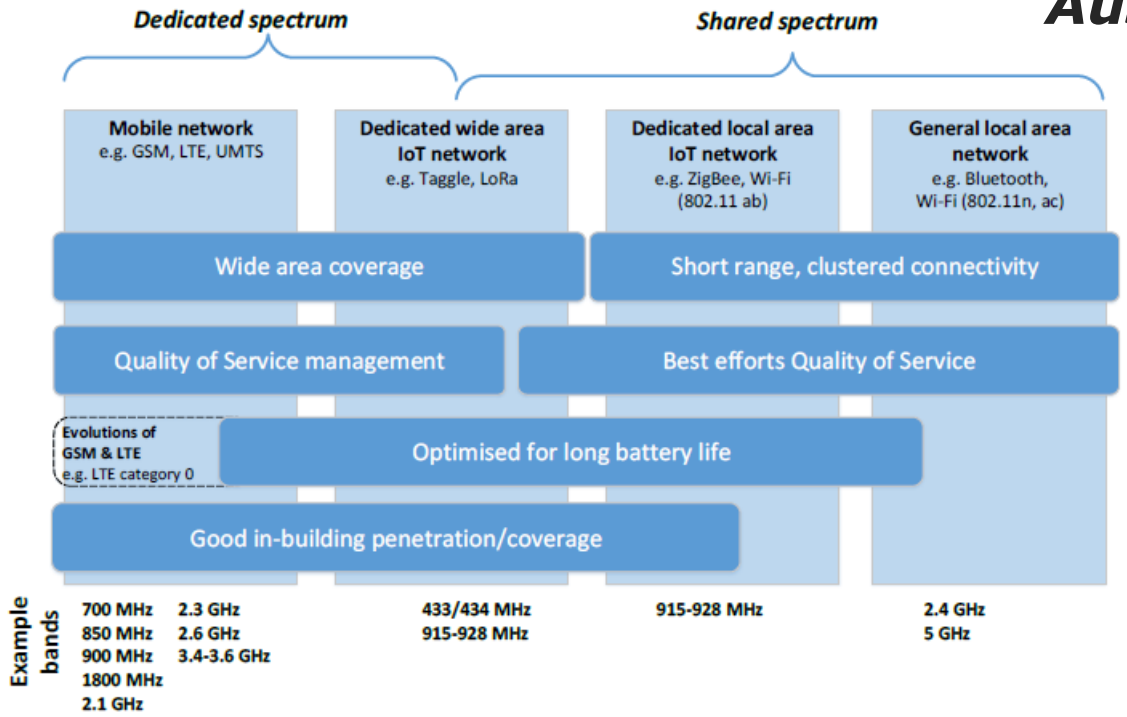
Source: BEREC (2016)

Plan for spectrum

A mix of licensing arrangements and variety of spectrum bands will be required to support different IoT purposes

Figure 2: Spectrum identified for IoT applications

Australia



Source: ACMA, based on Ofcom model 2015, updated for Australian spectrum band plans.

Source: ACMA (2015)

Network security

- "Providers of networks and services are obliged under existing legislation to take appropriate measures to manage risks to security and resilience. The existing legislation does not explicitly refer to the IoT. However, to the extent that they fall under **the definitions in the legislation**, we believe IoT networks and services would be covered by these **existing obligations**." (Promoting investment and innovation in the Internet of Things, Ofcom 27 January 2015)
- "TRC will conduct intensive studies in order to issue strong, flexible, and technology-neutral regulations and **recommend** reasonable and appropriate security practices for the operators to strengthen the data security." (Green Paper of "Internet of Things" TRC, Jordan December, 2017)

Build trust in the IoT

- A fundamental role of regulation is to ensure consumer trust in IoT, so as to achieve its potential and curb its threats.
- There are four main areas of intervention:
  - Ensuring data protection and privacy
  - Informing consumers and giving them control over data
  - Limiting the use if probabilistic predictions
  - Keeping data markets fluid.
- A key concern is how to deal with personal data, starting with the problem of defining it and separate it from the bulk of data.

Permanent roaming

- Providing worldwide reach for IoT devices will help mobile network operators to grow their revenues with new businesses at a global level.
- Extra-territorial use of numbers (including permanent roaming) is considered by many as a driver of growth for IoT / M2M, since the industry can standardise products and sell globally.
- National regulators/operators are reluctant to use foreign numbering resources in their own country.
- Among surveyed countries, permanent roaming appears to be illegal only in Brazil. In most countries, there is not yet specific regulation in force or proposed about permanent roaming for M2M communications.

Devices security

- A doll connected to the Internet was banned in 2017 by Germany's telecommunications regulator, the Federal Network Agency, "Items that conceal cameras or microphones and that are capable of transmitting a signal, and therefore can transmit data without detection, compromise people's privacy."
- Other complaints to the EU Commission include serious security flaws with two toys namely insufficient security measures to prevent unauthorised access to microphones and speakers.
- Connected devices may be particularly vulnerable to security risks. Sometimes they lack the adequate processing power and storage capability to host security software or being able to employ encryption or anonymisation techniques.

Summary conclusions

- IoT goods and services will be sold on a global scale and consumers will often want these devices to work wherever they are, therefore technical and legal frameworks, both domestic and internationally, should be interoperable in nature: e.g. standardisation, permanent roaming and cross-border data flows are key.
- In the short term Governments/NRAs could review their existing telecommunication laws and regulations in order to evaluate whether they provide for an adequate regulatory framework for IoT and M2M.
- Build trust in the IoT: IoT is all about data. Privacy, security, liability, and consumer rights are affected by the pervasiveness and longevity of the IoT. The diversity of policy and regulatory frameworks should converge globally to enable trust in the IoT.

Thank You

If you have any questions please contact me:
ps@incyteconsulting.com

Pedro Serra de Seixas, ITU Expert

Public Consultations

- Promoting investment and innovation in the Internet of Things, Ofcom 23 July 2014 and Ofcom Statement, 27 January 2015
- BEREC Report "Enabling the Internet of Things", February 2016
- Green Paper of "Internet of Things", Telecommunications Regulatory Commission, Jordan December 2017
- INTERNET OF THINGS (IOT) TECHNICAL REGULATORY ASPECTS & KEY CHALLENGES TECHNICAL REPORT Malaysian Communications and Multimedia Commission, 2018

Sources

- Ericsson Mobility Report, IoT Connections Outlook, June 2018
- Cisco, "Cisco VNI Global IP Traffic Forecast, 2016–2021", 2018
- ITU, "Overview of the Internet of things", Recommendation ITU-T Y.2060,2012
- GSMA, 2014
- ARCEP, Livre Blanc, Preparer La Revolution de l'Internet des Objets, 2016
- McKinsey Global Institute, ""The Internet of Things: Mapping the value beyond the hype", 2015
- Eurobarometer, 2015
- Australian Communications and Media Authority, "The Internet of Things and the ACMA's areas of focus". Emerging issues in media and communications, Occasional paper, November 2015
- Data protection. Rules for the protection of personal data inside and outside the EU. https://ec.europa.eu/info/law/law-topic/data-protection_en