Global ICT Regulatory Outlook 2018

Global ICT Regulatory Outlook 2018

...a unique and powerful annual report that
shines a light on the challenges and
opportunities of the digital economy – and how
collaborative regulation can shape it to benefit
all humanity.

The views expressed in this report are those of the authors and do not necessarily reflect the opinions of ITU Membership.

2018 ITU International Telecommunication Union
Place des Nations CH-1211 Geneva Switzerland

Table of contents

List of tables, figures and boxes

Tables

Figures

Boxes

Foreword

Regulation has entered a new age. The days when regulators dealt with purely technological changes – such as the analogue to digital transition – are over. Today, digital transformation is sweeping across whole economies, changing our outlook forever. As mobile phones have become even more ubiquitous in their coverage and use, they have also become portals to a host of online services. Regulators find themselves grappling with an ever-growing array of challenges associated across different sectors – including digital identity, data protection, blockchain and Artificial Intelligence (AI).

Regulation continues to evolve rapidly. Far from 'falling behind' or trying to 'catch up', I have seen first-hand the earnest efforts of governments and policy-makers to monitor, benchmark and understand the impact of digital transformation. ITU stands ready to support its membership, including regulators and policy-makers, in understanding and navigating these changes and in meeting the challenges they bring.

It has also become increasingly clear that policy-makers and regulators can work together as well as with other stakeholders to shape our common future in ways that make the most of the benefits of digital technologies, while safeguarding and protecting consumers. It is in this spirit that ITU has developed the key concepts of 'collaborative regulation' and 'fifth generation' regulation to describe how policy-makers and regulators can remain effective in the fast-evolving digital markets of today and tomorrow. Their actions will help improve people's lives around the world and help achieve the Sustainable Development Goals (SDGs).

The Global ICT Regulatory Outlook 2018 benchmarks regulatory progress worldwide, and, building on the 2017 edition, represents a significant achievement. Feedback on the previous edition shows that regulators, policy-makers and others found the publication a useful tool in forging meaningful, regulatory change. The trends identified in this year's edition will dominate 2019 and beyond. We are now casting the net more widely in addressing regulatory frontiers in this year's report, in the hope that more stakeholders in the regulatory debate will find valuable solutions and constructive means to engage as they chart holistic and progressive policies.

I am confident that this report will support regulators in furthering their collaboration and will help all of us to focus on achieving the goals of growth and development, while leaving no one behind.

Brahima Sanou,
Director, Telecommunication Development Bureau

Acronyms

5GIA	5G Infrastructure Association
ACCC	Australian Competition and Consumer Commission
AI	Artificial Intelligence
AIP	Administrative Incentive Pricing
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes
AU	African Union
AV	Autonomous Vehicle
BAZ	Broadcasting Authority of Zimbabwe
BDT	Telecommunication Development Bureau
BEPS	Base Erosion and Profit Shifting
BEREC	Body of European Regulators for Electronic Communications
CAPEX	Capital Expenditure
CAV	Connected Autonomous Vehicle
CDN	Content Distribution Network
CIS	Commonwealth of Independent States
CNIL	Commission Nationale de l'Informatique et des Libertés
COE	Council of Europe
CRASA	Communications Regulators' Association of Southern Africa
CTO	Commonwealth Telecommunications Organisation
DAU	Daily Active Users
DCRAI	Digital Communications Regulatory Authority of India
DFS	Digital Financial Inclusion
DPIA	Data Protection Impact Assessment
DTT	Digital Terrestrial Television
EC	European Commission
ECTA	European Competitive Telecommunications Association
EoI	Equivalence of Inputs
eMBB	Enhanced Mobile Broadband
EU	European Union
FCC	Federal Communications Commission
FTA	Free Trade Agreement
FTC	Federal Trade Commission
FTTH	Fibre to the Home
FTTx	Fibre to the x
FUTEBOL	Federated Union of Telecommunications Research Facilities for an EU-Brazil Open Laboratory
GATS	General Agreement on Trade in Services
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation

GIS	Geographic Information System
GSMA	GSM Association
GSR	Global Symposium for Regulators
GST	Goods and Services Tax
HTS	High-Throughput Satellite
ICT	Information and Communication Technology
IDC	International Data Corporation
IEPS	Impuesto Especial sobre Producción y Servicios
IFER	Imposition forfaitaire pour les entreprises de réseaux
IoT	Internet of Things
IMT	International Mobile Telecommunications
IP	Intellectual Property
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Standardization Sector
LDC	Least Developed Country
LLU	Local Loop Unbundling
M2M	Machine-to-Machine
MAAL	Multinational Anti-Avoidance Law
MAU	Monthly Active Users
MENA	Middle East North Africa
mMTC	Massive Machine-Type Communications
MIMO	Multiple-Input and Multiple-Output
MNOs	Mobile Network Operator
MoF	Ministry of Finance
MoU	Memorandum of Understanding
MVNO	Mobile Virtual Network Operator
NAFTA	North America Free Trade Agreement
NBTC	National Broadcasting and Telecommunications Commission
NGSO	Non-Geostationary Satellite Orbit
Nkom	Norwegian Communications Authority
NRA	National Regulatory Authority
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Co-operation and Development
OTT	Over-the-Top
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PPDR	Public Protection and Disaster Relief
PPPs	Public-Private Partnerships
PTA	Preferential Trade Agreement
QoS/E	Quality of Service and Experience

RIA	Regulatory Impact Assessment	UAE	United Arab Emirates
RUTEL	Redevance d'Utilisation des Services de Télécommunications	UAS	Universal Access and Service
SAFTA	Singapore-Australia Agreement Free Trade Agreement	UK	United Kingdom
		UNCTAD	UN Conference on Trade and Development
SDGs	Sustainable Development Goals	URLLC	Ultra-Reliable and Low-Latency Communications
SME	Small- and Medium-sized Enterprises	US	United States
SMP	Significant Market Power	USF	Universal Service Fund
TDLC	Tribunal de Defensa de la Libre Competencia	USO	Universal Service Obligation
TPP	Trans-Pacific Partnership	VAT	Value-Added Tax
TRA	Telecom Regulatory Authority	VOIP	Voice-over-IP
TRAI	Telecom Regulatory Authority of India	WBA	Wholesale Broadband Access
TSM	Telecom Single Market	WRC	World Radiocommunication Conference

Introduction

This edition of the Global ICT Regulatory Outlook builds on its predecessor first edition. New this year is unique evidence from around the world charting the evolution of policy and regulation in ICTs and, by extension, in the digital economy.

