Policies and Regulations Pertaining to IoT

Organization of the ITU and its functioning

ITU

- UN specialized agency for ICTs
- standards developing organization
- unique public/private partnership

Members:

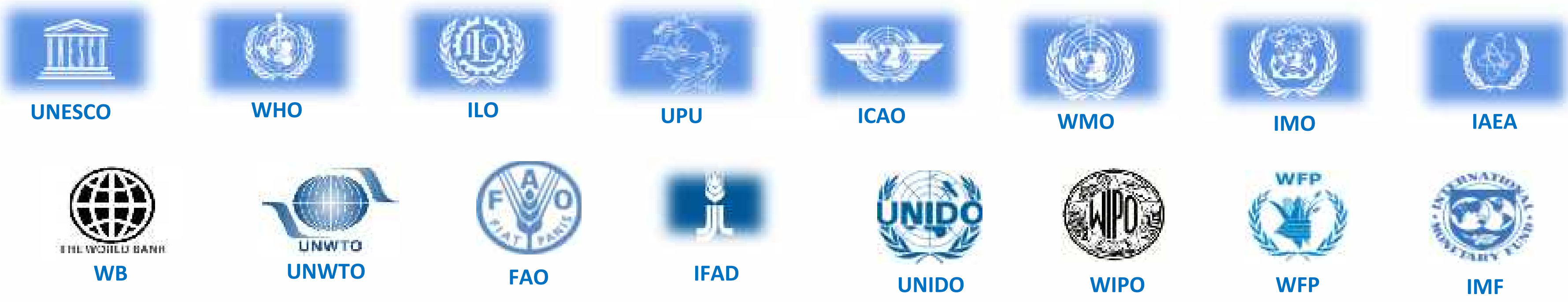
- 193 Member States (Governments and regulatory bodies)
- Over 700 Private Sector (Sector Members and Associates)
- Over 90 Academia

Brief introduction ITU

ITU at a glance

About us

Specialized Agencies of the United Nations


UNESCO WHO ILO UPU ICAO WMO IMO IAEA

WB UNWTO FAO IFAD UNIDO WIPO WFP IMF

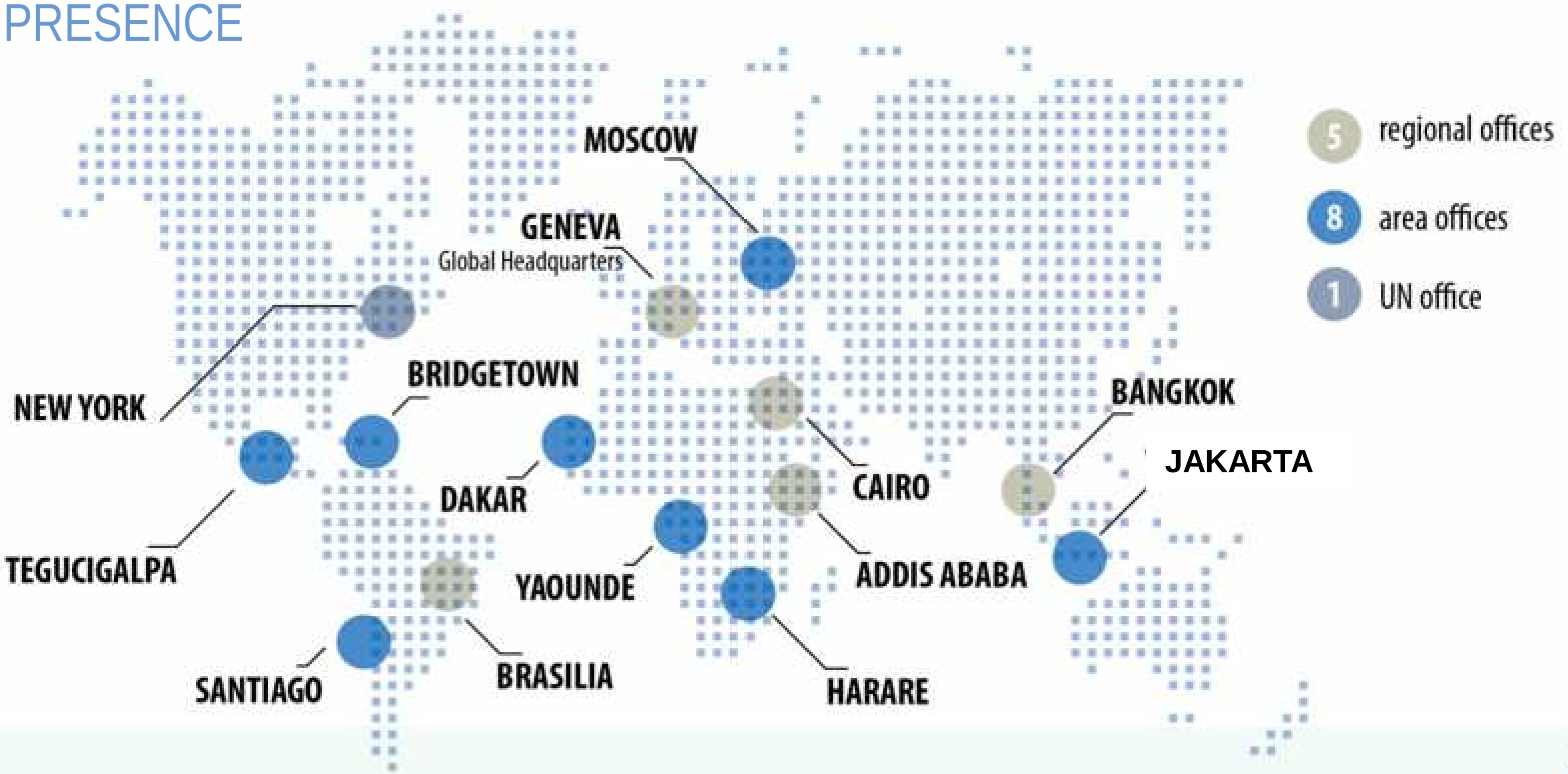
Specialized UN agency with focus on Telecommunication / ICTs

Brief introduction of ITU

ITU at a glance

Where are we?

PRESENCE



ITUACADEMY

Structure of ITU

ITU-T: standardization

produces interoperable technical ICT standards

General Secretariat

provides coordination for the whole organization

ITU-R: Radio comm.

coordinates global wireless communication

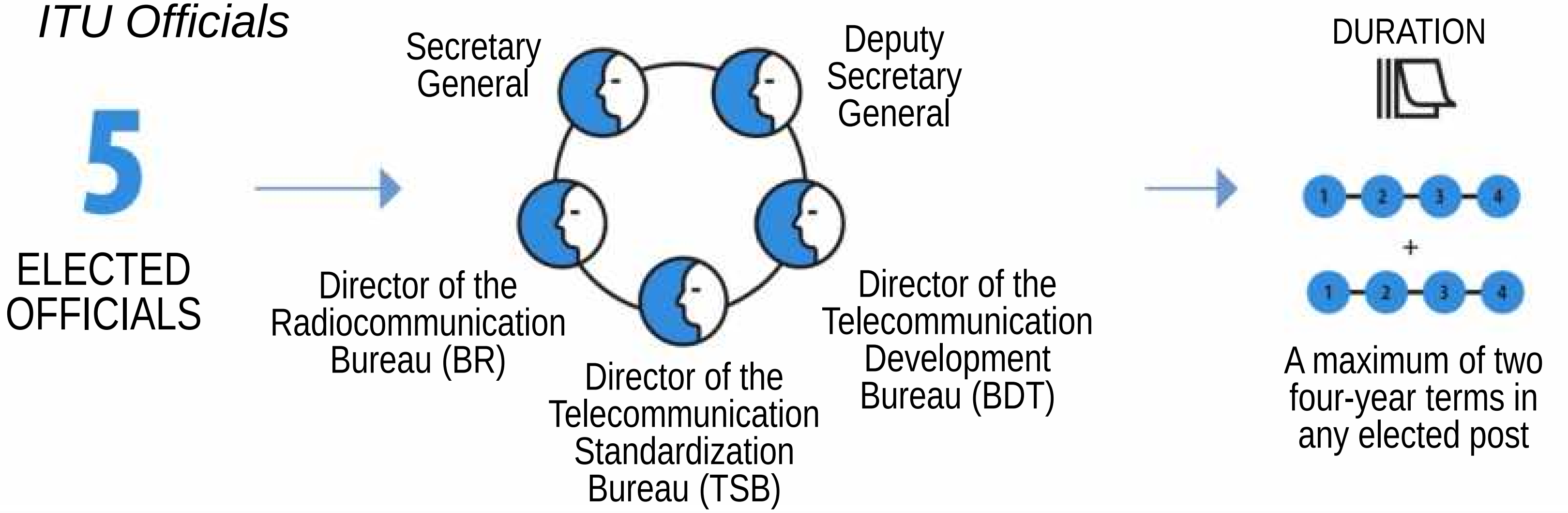
ITU-D: Development

provides assistance to the un-connected

WHO ARE WE?

ITU Elections : *during Highest Governance Forum i.e. Plenipotentiary conference*

ITU Officials



5

ELECTED OFFICIALS

Secretary General

Deputy Secretary General

Director of the Radiocommunication Bureau (BR)

Director of the Telecommunication Standardization Bureau (TSB)

Director of the Telecommunication Development Bureau (BDT)

DURATION

A maximum of two four-year terms in any elected post

ITU at a glance

Meet us

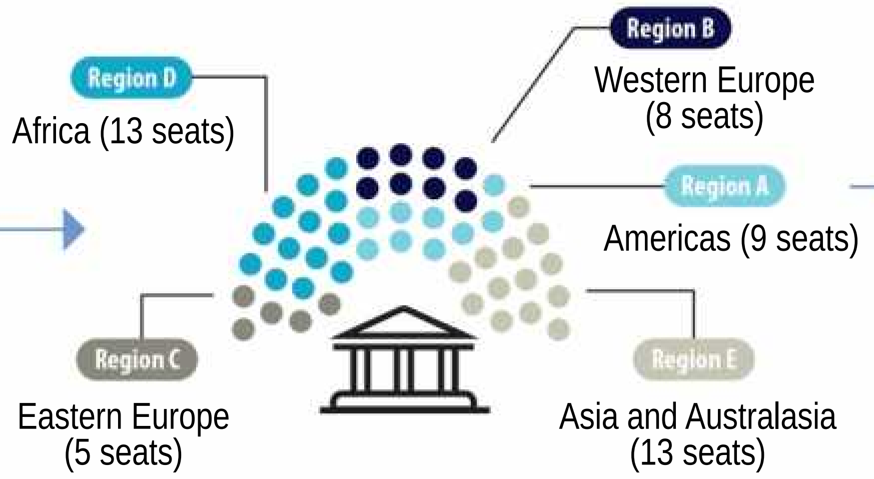
But what about the time between plenipotentiary conferences?