This is an exciting time for regulators – and what they need more than ever, is detailed evidence to support their decision-making, enabling them to lead the way in digital transformation with confidence.

This report is based on inputs from 190 countries and offers an objective/neutral perspective on the latest trends driving ICT policy and regulation. Regulatory topics are explored through factual graphic analysis and complemented by country experiences. This powerful combination enables us to decipher complex, multi-faceted issues and make sense of the rich body of regulatory experience from all regions. While some findings are intuitive, others offer surprises.

One overriding strength of the report – and a source of its credibility – is its direct link to the every day work of ICT regulators worldwide and its bottom-up, empirical approach.

The insights and patterns revealed by the extensive, cross-sector analysis indicate the general direction of regulation over the next years and allow us to chart the trends – sustained or emerging – in regulatory leadership for the digital transformation.

1.   Setting the scene

Market growth in rapidly evolving technologies

Rapid evolution and new business opportunities are driving rapid but uneven growth in digital technologies grow rapidly. Latest ITU data show that some 49 per cent of the world's population currently remain unconnected (ITU, 2018) – the milestone of half the world's population online have been achieved in 2018. The number of mobile broadband connections currently stands at around 4.4 billion, while the number of fixed-broadband connections could soon surpass one billion. GSMA has estimated that the number of unique mobile subscribers exceeded 5 billion in 2017, and will total around 5.1 billion by end 2018.

Much attention is currently focused on 5G technology, with 5G positioned as an intelligent network that supports data and analytics use cases, driving diverse usage scenarios. For instance, 5G is seen as enabling both developed and developing countries to make full use of new technologies such as IoT, cloud computing, M2M and data analytics.[1] Early trials and initial commercial deployments are likely in 2019, following approval of international standards for 5G at the World Radiocommunication Conference 2019 (WRC-2019). 5G deployments will ramp up significantly from 2019 onwards. China is predicted to have between 200 million (GSMA) or one billion[2] 5G users by 2023. Several Middle East North Africa (MENA) operators have started early trials on 5G. Zain and Etisalat have conducted 5G trials in Saudi Arabia, Kuwait and UAE. In mid-2018, the operator Elisa launched an early 5G trial in Finland. Verizon Communications already trialled 5G residential applications in 2017[3] and is trialling fixed-wireless 5G residential broadband services in several markets in the US in 2018.

Inequalities between countries in terms of speed of access

At the same time, strong inequalities between countries persist in terms of speed of access, as well as differences in how connectivity is used. In LDCs, by end 2017, the number of mobile-cellular subscriptions had reached 700 million, with a penetration of 70 per cent. Figure 1 shows average global connection speeds in early 2018, with significant differences in speed observed between the fastest regions (North America and northern Europe) and regions with lower average connection speeds (Africa, and some countries in Latin America and Asia). Point Topic (2018) reports that Asia-Pacific has seen its average download speeds increase sharply by 28 per cent in Q2

Figure 1: Average connection speeds globally, by country, 2018
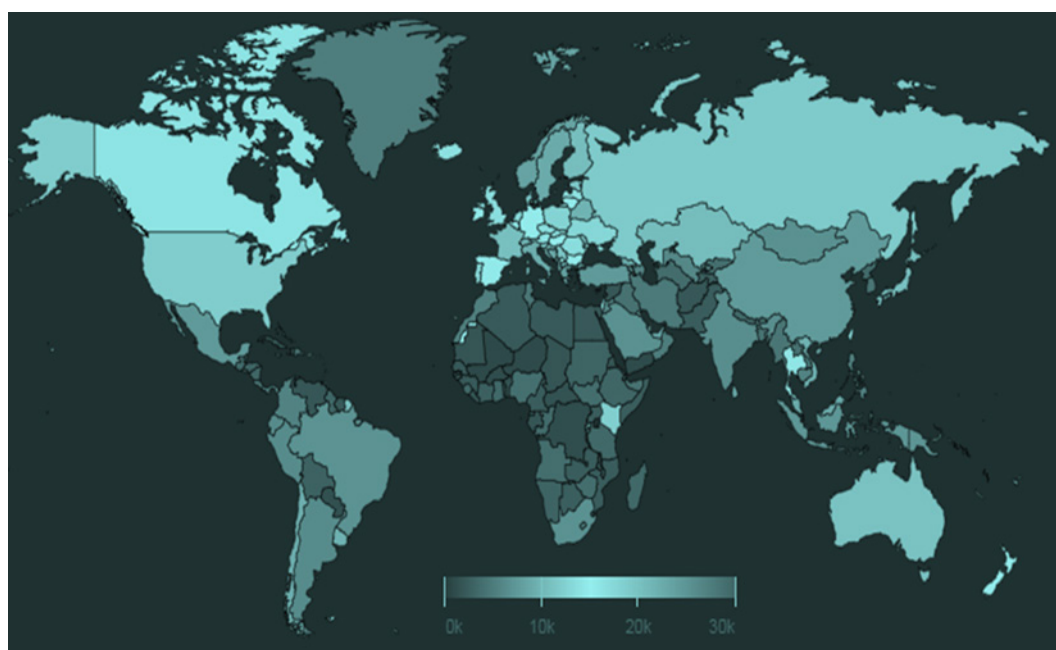
Source: Akamai