ITU Elections : *during highest Governance Forum i.e Plenipotentiary conference*

ITU Council

48

MEMBERS



DURATION

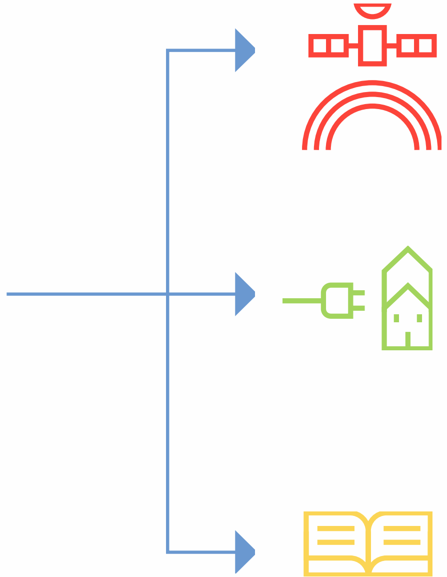
1 – 2 – 3 – 4

Elected for a four-year term

ITUACADEMY

WHAT WE DO

‘Committed to Connecting the World’



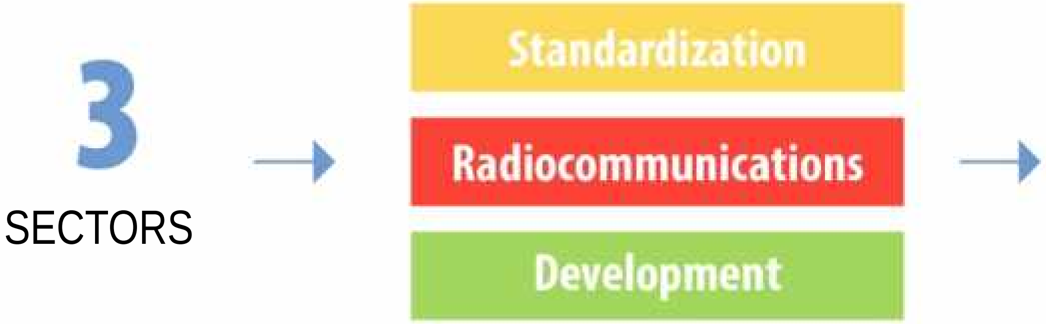
Coordinating radio spectrum and **assigning** orbital slots for satellites

Bridging the digital divide

Establishing global standards

WHO ARE WE?

Organization



3

SECTORS

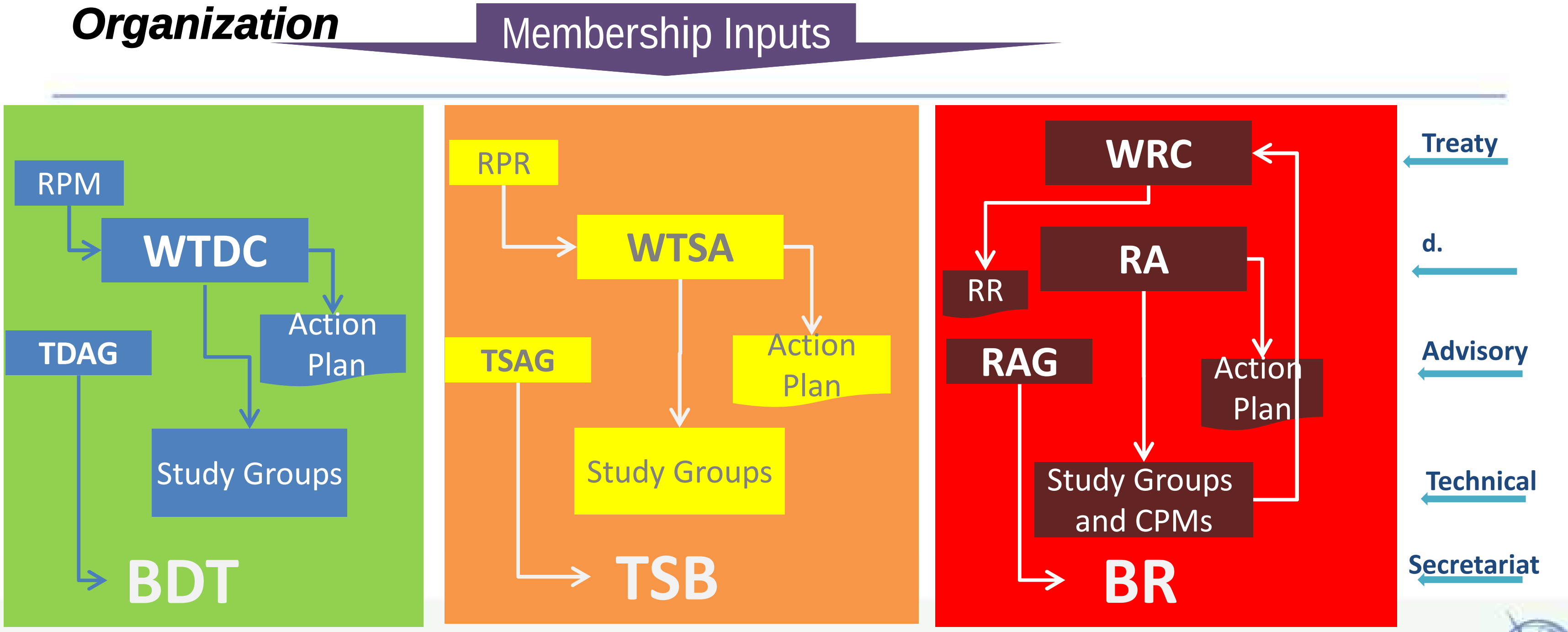
Standardization

Radiocommunications

Development

WHO ARE WE?

Organization



Membership Inputs

RPM

WTDC

Action Plan

TDAG

Study Groups

BDT

RPR

WTSA

Action Plan

TSAG

Study Groups

TSB

WRC

RR

RA

RAG

Action Plan

Study Groups and CPMs

BR

Treaty

d.

Advisory

Technical

Secretariat

IoT definition in the policy and regulatory context

Internet of things (IoT) [ITU-T Y.2060]: 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

NOTE 1 (from [ITU-T Y.2060]) – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

NOTE 2 (from [ITU-T Y.2060]) – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

Emerging ICT Infrastructure and Policy and Regulatory issues

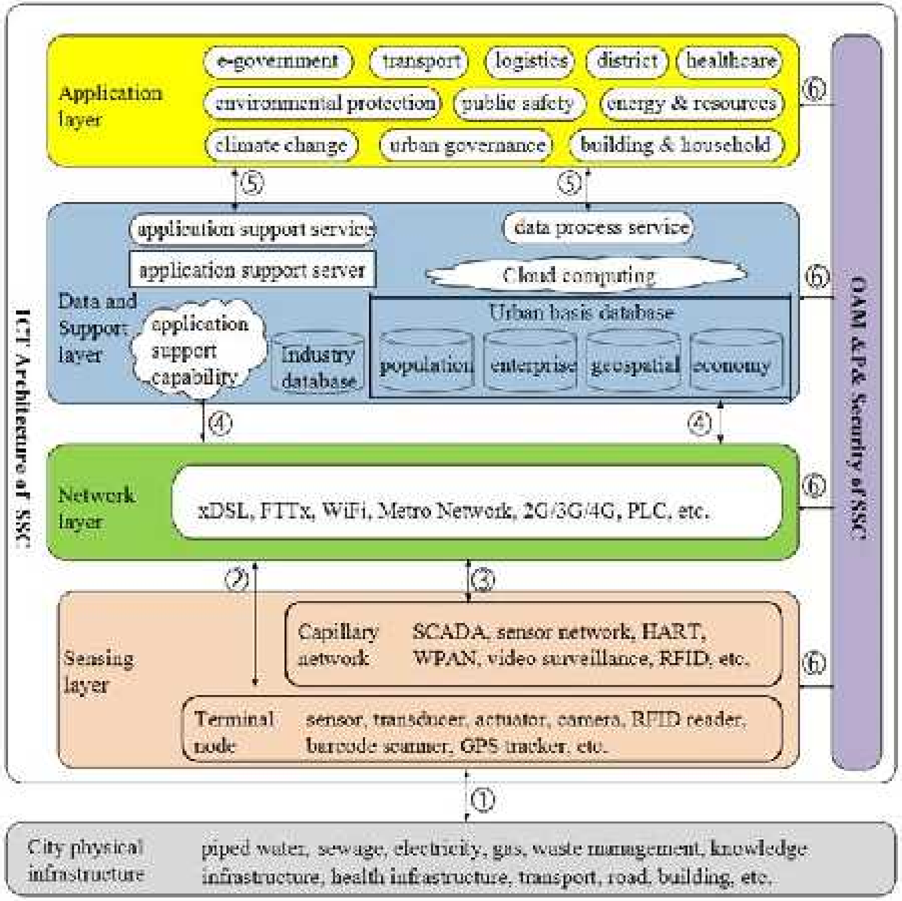
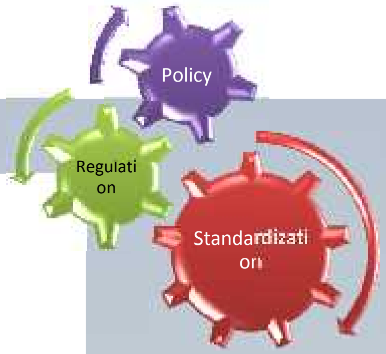

Application layer
e-government
transport
logistics
district
healthcare
environmental protection
public safety
energy & resources
climate change
urban governance
building & household
⑤
⑤
Data and Support layer
application support service
application support server
data process service
Cloud computing
application support capability
Industry database
Urban basis database
population
enterprise
geospatial
economy
④
④
Network layer
xDSL, FTTx, WiFi, Metro Network, 2G/3G/4G, PLC, etc.
②
③
Sensing layer
Capillary network
SCADA, sensor network, HART, WPAN, video surveillance, RFID, etc.
Terminal node
sensor, transducer, actuator, camera, RFID reader, barcode scanner, GPS tracker, etc.
①
City physical infrastructure
piped water, sewage, electricity, gas, waste management, knowledge infrastructure, health infrastructure, transport, road, building, etc.
⑥
⑥
⑥
⑥
ICT Architecture of SSC
OAM &P& Security of SSC

Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

A multi-tier SSC (smart sustainable city) ICT architecture from communication view (physical perspective)

Telecom/ ICT Sector Issues (examples)



Cross-Sector Collaboration

Competition

Investment

Licensing

Spectrum

HetNets

Broadband

Cloud

Roaming

Interoperability

QoS/QoE, Consumer

Numbering & Addressing

Big Data & Open Data

Security

Privacy

Right of Way

Infrastructure Sharing

Green ICTs

Data Centres

e-Waste

Number Portability

Emergency Telecommunications

Background

- In the IoT/M2M context as technologies enable deployment of IoTs **in general involves** the ICT sector policy makers and regulators (who are also going through a transformation otherwise)

- However, there are cases of standalone IoT use case for health, agriculture, finance that may not involve the ICT related policy maker and regulator.

- Furthermore in the context of IoTs some policy issues would have little or no ICT regulatory implication such as taxation, R&D, Innovation and incubation, inter-sector deployment, capacity building, test beds, pilot projects, inviting investments, ethical decision making that may be required in IoTs like autonomous cars, etc.

Background Contd.

- Policy issues driving IoT
  - Who would creating a policy for IoTs? ICT, Other sector, all?
  - Policy aspects that have ICT regulatory impact
  - Policy aspects that require other sectoral regulatory intervention
  - Policy aspects that need industry, academia , R&D
  - Policies that needs international cooperation (Standards, spectrum, inter border movement, international taxation, international resources, data protection, security and privacy)

- In this presentation, we concentrate on the IoT that involves the ICT sector policy maker and regulator while highlighting some of the issues related to international cooperation

Background Contd.

- Form the ICT policy maker and regulator point of view some of the challenges faced would be:
  - Licensing (new IoT aggregators, scope of license etc..)
  - Spectrum (regulation will change based on the service and also technology, e.g. Long range (NB-IOT, Sigfox, LoRA) Vs short range (RFID, Bluetooth, WiFi); It will also change based on the band used (free vs licensed)
  - Numbering and addressing (IoT identifier)
  - International roaming
  - Interoperability and Standards (Discussed in detail other sessions)
  - **Data protection**, privacy, consumer protection and **Security.**
  - Competition (platform competition, can the whole business or a smart city be treated as one customer reducing choice)
  - RoW: Use of Street furniture

  - Tariff regulation (e.g. long term pricing)
  - USO (coverage by PoP or coverage by geography, scope of USO fund)
  - Quality of Service and Quality of Experience

National Regulations

- There are many aspects of regulations that are national in nature Such as how to assign spectrum to telecommunication operators, decision to have national level licensing or region based licensing and many others

- Even national regulations have to be aligned to best practices to avoid issues such as cross border interference, technology neutrality, roaming, fee structure, etc

National Regulations

- Governments generally have lots of freedom in adopting national regulations.

- It is, however, always advisable to follow best practices. ITU has published many document that can be used to have an idea about best practices

Historic Perspective of ICT Regulation

- With the growth in Internet and availability of wireless broadband technologies paved the way for many new services
- The expectation and role of ICT was to change dramatically but generally regulations lagged behind the technologies
- Regulators are still coping with the issues related to Over The Top (OTT) services and the need to balance a new imbalance that has been where these traditional services provided by the telecommunication services provider

Historic Perspective of ICT Regulation

- Internet now a days is used provide all kind of services. This has led to convergence of some regulator specially the ICT and the Media Regulators.

- ICTs have now role including but not limited to Digital Financial Services, E-Health, E-Agriculture and even Transportation where services like Uber have been launched.

Historic Perspective of ICT Regulation

- ICT Regulations has in many ways become more complicated as there are issues related to security, privacy, data protection and even services that disrupt traditional services like Uber that had impacted the transportation sector and related jobs.

- Huge amount of data is generated by people and other connected devices. This data can be used to obtain useful information using Big Data Analytics and the decisions can be based on the analysis using Artificial Intelligence.

- These and others are known to be the components of the fourth industrial revolution that is based on the “cyber-physical” systems.

Historic Perspective of ICT Regulation

- The ICT or the converged regulator has to work with many other regulators and departments as well as the private sector. Thus the new era of regulations is called the collaborative regulations

- The role of the ICT regulator has become more of a facilitator, where on hand it still has to work on enhancing connectivity, while on the other hand it has to work with others to promote the use of ICTs in all the different areas like financial inclusion, health and agriculture.

Generations of Regulators

- 1G: Regulated Monopolies:
- 2G: Basic Reforms: De-Regulation
- **3G: Enabling Environment**
  - **Broadband**
  - **Spectrum Allocation for MBB**
- **4G: Integrated Regulations**
  - **Internet related issues**
  - **Light Touch Regulations**
- **5G: Collaborative Regulations**

5th Generation Regulations: Collaboration

- Services over the Internet
  - Health
  - Education
  - Agriculture
  - **Financial (Branchless Banking)**
  - Media
  - Smart Cities (IoT, Big Data Analytics)
  - Other (Taxi, Hotel, Job Portals, etc)

Collaborative Regulations

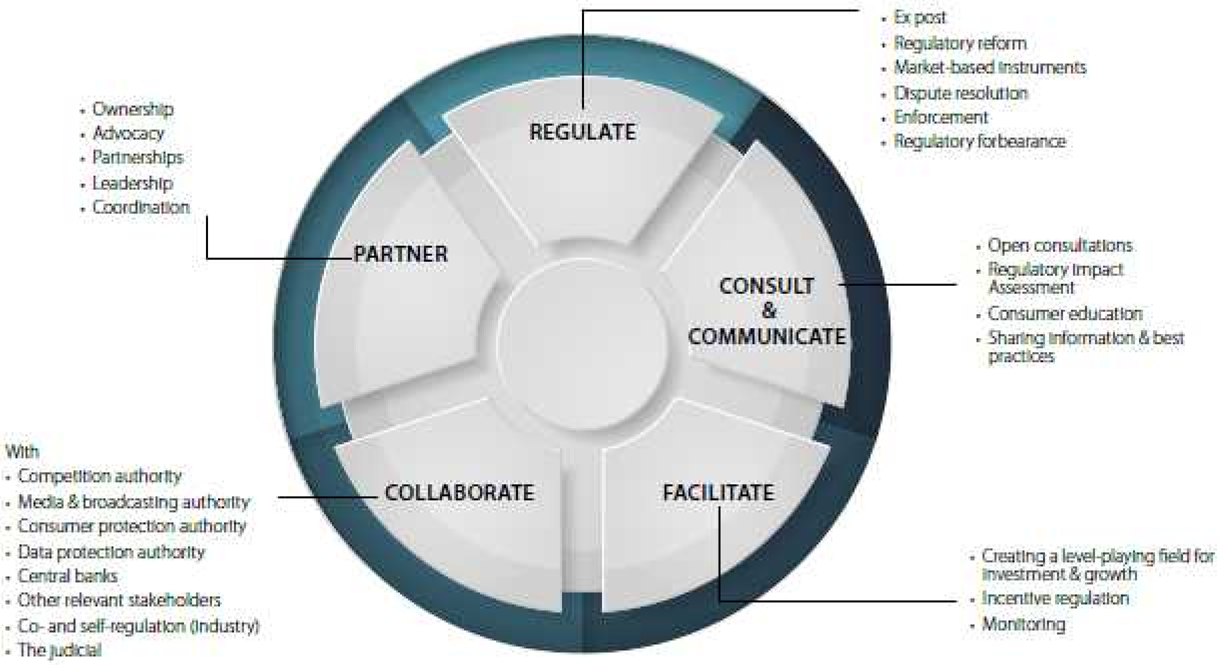


Figure 43:
THE WHEEL OF COLLABORATIVE REGULATION

Source: ITU.