Table 1: Estimates of the global telecom market: 2015, 2016, 2017, 2020 and 2021

Indicator	2015	2016	2017	2020	2021
Mobile cellular subscriptions	7.2 bn (ITU) 7.2 bn (GSMA) 7.2 bn (E)	7.4 bn (ITU) 7.5 bn (GSMA) 7.5 bn (E)	7.74 bn (ITU) 7.8 bn (E)	8.3 bn (GSMA) 8.4 bn (E)	8.4 bn (GSMA) 8.6 bn (E)
Unique mobile phone users	4.6 bn (GSMA) 5.0 bn (E)	4.8 bn (GSMA) 5.1 bn (E*)	5 bn (GSMA) 5.3 bn (E)	5.4 bn (GSMA) 5.7 bn (E) 5.4 bn (Cisco)	5.5 bn (GSMA) 5.8 bn (E)
LTE subscriptions	1.1 bn (GSMA) 1.1 bn (E) 1.37 bn (ABI Research) 1.068 bn (GSA)	1.8 bn (GSMA) 1.9 bn (E*) 2 bn (Strategy Analytics)	2.6 billion (GSMA) 2.8 bn (E*)	4.1 bn (GSMA) 3.5 bn (ABI) 4.8 bn (E) 3.6 bn (4G Am)	4.5 bn (GSMA) 5.3 bn (E)
5G subscriptions	--/--	--/--	--/--	70 m (GSMA) 55 million (E)	220 m (GSMA) 190 million (E)
Mobile broadband subscriptions	3.2 bn (ITU) 3.4 bn (GSMA) 3.6 bn (E)	3.65 bn (ITU); 4.1 bn (GSMA) 4.5 bn (E)	4.2 bn (ITU) 4.8 bn (GSMA) 5.3 bn (E*)	6.5 bn (GSMA) 7.0 bn (E)	6.9 bn (GSMA) 7.5 bn (E)
Smartphone subscriptions	3.3 bn (GSMA) 3.3 bn (E)	3.9 bn (GSMA) 3.8 bn (E*)	4.5 bn (GSMA) 4.4 bn (E*)	5.9 bn (GSMA) 5.8 bn (E)	6.2 bn (GSMA) 6.3 bn (E*)
Fixed broadband	820m (ITU)	884m (ITU)	979m (ITU) 1bn (E*)	1.1 bn (E*)	1.2 bn (E*)
Internet users	3.21bn (ITU)	3.49 bn (ITU)	3.58 bn (ITU)	4.16 bn (ITU)	-/-
Facebook users	1.59 bn MAU 1.04 bn DAU	1.71 bn MAU 1.13 bn DAU	2.13 bn MAU 1.4 bn DAU	-/-	-/-
LINE users	215 million	217 million	207 million	203 million	-/-
Sina Weibo users	222 million	313 million	392 million	411 million	-/-
Vkontakte users	66.5 million	77.8 million	81.1 million	97 million	-/-
WeChat users	600 million*	806 million	963 million	1 billion	-/-
Smartphone stock	2.2 bn (Del); Q1/15	-/-	-/-	2.1 billion (BI)	-/-

Source: Various. EST = Estimate; MM = Mary Meeker; Del = Deloitte; Facebook, E = Ericsson Mobility Report June 2018; GSMA = GSMA database; ABI = ABI Research; SA = Strategy Analytics; BI = Business Intelligence; Cisco. For Facebook figures, MAU = monthly active users; DAU = daily active users. * Mid-year figures

2018 as operators in Singapore and Japan offered faster fibre and cable broadband packages.

Strong growth of subscriber numbers has occurred on social media

Equally strong growth of subscriber numbers has occurred on social media (see Figure 2). WhatsApp (owned by Facebook) now offers messaging and calling services to some 1.5 billion users in over 180 countries.[4] Viber (owned by Rakuten) currently offers calling, video and messaging services to over 800 million people.[5] Facebook listed some 2.23 billion monthly active users (MAU) on Facebook for mid-2018, an 11 per cent increase year-on-year.[6] Some 1.47 billion people on average logged onto Facebook as daily active users (DAU) for mid-2018, matching the growth in MAU with a 13 per cent increase year-on-year. However, DAU and MAU are not measures of data traffic, and use of Facebook

varies considerably in different regions of the world.

Data grows and grows

In addition to infrastructure and basic access, growth in data is also a key trend. Seven out of the top ten largest companies by capitalization in the world in Q3 2017 are digital companies with a strong digital component to their business.[7] Estimates of data growth are generally difficult to come by, but Cisco estimates that traffic over the Internet will grow by over 20 per cent a year between 2015-2020,[8] and that by 2021, global IP traffic will reach an annual run rate of 3.3 zettabytes. Cisco also projects that, by 2021, 80 per cent of all Internet traffic will be video, up from 67 per cent in 2016. Over-the-Top (OTT) applications such as YouTube and Netflix are contributing to this growth in data flows and Internet traffic, with strong growth in subscriber and user numbers for several key services (see Figure 2).

Growth in devices – especially in developing countries

In January 2018, Apple achieved a significant milestone with its active installed base reaching

1.3 billion devices, an increase of 30 per cent over two years.[9] Smartphone penetration is increasing in most markets, although global sales may have flattened recently. Deloitte predicts that by the end of 2023, the penetration of smartphones among adults in developed countries will exceed 90 per cent, up 5 per cent in 2018, while smartphone sales will amount to USD1.85 billion per year by 2023.[10] Some 40 million smartphones were sold in India in Q3 2017. With over 400 million Indians connected by 2G phones, India has overtaken the US to become the second-largest smartphone market and is even gaining in global share against China. However, Mary Meeker (2018) notes that overall, there was little net growth in the number of smartphones shipped globally[11] and Apple reported flat device sales for Q1 2018.[12] Data traffic from smartphones surpassed voice traffic in 2009, and has grown rapidly since then. Close to 85 per cent of mobile data traffic is generated by smartphones today, expected to reach 95 per cent by end 2023 (Ericsson, 2018).

The advance of IoT

In the context of IoT, Gartner forecasts that 8.4 billion connected things were in use in 2017, up 31 per cent from 2016, and growing to 20.4 billion by 2020. GSMA predictions are more conservative, forecasting that the number of IoT connected

Figure 2: Strong & continued growth in number of users of messaging and hybrid networks, 2011-2017
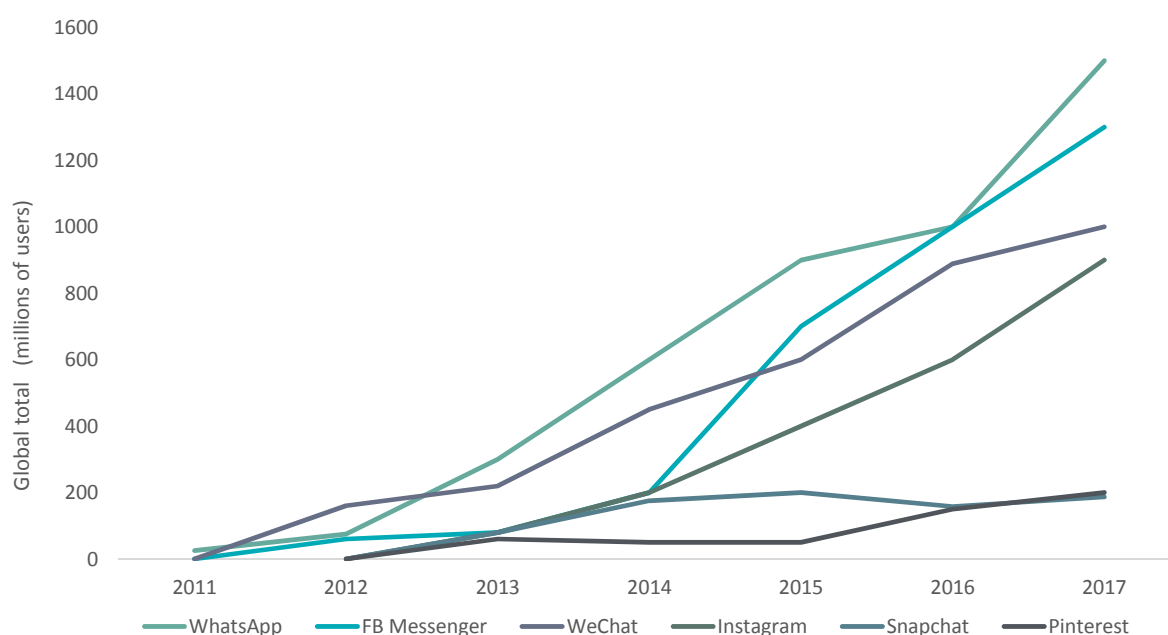
Source: Various, including Activate.com