Source: ITU

ICTs are multi-sectoral

Emergency

Education

Health

Agriculture

Governance

Investment

Applications

Policy & Regulation

Capacity Building

Transport

IoT, Sensor Networks

Universal Broadband

Green ICT & E-Waste

Measurements

Electricity

Privacy & Security

Infrastructure Security

Water

SMART SOCIETY

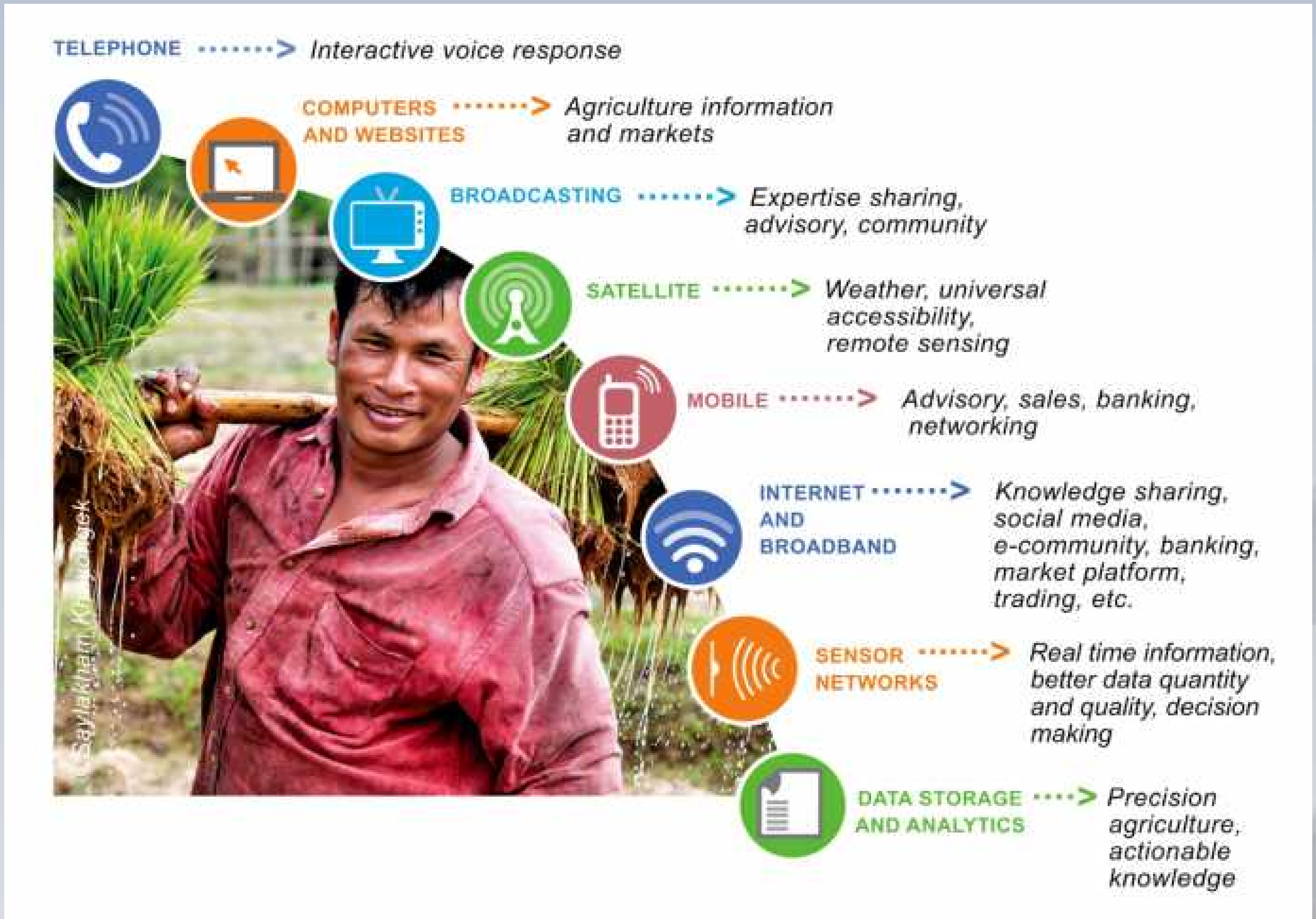
Digital Inclusion

Spectrum Management

Standards, Conformity & Interoperability

Finance

ICT and agriculture application trends



TELEPHONE → Interactive voice response

COMPUTERS AND WEBSITES → Agriculture information and markets

BROADCASTING → Expertise sharing, advisory, community

SATELLITE → Weather, universal accessibility, remote sensing

MOBILE → Advisory, sales, banking, networking

INTERNET AND BROADBAND → Knowledge sharing, social media, e-community, banking, market platform, trading, etc.

SENSOR NETWORKS → Real time information, better data quantity and quality, decision making

DATA STORAGE AND ANALYTICS → Precision agriculture, actionable knowledge

Source: FAO-ITU E-agriculture Strategy Guide

mHEALTH FOR NON-COMMUNICABLE DISEASES (NCDs) INITIATIVE
Cancers
Cardiovascular Diseases
Diabetes
Respiratory Diseases
BE HE@LTHY BE MOBILE
MOBILE TECHNOLOGY FOR A HEALTHY LIFE
1
2
3
4
5
6
7
8
9
*
0
#

Be He@lthy Be Mobile: Scaling up Digital Health Globally

www.who.int • mhealthfnccs.itu.int

A collaborative initiative between

World Health Organization

ITU

The toolkits

- mDiabetes
- mCessation
- mSmartlife
- mHypertension
- mCervicalCancer
- mAgeing
- mTuberculosis_Tobacco
- …….

"We should all w targ NCDs."

mHEALTH ENABLES PUBLIC HEALTH SERVICES TO

- existing infrastructure
- Scale up delivery of health programs cost effectively
- Reduce NCD prevalence
- Save costs on healthcare

Policy Framework to Enable IoT

- IoT is quite different from the general connectivity that the ICT regulators strive to enable

- In connecting people the "connectivity" is the main service, whereas in IoT it is the Application and related device and sensors

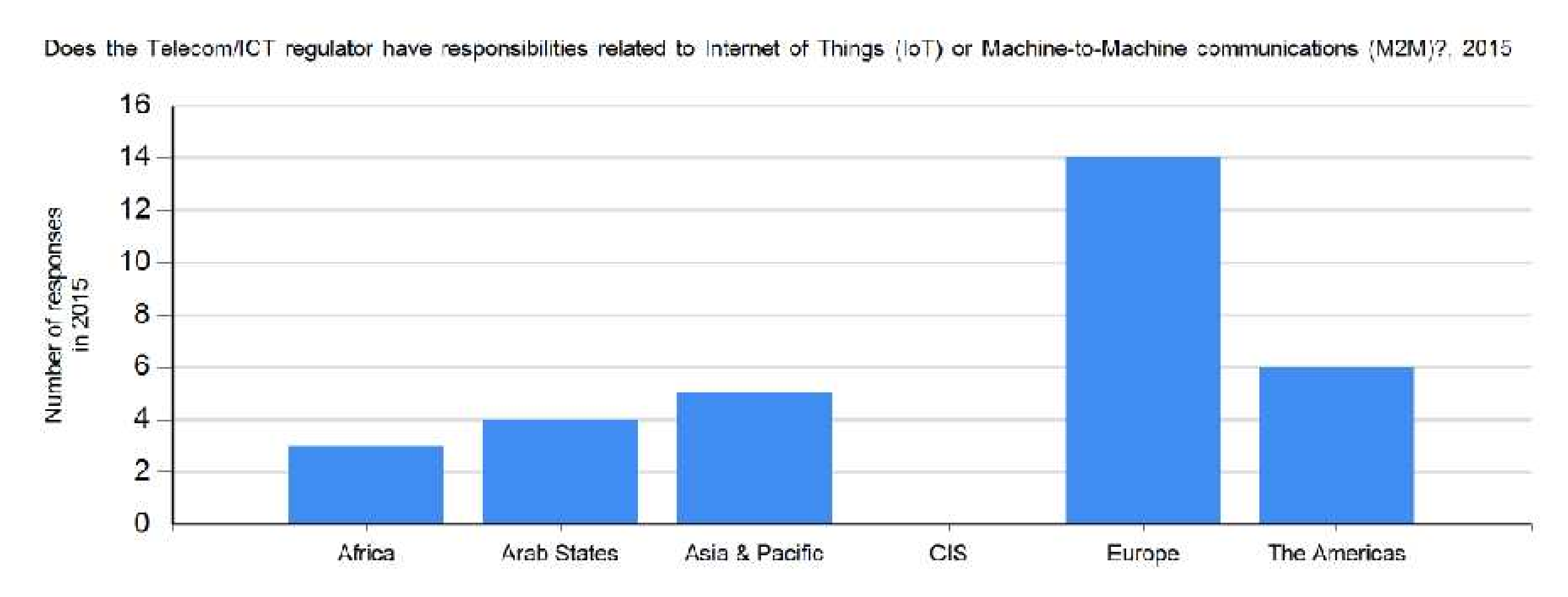
- Business models are different, so is the footprint

Policy Framework to Enable IoT

- The policies must address the previously unaddressed issues like privacy, data protection and security

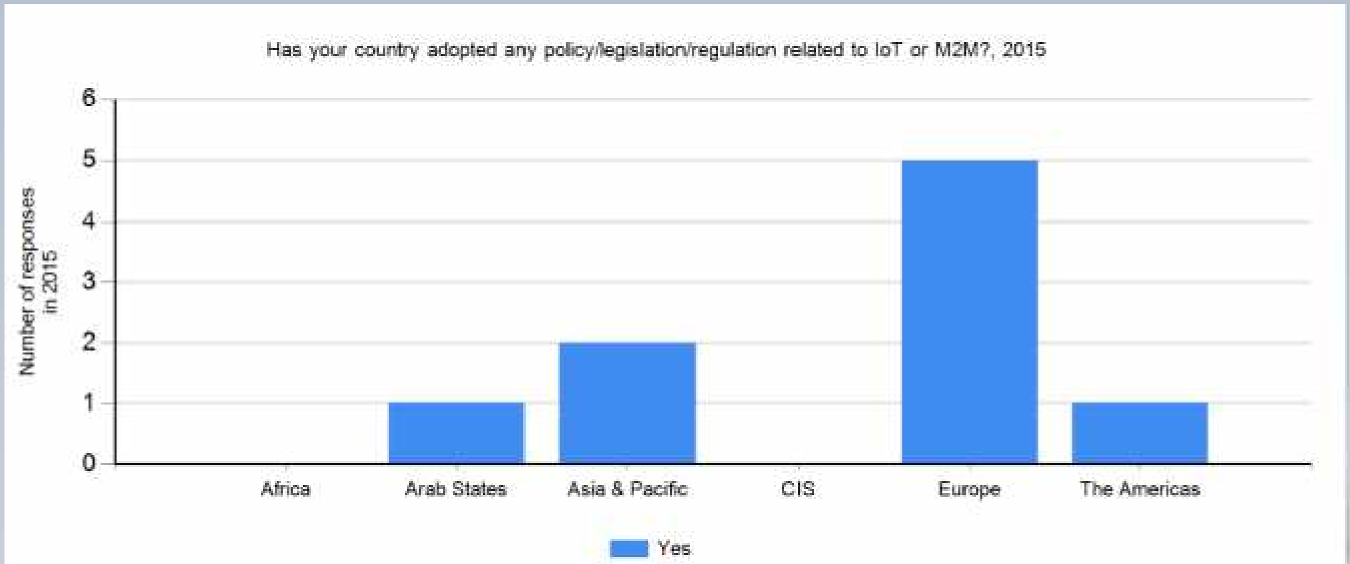
- Whereas some known issues such as spectrum allocation and licensing requires a re-work