Table 2: Estimated summary statistics for data-rich and data-dependent companies (indicative and only tentative, as reporting dates/years differ between companies)

Company	Market cap (2018)	Revenues	No. users
Apple Inc.	1 091m	USD229,234m for fiscal year ending 30 Sept 2017 (Source)	1.3bn active devices (Source) 715m iPhones in use at Dec 2016 (Source)
Amazon.com	976.65m	USD177,866m for fiscal year ending 31 Dec 2017 (Source)	Market estimates: 65-80m Prime subscribers (Source)
Microsoft	877.4m	USD110.36 bn – 2018	1.4 bn users Windows
Alphabet Inc.	839.74m	USD110,855m for year ending 31 Dec 2017 (Source)	2.7 bn users Android
Facebook	473.85m	USD40,653m for year ending 31 Dec 2017 (Source)	2.23 billion (MAU)
Alibaba Group	423.6m	USD39.898m (for year ending 31 March 2018) (Source)	576m users
TenCent	388.08m	USD21.9bn – RMB 237,760m for year ending 31 Dec 2017 (Source)	1 bn users – Feb 2018 (Source)

Sources: Various, ranking based on Wikipedia

devices will increase from 8 billion in 2017, to 13 billion in 2020 and will exceed 25 billion in 2025. International Data Corporation (IDC) forecasts are considerably higher, forecasting that some 80 billion IoT devices will be online by 2025, creating 180 zettabytes of data. According to Ericsson, the number of cellular IoT connections is expected to reach 3.5 billion in 2023, with an annual growth rate of 30 per cent. Of the 3.5 billion cellular IoT connections forecast for 2023, North-East Asia is anticipated to account for some 2.2 billion.[13]

Digital universe is 'doubling in size every two years' – but inequalities growing too

There is significant growth in data and devices (see Box 1). According to some estimates, some 2.5 quintillion bytes of information are generated daily, while Google alone is estimated to store over ten exabytes of data on a daily basis.[14] IDC/EMC (2014) reported that "the digital universe is doubling in size every two years and will multiply ten-fold between 2013 and 2020."[15] More recent IDC estimates put the size of the digital universe at around 2.7 zettabytes of data, but that by 2020, 30 zettabytes of data will be generated annually. However, there are some indications that inequalities in access to and use of intelligent connectivity may be growing.

Fibre connections

Fibre has been one of the main enablers of global connectivity to ICT and digital online services. As the majority of ICT services are at least partly delivered over fibre – including mobile and fixed broadband – fibre investment and deployments have climbed the policy agendas in all regions.

Box 1: The growth of our hyperconnected world

- 27.1 billion networked devices and connections by 2021
- 45 billion cameras by 2022
- By 2020, 1.7 MB of data generated per person on Earth per second
- 2.5 quintillion bytes of data generated daily
- 830 million connected wearable devices by 2020
- 75 billion IoT devices by 2025, a quarter of which will be for smart cities
- 3.5 billion cellular IoT connections by 2023

Source: IBM, presented to the GMIS-UNIDO-ITU Special Session on Technology and Innovation Powering Connectivity for Inclusive and Sustainable Industrial Development, ITU, 1 October 2018

Figure 3: Fibre backbone connectivity, worldwide, 2018

Population within reach of a fibre node
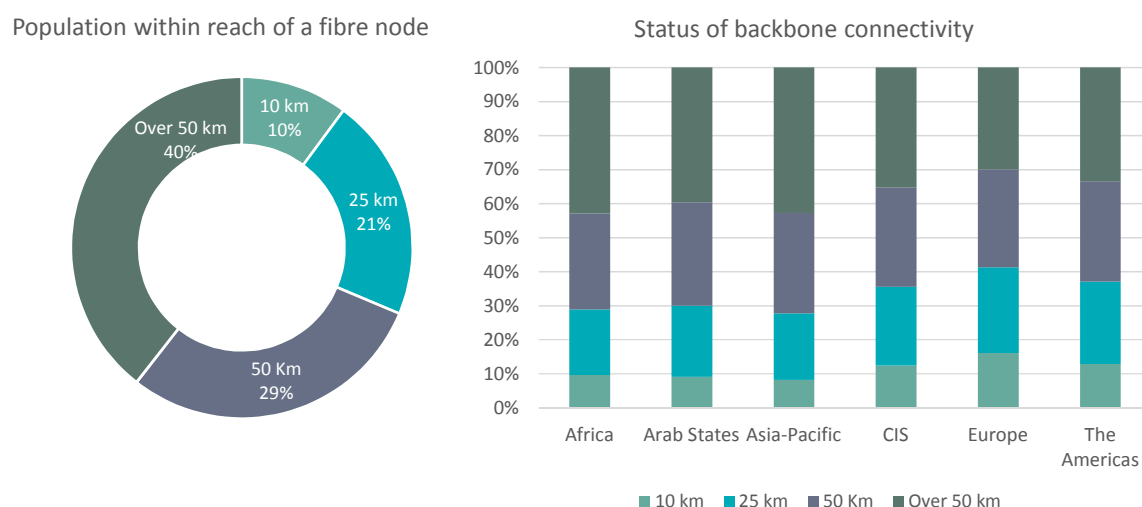
Status of backbone connectivity

Looking at fibre backbone connectivity, only one out of ten people worldwide is within the 10-km zone from a fibre node, ensuring fast and reliable access to ICT and digital services at all times (see Figure 3). Cumulatively, a third of world's population is within 25-km of reach from a fibre node, which could generally allow for good user experience most of the time, depending on the kind of service used. Another third of people worldwide are within the 50-km parameter from a node, largely ensuring basic connectivity. Sadly, 40 per cent of global population are further than 50 km from a fibre node, or otherwise outside the reach of advanced ICTs and many online services.

Fibre backbone connectivity across the regions follows a similar pattern, although some regions are slightly more advanced than others. Europe has the highest fibre reach in terms of the proportion of the population with access to fibre, within the three distance ranges, followed by the Americas and CIS. Asia-Pacific is the region with the largest amount of fibre backbone kilometres; however, it still needs to connect a third of its population. Africa and Arab States have around one-tenth of their population covered within 10 km of reach and around 40 per cent are out of reach, matching the world average.

The share of fibre connections in total fixed-broadband subscriptions continued to increase in all regions, with highest growth recorded in Asia and the Americas.[16] Figure 4 shows the technology market share by region for all regions for Q1 2018.

Surprisingly, a drop in fibre to the x (FTTx) lines has been observed since 2016, due to this technology being replaced with fibre to the home (FTTH) on a large scale in China, and to some extent in other countries.

Figure 4: Technology market share by region, Q1 2018
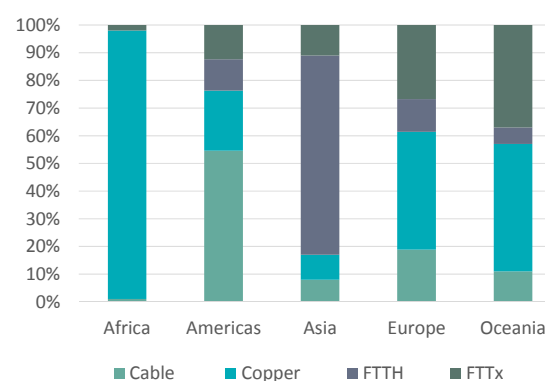
Satellite technologies – reaching the furthest corners of the Earth

Recent technological evolution in satellite technologies, offering broadband capacity across the globe, is bringing reliable connectivity to the furthest corners of the Earth.[17] High-throughput satellite (HTS) systems can use multiple spot beams and sophisticated ground infrastructure to provide speed and capacity similar to terrestrial technologies in many cases. Recently deployed and

upcoming non-geostationary satellite orbit (NGSO) systems in low-Earth orbits can now provide low-latency connectivity supporting a wide range of applications. And advances in satellite construction and competitive pressures are reducing the cost of services for users.

Satellite connectivity is starting to compare favourably with terrestrial wired solutions in terms of cost versus capacity. Advanced satellite systems have recently been launched or are planned for the near future. As the technology and market continue to evolve, satellite capabilities will continue to improve, while their cost will fall significantly – bringing satellite services in line with terrestrial solutions. In terms of coverage, satellites are an effective means for reaching remote and rural areas, as well as passengers in mobile environments, aircrafts and ships. Satellite technology can help relieve congestion and overloading of networks. In future, it will support 5G and ensure connectivity where terrestrial networks are unavailable.

Satellite systems should be given consideration as complementary solutions for next-generation broadband network deployments in rural and remote areas, as well as in diverse environments and deployment scenarios. The global satellite market grew by 2 per cent in 2016, with the global satellite industry worth USD339 billion with revenues of USD260 billion in 2016, according to the Satellite Industry Association.[18] Some analysts predict that 5G networks will be augmented by next-gen satellite capabilities, making satellite operators key players in the emerging communications ecosystem. Next-generation HTS are built on open architectures and will be much more flexible and easier to integrate into 5G infrastructure. In the 5G era, new satellite technologies will help address capacity and performance requirements.[19]

In 2016, the growing importance of the industry was once again underlined by the continued increase in number of operational satellites and by plans for new satellites with increased capabilities, as well as multiple constellations. By mid-2018, the total number of operating satellites came to 1 886[20] and a record number of 345 satellites were launched in 2017. From those, a total of 64 commercially-procured launches were conducted in 2017, matching the same number of commercial launches in the previous year.[21] The US has by far the greatest number of operational satellites in orbit, with China having nearly a third of this number. However, the market is relatively concentrated, with only five countries accounting for the vast majority of satellites.[22]

Endnotes

1   https://gsacom.com/building-5g-data-analytics-artificial-intelligence

2   TechRadar (18 October 2017) "China to blaze Connectivity Trail with a Billion 5G users by 2023": www.techradar.com/news/china-to-blaze-connectivity-trail-with-a-billion-5g-users-by-2023

3   https://www.telegeography.com

4   https://www.whatsapp.com/about/

5   https://www.viber.com/en/about

6   https://zephoria.com/top-15-valuable-facebook-statistics/

7   ICT4D Report 2018: Data-Driven Development, World Bank, Washington, DC, forthcoming

8   Cisco Virtual Networking Index 2017

9   https://venturebeat.com/2018/02/01/apple-reports-record-88-3-billion-revenue-in-q1-2018/

10   Deloitte TMT Predictions 2018: https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/tmt-predictions.html

11   Mary Meeker, "State of the Internet 2018" presentation: https://www.kleinerperkins.com/perspectives/internet-trends-report-2018

12   https://venturebeat.com/2018/02/01/apple-reports-record-88-3-billion-revenue-in-q1-2018/

13   https://www.ericsson.com/en/press-releases/2018/6/5g-on-a-roll-cellular-iot-deployments-ramping-up--ericsson-mobility-report

14   CXOtoday.com (17 July 2017) "Artificial Intelligence: Re-Imagining Big Data's Applicability": www.cxotoday.com/story/artificial-intelligence-re-imagining-big-datas-applicability/

15   EMC (9 April 2014) "Digital Universe Invaded By Sensors": https://www.emc.com/about/news/press/2014/20140409-01.htm

16   Point Topic: http://point-topic.com/free-analysis/world-broadband-statistics-q4-2017/

17   "Report of the Broadband Commission. Working Group on Technologies in Space and the Upper Atmosphere. 2017": www.broadbandcommission.org/workinggroups/Pages/spacetechnology.aspx

18   https://www.sia.org/wp-content/uploads/2017/07/SIA-SSIR-2017.pdf

19   https://www.globaldata.com/5g-may-usher-next-wave-satellite-communications-says-globaldata/

20   https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/

22   https://www.worldatlas.com/articles/countries-with-the-most-operational-satellites-in-orbit.html

2. Global context

Today's world is characterized by accelerating technological development and digital transformation that are driving massive upheaval and change. Half the world's population is already online. Before long, they will be joined by huge numbers of objects and devices connecting to private networks and the public Internet.[1] Digital transformation is being fueled by advances in computing power, big data (generated by the Internet of Things (IoT)) or simply by 'digital exhaust' generated by people's activity online and offline. Such data constitute the lifeblood of the Internet of Things, machine-to-machine (M2M) communications, machine learning (ML), artificial intelligence (AI) and intelligent machines and sensors, including robots and automated vehicles.