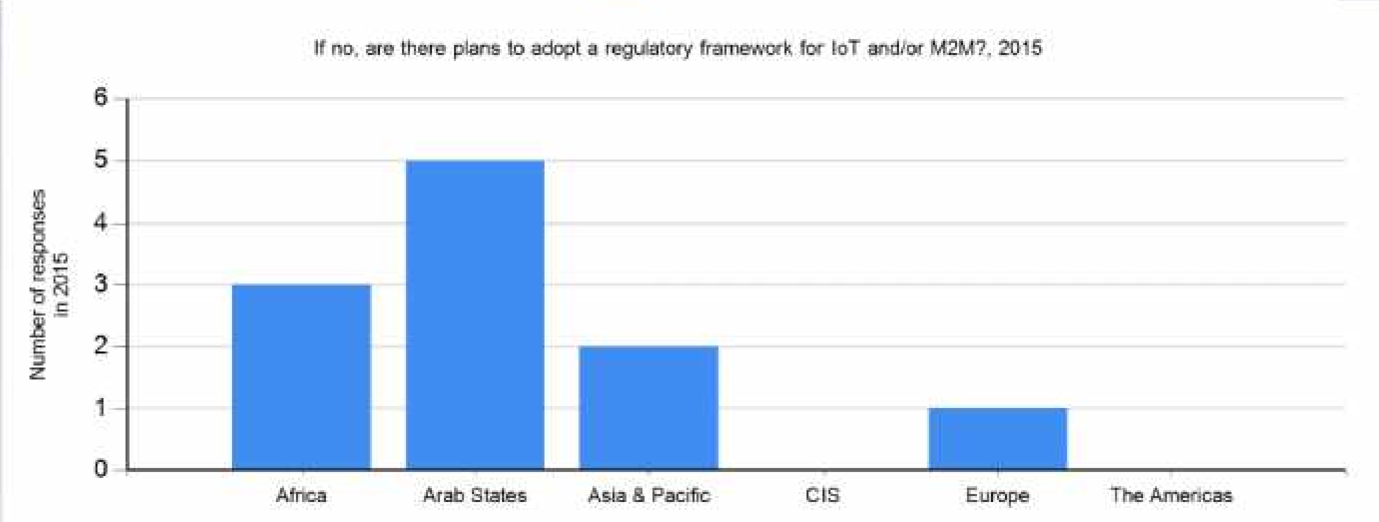
IoT AND REGULATORY AUTHORITY



Source: ITU World Telecommunication Regulatory Database

IoT policy and legislation


Has your country adopted any policy/legislation/regulation related to IoT or M2M?, 2015


If no, are there plans to adopt a regulatory framework for IoT and/or M2M?, 2015

Source: ITU World Telecommunication Regulatory Database

ITU-T Study Group 20: Internet of things (IoT) and smart cities and communities (SC&C)

Responsible for studies relating to IoT and its applications, and smart cities and communities (SC&C).

It includes studies relating to Big data aspects of IoT and SC&C, e-services and smart services for SC&C

Lead study group on

Internet of things (IoT) and its applications

Smart Cities and Communities (SC&C), including its e-services and smart services

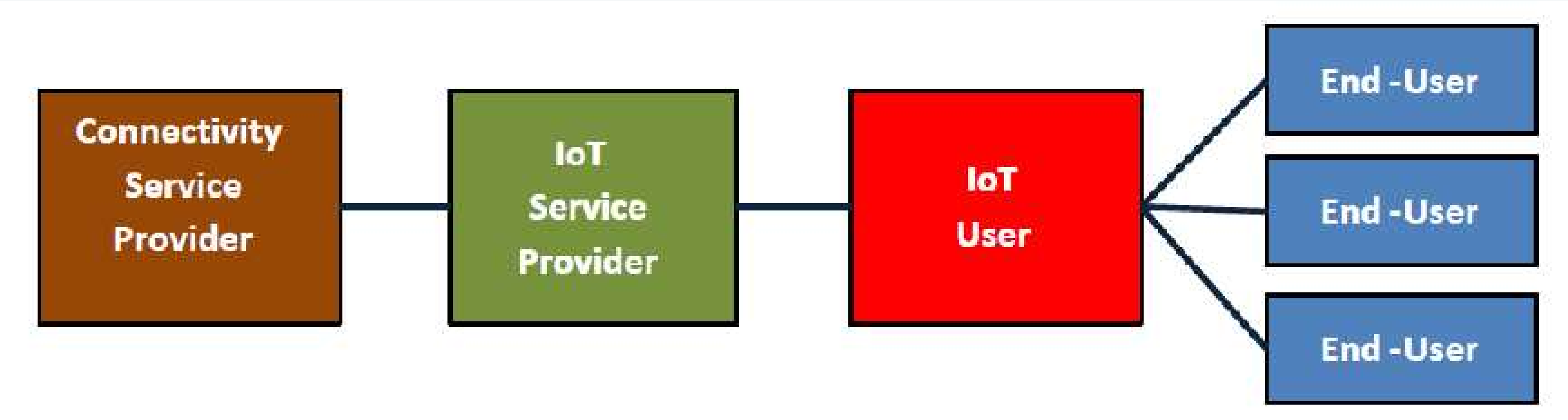
IoT identification

ITUACADEMY

ITU-T SG20 Structure

WP1/20	Questions
Q1/20	End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C
Q2/20	Requirements, capabilities, and use cases across verticals
Q3/20	Architectures, management, protocols and Quality of Service
Q4/20	e/Smart services, applications and supporting platforms
WP2/20	
Q5/20	Research and emerging technologies, terminology and definitions
Q6/20	Security, privacy, trust and identification
Q7/20	Evaluation and assessment of Smart Sustainable Cities and Communities

IOT Value Chain



Source: BEREC **Report “Enabling the Internet of Things”**12 February 2016

SERVICE LICENSING ISSUES

- A large number of countries still have service specific licensing framework
- What type of telecom service does the IoT provides?
- What about services that are cross-sectoral in character? Licensed Vs Non-licensed services
- How and to whom do the rights and obligations apply? Licensees, Resellers, Others…?

		Number of countries/economies						
		Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Authorization type *	Unified / Global License	9	3	5	0	0	8	25
	Multi service	1	0	3	0	0	1	5
	Multiservice individual license	4	2	6	3	5	4	24
	Service-specific individual license	20	11	13	4	9	18	75
	General Authorization (Class License)	4	4	4	0	20	4	36
	License Exempt	2	1	1	0	1	0	5
	Simple notification	1	0	0	2	9	0	12
Remarks		11	4	9	1	21	13	59
Region size		44	21	40	12	43	35	195

* This indicator allows multiple choice per country/economy

Source: ITU World Telecommunication/ICT Regulatory Database

ITU ICT-Eye: http://www.itu.int/icteye

INTEROPERABILITY AND STANDARDS

- IoTs have both public and proprietary standards currently
- Standardization is important for Interoperability, reducing costs and barriers to entry
  - ITU-T SG 20 (IoT and Smart Cities, Smart Communities)
  - National Standardization bodies
  - International Standardization bodies
- How to coordinate interoperability amongst public and private sector entities?
  - For example parking meters, thermostats, cardiac monitors, tires, roads, car components, supermarket shelves
- Cross-sectoral collaboration is very important as IoT are deployed in multiple sectors

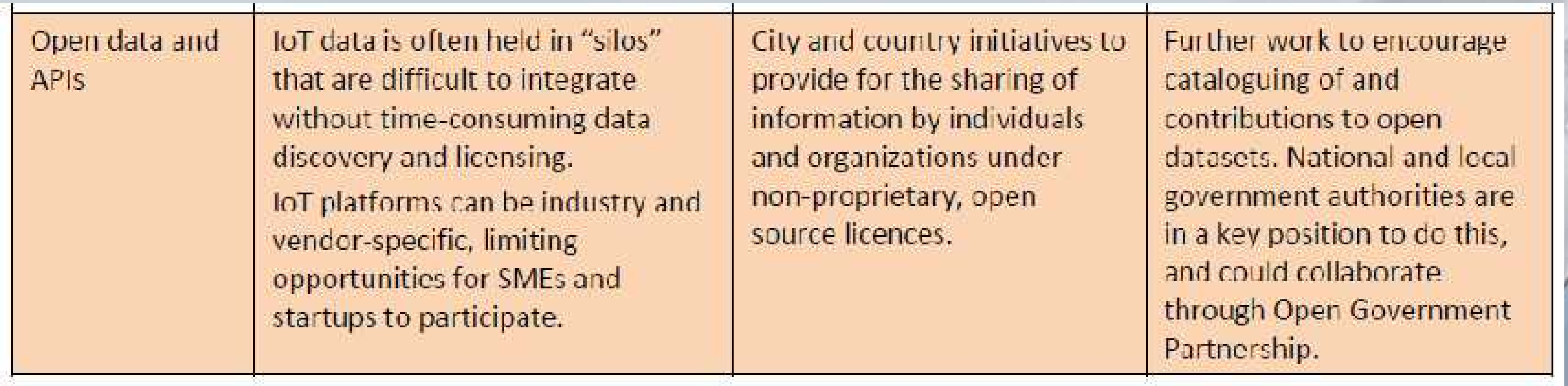
NUMBERING, ADDRESSING AND NUMBER PORTABILITY ISSUES

- Public Numbers
  - National E.164 numbers;
  - International/global E.164 numbers 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.
- Eligibility to receive MNCs
- Sufficiency of numbering resources
- IP addresses (IPv4 to IPv6 transition)
- MAC addresses
- How to switch the IoT devices when changing operators?
- OTA (Over-the-air) programming of SIMs

Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016,

PRIVACY AND SECURITY ISSUES

- Privacy Issues as in IoT environment, data is collected and shared automatically by devices, and some may be critical in nature
  - Data protection vs Open data
  - Applicable laws
  - Entity responsible for data protection
  - Who can have access to the data collected?
  - Data classification and processing
  - Consent of data owner?
  - National vs International collection and sharing of data
- Security of device and data
- Consumer protection
- IoT devices should follow a security and privacy “by design” approach



Open data and APIs	IoT data is often held in “silos” that are difficult to integrate without time-consuming data discovery and licensing. IoT platforms can be industry and vendor-specific, limiting opportunities for SMEs and startups to participate.	City and country initiatives to provide for the sharing of information by individuals and organizations under non-proprietary, open source licences.	Further work to encourage cataloguing of and contributions to open datasets. National and local government authorities are in a key position to do this, and could collaborate through Open Government Partnership.

PRIVACY AND SECURITY ISSUES: Potential regulatory measures

- R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems

- Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn.

- Greater use of Privacy Impact Assessments by organizations building and configuring IoT systems.

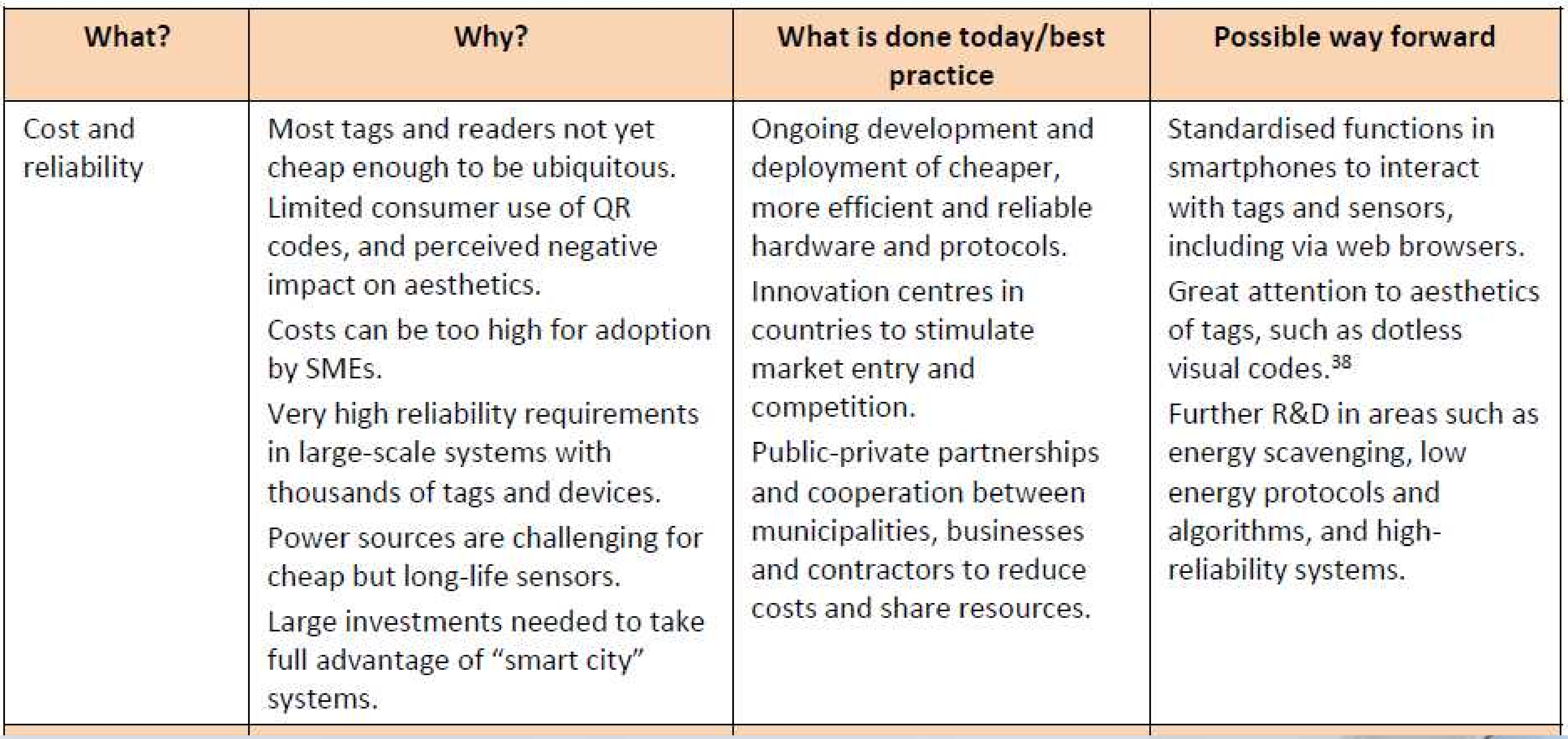
- More cooperation between telecoms and other regulators such as privacy/data protection agencies.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015**

COMPETITION ISSUES

- Licensed Vs Non Licensed services
- Area of license
- OTT
- Net Neutrality
- Infrastructure sharing
- Access to data and open IoT platforms
- Data analytics
- Customer lock-in
- Mobile data roaming
- Consumer protection
- Quality of Service

COST AND RELIABILITY



What?	Why?	What is done today/best practice	Possible way forward
Cost and reliability	Most tags and readers not yet cheap enough to be ubiquitous. Limited consumer use of QR codes, and perceived negative impact on aesthetics. Costs can be too high for adoption by SMEs. Very high reliability requirements in large-scale systems with thousands of tags and devices. Power sources are challenging for cheap but long-life sensors. Large investments needed to take full advantage of "smart city" systems.	Ongoing development and deployment of cheaper, more efficient and reliable hardware and protocols. Innovation centres in countries to stimulate market entry and competition. Public-private partnerships and cooperation between municipalities, businesses and contractors to reduce costs and share resources.	Standardised functions in smartphones to interact with tags and sensors, including via web browsers. Great attention to aesthetics of tags, such as dotless visual codes.[38] Further R&D in areas such as energy scavenging, low energy protocols and algorithms, and high-reliability systems.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015, Prof. Ian Brown**

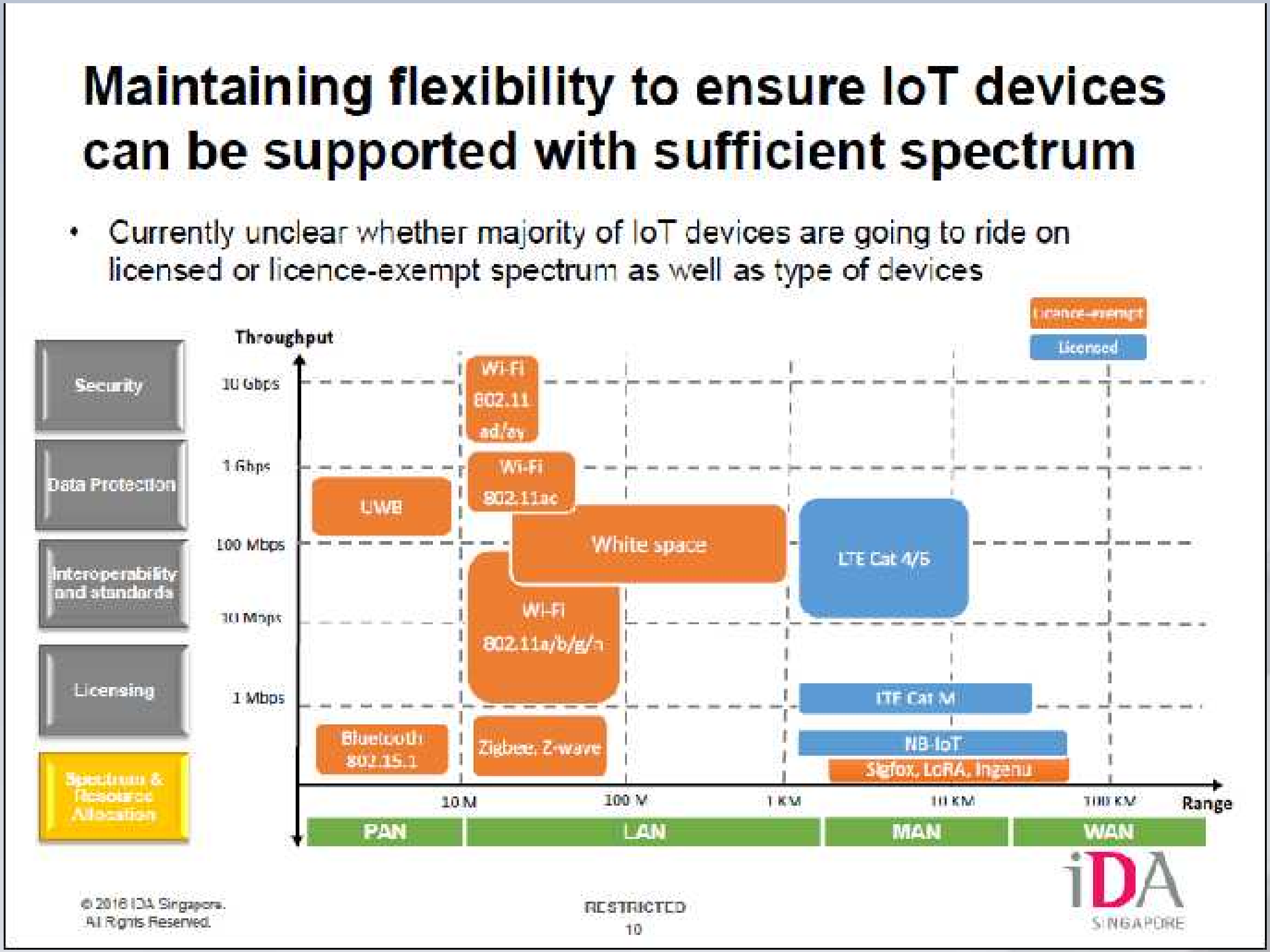
Spectrum Requirement for IoT

- **In many cases IoT devices need to use Wireless Technologies**
- **Diversity of IoT application requirements:**
  - Varying bandwidth requirements (how much information is sent)
  - Long-range vs short-range
  - Long battery life
  - Various QoS requirements