We are moving away from an environment dominated by networks, hardware and tangible assets to one in which services, the strength of an idea or an algorithm can create markets and companies worth billions of dollars. Fixed locations and boundaries (sometimes geographical) are supplanted by global borderless platforms and cyberspace, where national borders may be meaningless and difficult to police, and boundaries and firewalls may prove only too porous. Relationships are changing, between institutions, market players and people. In some markets, transaction costs are falling (e.g. Forex or trading stocks) and intermediaries are being eliminated or pushed out (e.g. retail banks), while in other markets, the role of the broker is becoming paramount (e.g. Uber, Amazon and Alibaba).

Ubiquitous connectivity, software and programmes (public or private) are also changing relationships. With teleworking, you may be able to work from different locations. In some sectors, your boss may be a world away and your 'team' distributed across many countries. In your personal life, you may see your friends less frequently, but may follow their updates daily on social media.

These changes are affecting policy settings and are prompting a need to review policy and regulatory frameworks, to coordinate policies and regulations beyond traditional boundaries or sectors, and to support those who may benefit least from digital transformation.

Against this background, ICT regulators are navigating considerable change. The days in which regulators had to deal with discrete issues (e.g. number portability) or changes (e.g. the transition to Internet Protocol or IP networks) are gone. Digital transformation is pervasive and cross-sector. Regulators now deal with profound changes with far-reaching consequences, including:

- Changes in business and investment models and financing of telecommunication/ICT infrastructure, which has become a fundamental infrastructure layer for the digital economy;

- Changes in regulatory processes and approaches to foster innovative regulatory approaches (regulatory sandboxes, concrete collaborative regulatory approaches);

- Concepts, such as digital identity across a growing number of services;

- Principles, such as consumer protection, confidentiality or data protection;

- End-to-end process change, such as blockchain and AI across sectors like finance and health.

In response, regulators are adopting a collaborative, cross-sectoral approach, working with other stakeholders to shape a common digital future in ways that maximize benefits, while introducing safeguards and protecting consumers. In 2016, ITU introduced the term 'collaborative regulation' to describe this approach.

Collaborative or fifth-generation (G5) regulation does *not* mean more regulation. Rather, it denotes regulation that is hands-on, inclusive, evidence-based and decision-oriented. It makes use of knowledge, experience and tools forged in previous generations and adds to the regulatory toolbox – while promoting cooperation across different sectors to address issues raised by the growth of services such as e-commerce, e-banking and e-health.

The Global ICT Regulatory Outlook 2018 examines this changing regulatory landscape. It shows how regulators are working much more closely with a broad range of stakeholders and other regulatory agencies including consumer, competition and data protection authorities, financial regulation

authorities, energy agencies, and authorities dealing with Internet-related issues. It charts the rise of collaborative regulatory approaches, and presents case studies of collaborative regulation in action across a range of countries, developed and developing countries alike. Finally, it considers important emerging issues that regulators will be facing in the near future such as blockchain and AI.

Box 2: Universal access and service in the digital economy

ICTs are at the core of the achievement of the 17 Sustainable Development Goals (SDGs) that will undoubtedly rely on the digital ecosystem, given the ever-expanding variety of services and applications that apply to all facets of daily life.

ICT regulators and policy-makers as well as the wider community of stakeholders, now recognize that ICTs play an essential role in the achievement of the SDGs. Issues such as affordability and availability – as well as creating incentives for innovation and entrepreneurship – must be addressed holistically and comprehensively at the policy and regulatory levels. The issues are complex and multi-faceted, but what is clear is that there is an interdependence of targets and goals – and ICTs have an important role to play in helping to achieve them.

The World Telecommunication Development Conference (Buenos Aires, 2017) declared that:

- universally accessible, secure and affordable telecommunications/ICTs are a fundamental contribution towards achievement of the WSIS action lines and the 2030 Agenda for Sustainable Development and towards the development of the global information society and the digital economy;
- policy-makers and regulators should continue to promote widespread, affordable access to telecommunications/ICTs, including Internet access, through fair, transparent, stable, predictable, non-discriminatory enabling policies and legal and regulatory environments.

Despite all the progress that has been made, there are still a large number of populations that either remain unconnected, or connected by unaffordable or unreliable infrastructure. The areas that have been left behind vary widely, including unserved and underserved populations of larger and developing nations, as well as landlocked, least developed countries, and small island developing states.

To help ensure these communities can take their place in the digital economy, the necessary regulatory framework should be in place, providing available and affordable access to all. Key issues central to providing affordable telecommunications/ICT access include building network capacity and expanding network coverage. Also necessary are effective telecommunications policies that reflect the need for a wide diffusion of digital networks. Additional measures include national broadband strategies that can help reach disadvantaged groups, and unserved and underserved areas and ensuring sound competition, including through market openness. In the case of international transit, monopolies also generally hinder affordable access or access to international bandwidth. Higher costs of international transit translate into higher costs for retail operators and, ultimately, consumers.

A combination of approaches and the efforts of multiple stakeholders will be required to reach affordable access to ICTs. Digital transformation affects multiple layers of the economy, society, and government. Therefore, collaborative regulatory approaches to reach across traditional policy silos and levels of government are needed, as well as developing a whole-of-government collaborative approach to enable access to infrastructure. Key stakeholders across different economic sectors can also enrich the policy-making process, implementation and monitoring. Legislative and regulatory actions can remove barriers, enhance competitive incentives and provide greater predictability for investors and lower costs for network deployment. A number of countries are also implementing various funding and operating models. The right choice for each country depends on multiple factors.

The wide variety and large number of factors in the affordable connectivity equation underscore the need for an integrated and collaborative approach to provide continuous affordable access to telecommunication/ICT infrastructure. Following the learnings from the ITU global study "Maximizing availability of international connectivity in developing countries: strategies to ensure global digital inclusion" released in 2017, and other activities to maximize infrastructure development, ITU is seeking to define insights and concrete recommendations on current connectivity trends and how access to infrastructure within countries can power the digital economy for people around the world.

Source: ITU

2.1. Economic impact of digital[2]

Good ICT regulation has a positive impact on the growth of national economies as ITU research has previously shown.[3] Regulation has real impact – and, building on our previous work, we have developed two of the most comprehensive, robust metrics in their respective areas which lay out compelling, new evidence.

To build the case for broader adoption of digital technologies and policies, we undertook multi-faceted quantitative analysis of large quantities of small data. This has enabled us to explore, understand and quantify how digital technologies can contribute economically to growing the larger digital ecosystem. Our evidence is clear, with a high degree of accuracy and reliability – the small data is validated as coming from certified, mainly first-hand sources; it is curated and consistent, and no random or irrelevant items blur the focus.

The evidence is clear. ITU has released a landmark study on the impact of broadband, digital transformation and the interplay of ICT regulation on national economies, based on econometric modelling.[4] It builds on our work in the area over the past ten years using top-tier data metrics on the development of the digital ecosystem (the CAF Digital Ecosystem Development Index[5]) and on the maturity of ICT regulatory frameworks (the ITU ICT Regulatory Tracker[6]).

Our extensive analysis has yielded important findings. In addition, the structural models provide estimates for other important economic parameters.

Broadband has economic impact

Fixed broadband: higher economic impact in more developed countries

- Fixed broadband has had a significant impact on the world economy during the last eight years (2010-2017).

- An increase of 10 per cent in fixed broadband penetration yields an average increase of 0.8 per cent in GDP (based on a structural econometric model developed for the study).

- Fixed capital formation (proxied by investment) is a strong catalyst of GDP growth, suggesting an important contribution on the economy (0.19 coefficient). Similarly, the labour force critically affects economic growth: it is estimated that increasing the skill levels of labour with 10 per cent would increase a country's GDP by 0.5 per cent.[7] This can be attributed both to a limited expansion of infrastructure and the large dependency on quality of the labour force.[8]

- Prices are the key enablers for adoption of the technology. Strikingly, a 10 per cent drop in prices boosts adoption by more than 3 per cent.[9] Income variation across the sample period seems to have a similar impact on this process. Hence, increasing the average disposable income (proxied by GDP) by 10 per cent, yields 8.3 per cent more fixed broadband adoption. Essentially, this translates into the increasing importance of the infrastructure and the subsequent service provided over it.

- Increasing the disposable income (proxied by GDP) by 10 per cent attracts 1.23 per cent more supply. Supply dynamics suggest that, as expected, income levels affect the revenues and investments of operators. The consumption propensity for broadband services seems to have a significant impact on increasing the supply of digital offerings. Finally revenues are found to have a significant impact on the performance of the industry, implying a reinvestment of the output to the productive basis of the economy.[10] This is an additional angle supporting the increasing returns to scale of ICT infrastructure.

- The only model where statistically significant positive effects were found for fixed broadband is for countries with GDP per capita higher than USD 22 000 (higher income countries). The study found that a 10 per cent increase in broadband penetration yields a 1.4 per cent increase in GDP growth. This value is consistent with findings in the general model. On the other hand, while the impact of fixed broadband for middle and low-income countries had a positive sign, both coefficients lack statistical significance. To address the model limitations for middle-income countries, the data set was reduced from 3Q 2013 to 4Q 2017 following the argument that before 2013,

In summary, the broadband economic impact models confirm these three hypotheses:

- In the aggregate, mobile broadband appears to have a higher economic impact than fixed broadband;

- The economic impact of fixed broadband is greater in more developed countries than in less developed;

- The economic impact of mobile broadband is greater in less developed countries than in more developed.

The results of the models are presented in Figure 5.

Figure 5: Economic impact of broadband worldwide
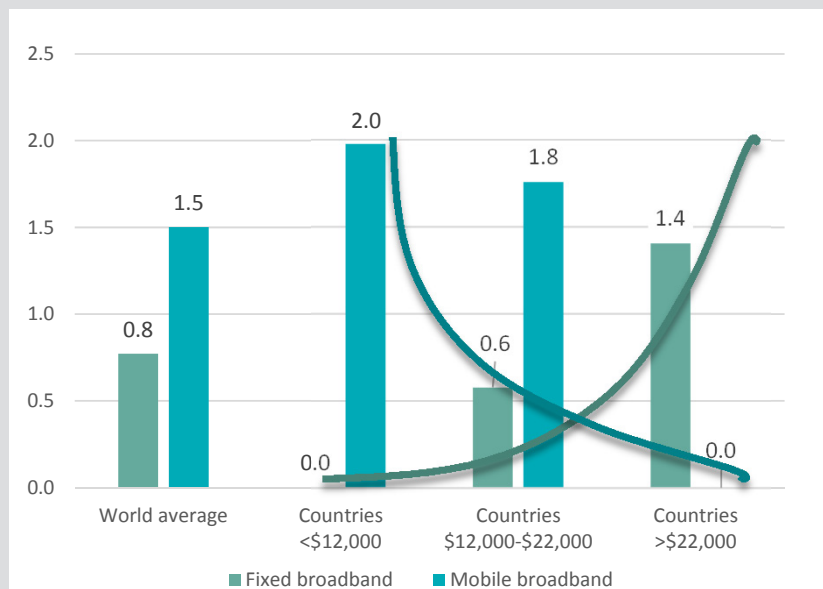
Note: Values expressed as impact on GDP of 10% increase in broadband penetration; for example, when broadband penetration increases from 10% to 11% or from 20% to 22%.
Source: ITU (Katz and Callorda 2018)

fixed broadband penetration was low and therefore economic effects were likely to be negligible. In this case, the economic impact of fixed broadband was positive and significant at the 5 per cent level.

- This confirms that the impact of fixed broadband appears at higher levels of economic development (critical mass) and also supports the 'return to scale' argument: fixed broadband economic impact tends to increase with economic development. Given the

correlation between GDP per capita and fixed broadband penetration, it is fair to say that fixed broadband technology has an economic impact at higher penetration levels (above 30 per cent).

- Furthermore, the model's results could also indicate that we are witnessing a fixed to mobile substitution: in low GDP per capita countries with low fixed broadband penetration, mobile broadband technology

becomes the preeminent technology driving economic growth.