IoTs and cloud technologies and are the two unstoppable forces promoting digital capabilities

Spectrum needs to be made available in a range of frequency bands to cater for various cases

Example from Singapore



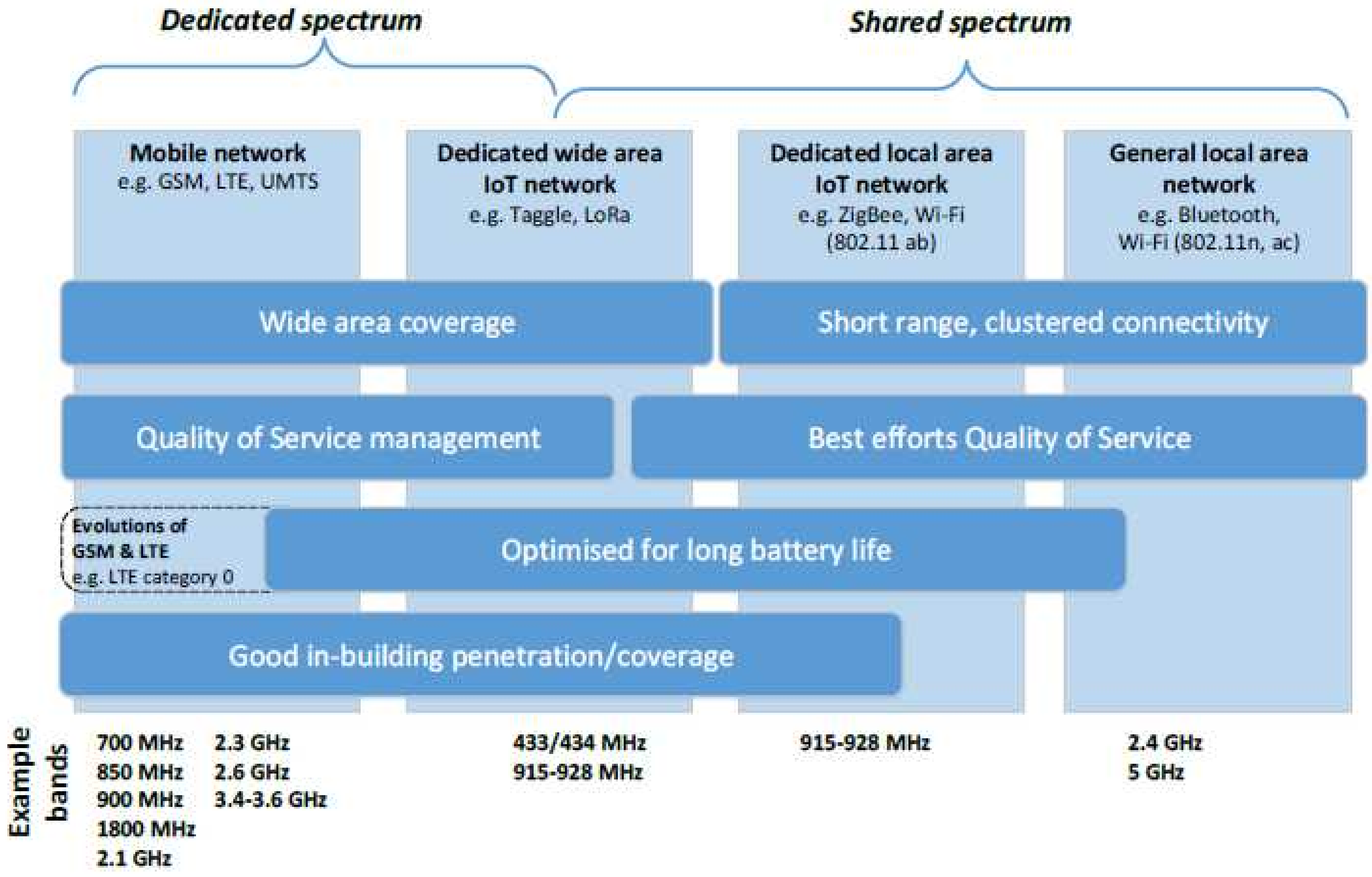
Maintaining flexibility to ensure IoT devices can be supported with sufficient spectrum

- Currently unclear whether majority of IoT devices are going to ride on licensed or licence-exempt spectrum as well as type of devices

RESTRICTED

Example from Australia

Figure 2: Spectrum identified for IoT applications



Dedicated spectrum

Shared spectrum

Mobile network
e.g. GSM, LTE, UMTS

Dedicated wide area IoT network
e.g. Taggle, LoRa

Dedicated local area IoT network
e.g. ZigBee, Wi-Fi (802.11 ab)

General local area network
e.g. Bluetooth, Wi-Fi (802.11n, ac)

Wide area coverage

Short range, clustered connectivity

Quality of Service management

Best efforts Quality of Service

Evolutions of GSM & LTE
e.g. LTE category 0

Optimised for long battery life

Good in-building penetration/coverage

Example bands

700 MHz
850 MHz
900 MHz
1800 MHz
2.1 GHz
2.3 GHz
2.6 GHz
3.4-3.6 GHz

433/434 MHz
915-928 MHz

915-928 MHz

2.4 GHz
5 GHz

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

Source: The Internet of Things and the ACMA's areas of focus Emerging issues in media and communications Occasional paper, Nov 2015

IoT Addressing

- IoT devices may have a globally unique and routable communications address
- This will require a very large protocol address space
- Thus allowing limited inter-network connectivity; or make use of local networks only to share data with and receive instructions from a nearby controller.

IoT Addressing

- In some cases these devices can be a computer, smartphone, or specialized management device – in which case a globally-unique address is not required

- Enabling peer-to-peer connections between devices can increase the reliability of communications, compared to requiring a large and complex global network

- This matches the common use case of an individual discovering and interacting with nearby devices.

IoT Addressing

- However when devices must be globally reachable – most likely, via the Internet, a large space is required to individually identify each IoT
- The number of unallocated addresses for the current version of the Internet Protocol (IPv4) is extremely limited, but the new version (IPv6) being rolled out by ISPs around the world has enough addresses for almost any conceivable number of devices.
- The transition from IPv4 to IPv6 has taken longer than expected, and policy makers may need to continue with programmes to encourage the transition in the medium term.

IoT Addressing

- The US government example, set up a Federal IPv6 Task Force to move all federal agencies from IPv4 to IPv6, with one aim being to encourage the private sector to do the same. Many other countries have also set up IPv6 Task Forces to encourage national transitions

- For any IoT identification scheme, there will be trade-offs between performance, scalability, interoperability, efficiency, privacy preservation, ease of authentication, reliability, flexibility, extensibility, and mobility support.

IoT Addressing

- Beside the IPv6 addresses system, the other main identification standards being developed are from ISO and GS1, as well as ITU-T Recommendation E.212 for the use of the International Mobile Subscriber Identifier (IMSI) for machine-to-machine communications

- The latter has the advantage of a well-developed authentication, payment and global roaming framework, operated by mobile telephony providers, with hardware security based on SIMs

IoT roaming

- The term roaming is usually used in the context of cellular communication

- IoTs on the other hand are based on several different technologies. In fact the IoT based on cellular technologies would be a small portion of the total IoT market. The IoTs may also be agnostic of the technology that is used at the physical layer.

- The technology agnostic part will be specially significant once we have complete implementation of IPv6

IoT Roaming: Cellular

- In general many National Regulatory Authority at this point in time are working on or have regulations related to cellular technology based IoTs

- These IoTs may have a regular SIM card or may have an embedded SIM

- There is a need to look at the issue of roaming in a more comprehensive manner in general context of regulations related to IoTs

IoT Roaming: Other Technologies

- Technologies other than cellular technologies, like LoRa, Sigfox networks may also require similar roaming agreements

- This may require agreements between Sigfox or LoRa network operators

- Such time of roaming for the time being has not caught the attention of regulators but with may require handling in the future.

Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016

Regulation on street furniture usage where IoT devices

- The Street furniture is usually the property or under control of the local administration

- Even in presence of a National Policy related to Infrastructure, the local government may have there own policy, rules and regulations

- As an example, the council in Milton Keynes came up with their own Telecommunication Policy that among many other factors also considered the environmental impacts

Source: Telecommunication Systems Policy, Council of Milton Keynes

Infrastructure Sharing

- In telecommunication infrastructure sharing is becoming very popular because of its environmental impact and cost savings

- The use of street furniture for IoTs can be considered as an extension of this policy albeit across several stakeholders

- In fact this use of furniture may not only be for IoT but for providing broadband services to the people and in the longer run for 5G services, where IoT will just be one part

Use of Street Furniture

- In general it is usually considered a given that street furniture will be used for IoT

- However, the regulations are in this regard are unclear

- More precisely, the exact jurisdiction is blurry

Use of Street Furniture

- Delivering extensive coverage at high data speeds and with robust reliability, with each operator running a separate network, would require vast levels of investment

- There must be an increased role for infrastructure sharing, not only to reduce the costs of network deployment where possible.

Source: National Infrastructure Commission of UK report | Connected Future

Use of Street Furniture

- The networks of the future must make the best use of the limited supporting infrastructure such as street furniture in the towns and cities
- Any regulation of network infrastructure should seek to be supportive of this sharing, whilst ensuring competition and fair access are maintained.

Source: National Infrastructure Commission of UK report | Connected Future

Use of Street Furniture: Example

- A notable feature of small cell densification and IoT will be the need for access to street furniture.

- This will require collaboration between network operators and landlords (generally local authorities) to handle agreements and issues that might occur due to deploying telecommunications equipment on infrastructure not designed for that purpose

- There is currently no common approach to this type of collaboration, though pioneering Smart cities projects such as Bristol is Open and collaborations between forward thinking authorities such as Aberdeen Council and network providers will offer valuable insight into how best to drive network provision

Source: National Infrastructure Commission of UK report | Connected Future

General regulatory issues around data

General Regulatory Issues around Data

- Now-a-days not only IoT collect data but many other platforms (e.g., social media) collect data

- At times the collected data is shared without the knowledge of the users (or the user has naively given the permission in order to subscribe to a certain service).

- Data is stolen from these platforms

- Many countries in the world are trying to come up with regulations to protect user data

General Regulatory Issues around Data

- Many Countries and regions still have no grasp of the issue and do not have any specific regulations or in some cases they have very old regulations that are too restrictive

- Following are some of the principles that need to be adhered to when regulations are laws and regulations are promulgated
  - Data protection vs Open data
  - Entity responsible for data protection
  - Who can have access to the data collected?
  - Data classification and processing
  - Consent of data owner?
  - National vs International collection and sharing of data
  - Consumer protection

Potential Regulatory Measures

- Incentives for companies to develop new mechanisms for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn.

- Greater use of Privacy Impact Assessments by specialized organizations

- Development of further guidance from global privacy regulators on application of the principles of data minimization

- More cooperation between telecoms and other regulators such as privacy/data protection agencies.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015**

Regulatory issues around data

- Different Regions and even individual countries in the same region deal with data issues differently

- The main problem stem from the fact that most of the ICT regulator have evolved from regulating the Telecommunication sector.

- The telecommunication services were and are licensed services and the regulators through license conditions used to impose restriction on use of consumer data

Regulatory issues around data

- The main data used to be the Call Detail Record (CDR) and the subscriber antecedents. The Telecommunication companies had the data and they were suppose to keep it safe
- However, with the increase in the availability of mobile broadband, smart phones equipped with a GPS receiver, different applications have been launched by many companies and are providing different kind of services. These are generally called Over the Top (OTT) Services
- These OTT services collect lots of user and then there are data breaches etc

Regulatory issues around data

- Some countries have a established a separate entity for Data Protection

- ICT Regulator still maintain some control over how data should be shared

- The main issues faced are as follows:
  - With whom and how (e.g. anonymization) data should be shared
  - What kind of data has to remain within the geographical boundaries and which can reside outside the country

Regulatory issues around data

- The data generation by the users has enhanced many folds

- This data can be used in the decision making process for many applications both in the private as well as the government sector.

- New technologies are like IoTs has the potential to generate even more data then people can

- Technologies like Cloud computing, do require data to be placed at different locations that may be out side the geographical boundaries of a country.

Regulatory issues around data

- Large amount of data can only be used through big data analytics again requiring the use of cloud computing
- These analysis are required in artificial intelligence
- Therefore, there is a need to have least restrictive regulations around data sharing

Regulations around Data in Asia

- As pointed out earlier Data regulations are at different stages even within the same region

- In general the regulations are more advanced in countries that are doing well in general in the ICT sector. For example in Singapore, the main law on this issue is the Personal Data Protection Act 2012. It is quite comprehensive and covers many different aspects.

- On the other hand, in Vietnam there is no unified law regulating data privacy

Regulations around Data in the United States

- In the United States, the privacy and security of personal data is governed by a wide range of federal and state laws
- At the highest level, the Fourth Amendment to the United States Constitution protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures
- In the regulatory sector, multiple federal agencies enforce various privacy laws tailored to specific industries, or types and uses of information.

Source: Data protection regulations and international data flows: Implications for trade and development, United Nations Conference on Trade and Development (UNCTAD) Report, 2016

Regulations around Data in the United States

- These laws include but not limited to health information, financial information, educational records, children's information, and governmental use of personal data

- The regulatory agencies tasked with their enforcement include but not limited to the Federal Trade Commission (FTC), the U.S. Department of Health and Human Services (HSS), the Consumer Financial Protection Bureau (CFPB), and the Federal Communications Commission (FCC). There are also state level agencies, including State Attorneys general, that enforces state privacy laws.

Source: Data protection regulations and international data flows: Implications for trade and development, United Nations Conference on Trade and Development (UNCTAD) Report, 2016

Regulations around Data in the European Union

- The main regulation in the EU is the General Data Protection Regulation (GDPR)

- The GDPR provides for a uniform and simplified legislative framework

- It will establish one single pan-European set of rules that will make it simpler and cheaper for companies to do business in the EU

Regulations around Data in the European Union

- The GDPR envisages that
  - the rights of individuals are more effectively protected across the continent
  - consistency of interpretation of the new rules be guaranteed
  - in cross-border cases where several national data protection authorities are involved, a single supervisory decision is adopted

Adequacy Approach of GDPR

- The 'adequacy' approach (sometimes known as a whitelist approach) assesses whether an entire target jurisdiction provides a sufficient degree of protection for the transfer of personal data

- This approach is used by a variety of countries, including the members of the European Union (EU), Israel, Japan and Switzerland

EU and the United States

- The European Union and the United States have re-negotiated a long standing cross-border data protection agreement

- It used to be called the EU-US Safe Harbor Frameworks, now to be known as the EU-US Privacy Shield

EU and the United States

- The EU-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission

- The objective was to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce

Source: https://www.privacyshield.gov/Program-Overview

The Privacy Shield Model

- The Privacy shield model has been followed elsewhere also

- For example, Switzerland and Israel both publish lists of jurisdictions where data can be sent because their laws have been approved as adequate.

Data regulation and data protection laws specifically pertinent to the IoTs

- In general, all the general data protection regulations are also applied to IoTs

- There may be additional requirements for IoTs

- As an example and a case study, this issue is considered in light if the European Union’s General Data Protection Regulation ("GDPR") is presented

GPDR and IoT

- The data protection issues arising from the IoT were considered in an opinion of the Article 29 Data Protection Working Party issued in 2014

- This data protection related to the IoT was considered because its great potential and the fact that it can generate extensive data.

- This has given rise to the concern that the expansion of the IoT could pose significant data protection and personal privacy risks and challenges

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

1. Security Breaches

- One of the principal privacy concerns that have been expressed in relation to IoT devices is that they provide soft targets for hackers and are susceptible to security breaches

- The GDPR introduces a general mandatory notification regime in the event of personal data breaches

- Data controllers will be required to report personal data breaches to their supervisory authority no later than 72 hours after becoming aware of such breach

- In some cases, they will also be required to report such breaches to affected individuals. Data controllers using the IOT will need to ensure that they are in a position to identify and react to security breaches in a manner which complies with the requirements of the GDPR.

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

2. Consent

- Doubt has been expressed about the ability of IoT devices, even under the existing EU data protection regime, to obtain consent of sufficient quality from users of such devices in relation to data processing activities

- The GDPR has requirements in relation to data subject consent, requiring data controllers to demonstrate consent has been given by way of a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data

- The GDPR provides that consent cannot be presumed through the inaction of the data subject and that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

3. Privacy by design and privacy by default

- Privacy by design and privacy by default are concepts which exist in current data protection legislation in the GDPR

- It imposes obligations on data controllers to adopt significant new technical and organisational measures to demonstrate their compliance with the requirements of the GDPR

- These may include conducting **data protection impact assessments** in certain circumstances which are likely to arise in connection with IoT systems.

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

4. Enhanced data subject rights

- The GDPR gives new substantive rights on data subjects in relation to their personal data. These substantive rights include an express right to be forgotten, data portability rights and the right to object to automated decision making

- Thought will need to be given in the design of IoT devices, applications and systems as to whether the necessary capabilities have been built-in to facilitate the exercise of these data subject rights in compliance with the GDPR, particularly in relation to data portability.

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

5. Processing Personal Data relating to children

- The GDPR makes it impossible for children under the age of 13 to consent on their own behalf to the processing of their personal data in relation to online services
- For children between the ages of 13 and 15 (inclusive), the position will depend on legislation in each Member State (although the default position will be that children between those ages will not be able to give consent on their own behalf)
- These provisions pose challenges for those intending to bring to market IoT devices that may be used by children, both in relation to the feasibility of introducing parental/guardian consent mechanisms to the devices and in relation to the ability to market such devices at an EU-wide level, given that the law relating to children between 13 and 15 may not be uniform across all Member States

Source: GDPR and the Internet of Things: 5 Things You Need to Know:

Conclusions

- Policies and regulations related to IoT are still n the developmental stage and spread across sectors.
  - Licensing (new IoT aggregators, scope of license)
  - Spectrum (regulation will change based on the service and also technology, e.g. Long range (NB-IOT, Sigfox, LoRA) Vs short range (RFID, Bluetooth, WiFi); It will also change based on the band used (free vs licensed)
  - Numbering and addressing (IoT identifier)
  - International roaming
  - Interoperability and Standards
  - **Data protection**, privacy, consumer protection and **Security.**
  - Competition (platform competition, can the whole business or a smart city be treated as one customer reducing choice)
  - RoW: Use of Street furniture

- In this presentation we mainly discussed policies and regulations from the point of view of an ICT policy maker and regulator. However, a holistic view may be required.

Future Issues

- **Data Ownership**
- **Rights around derivative use of data**
- **Dynamic decision rights (change in consent)**
- **Consumer awareness**
- **Privacy rights**
- **De-aggregation standards for data privacy**
- **Cybersecurity**
- **Liability (decision made by AI: health, transportation)**
- **Reliability and accuracy standards**
- **Trustworthiness (Like in financial services)**
- **Public profit sharing**
- **Preventing oligopolies (Large tech companies taking over)**
- **Education**
- **Fairness (Some may not be able to afford)**
- **Disposal of electronic waste**

Source: Dr. Shoumen Datta of Massachusetts Institute of Technology (MIT)

Thank You

E-mail: ismail.shah@itu.int