- Equally important, since the impact of mobile broadband achieves saturation at higher levels of economic output, this confirms the need to develop holistic and technology neutral policies allowing growth in parallel fixed and mobile technologies in order to maximize their benefits over time.

Mobile broadband: higher economic impact in less developed countries

- Mobile broadband appears to have a higher average impact on economic growth than fixed broadband. An increase of 10 per cent in mobile broadband penetration yields an increase of 1.5 per cent in GDP.

- The importance and direction of impact of fixed capital formation is confirmed in the fixed and mobile broadband models. Service pricing is less significant in driving demand, but affordability appears less of a barrier. This could result from a relatively low mobile broadband cost since it is an addition in the

mobile plan and the global spread of zero-rate service offers.

- Mobile broadband's contribution to the economy is higher in less developed than in more developed countries, a reflection of the saturation effect.

- Two subsets of countries reflected a positive and significant impact of broadband on GDP:

  ° For countries with GDP per capita between USD12 000 and USD22 000, a 10 per cent increase in mobile broadband penetration yields 1.8 per cent increase in GDP growth;

  ° For countries with GDP per capita below USD12 000, a 10 per cent increase in mobile broadband penetration yields 2 per cent increase in GDP growth;

  ° No economic impact was detected for countries with GDP per capita above USD22 000. In other words, the model indicated that the lower the income level, the higher the economic impact of mobile broadband.

2.2. Digitization has strong economic impact

Digitization is a mega market trend stretching over the past three decades, enabling a wide array of mobile, fibre and broadcasting technologies that define the digital world. Its development is not linear and has advanced in waves (see Box 3). Each new wave brings about unrivaled opportunities for market growth and near-universal adoption of services while raising challenges too. Their impact on national economies has been profound and lasting. We can now more accurately quantify the impact of digitization on economic growth.

To quantify the economic contribution of digitization, the cross-sectional models test its impact on variables such as GDP, employment and productivity and in doing so, are based on the CAF Digital Ecosystem Development Index composed of 64 indicators across 75 countries[11] (including developed and developing countries and emerging economies[12]) between 2004 and 2015 (see Figure 7). Countries included are those with GDP per capita higher than USD5 000 and a population of more than 5 million.

To assess the strength of the causal link between digital ecosystem development and economic development, an endogenous growth model was used, based on the Cobb-Douglas production function, linking the stock of fixed capital, labour force, and the CAF Digital Ecosystem Development Index. The model also controls for GDP per capita

for the previous year to account for inertia effects. By converting all equation terms to logarithms, it was possible to estimate the impact of each variable of the growth of the digital ecosystem.

The model revealed three key findings:

Finding 1: Economic impact of digitization is higher than that of broadband alone

The development of a digital ecosystem correlates with economic development, within the sample of 74 countries around the world and for the period 2004-2015.

The economic impact of digitization is higher than that of fixed broadband and is on a par with mobile broadband. An increase of 1 per cent in the CAF Digital Ecosystem Development Index results in a 0.13 per cent growth in GDP per capita. This means, for example, that an increase in the CAF Digital Ecosystem Development Index from 50 to 51 will yield an increase of per capita GDP of 0.26 per cent (accounting for direct and indirect effects on output).

The significance then of this finding is that the full economic impact of ICT is achieved through the cumulative adoption of all technologies, in addition to its assimilation and usage in the production and social fabric. Broadband penetration is *only one aspect* of required policies; the biggest economic impact can be achieved only through a holistic set

Figure 6: Waves of digitization – a conceptual blueprint

Third wave
Bigdata, robotics, machine learning

Second wave
Computers, broadband, mobile telecommunications

First wave
Computers, broadband, mobile telecommunications
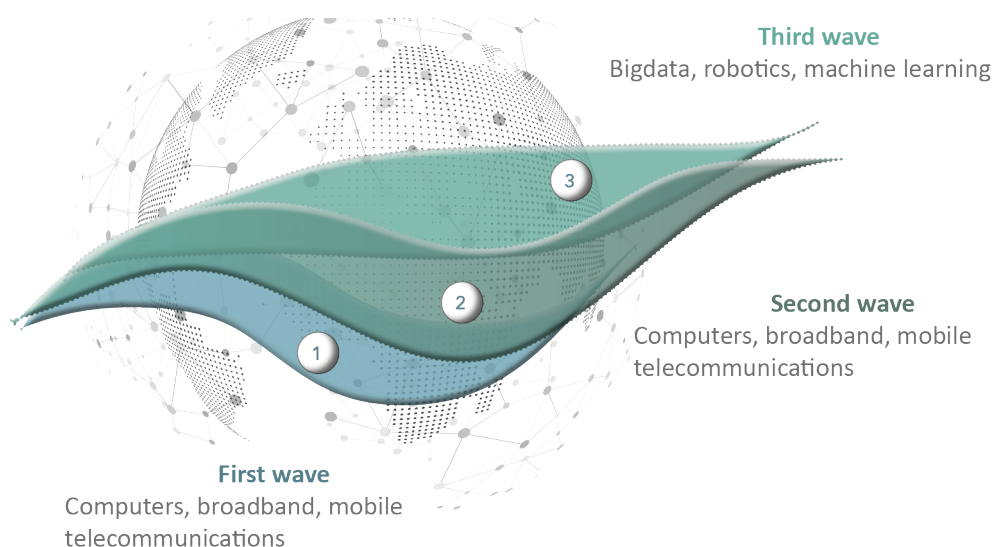
Source: ITU

Box 4: Waves of digitization and policy stakes

Digitization refers to transformations triggered by massive adoption of digital technologies that generate, process, share and transfer information. Digital transformation is not a one-time event. It proceeds in waves driven by technological progress and diffusion of innovation.

- First wave: the introduction and adoption of 'mature' technologies. These include management information systems automating data processing and monitoring and reporting of business performance, telecommunication technologies such as broadband (fixed and mobile) and voice telecommunications (fixed and mobile), which allow remote access of information.
- Second wave: the diffusion of the Internet and its corresponding platforms (search engines, marketplaces), which enable the networking of enterprises to consumers and enterprises among themselves for purchasing of supplies, and distribution of output.
- Third wave: the adoption of advanced technologies such as big data and analytics, Internet of Things, robotics, sensors, and artificial intelligence. These enhance information processing and the quality of decision-making, while further automating routine tasks within business enterprises and governments. These technologies are integrated with first and second wave mature technologies.

Each wave has a specific set of social and economic impacts. Computing, broadband and mobile telephony networks have helped relax industry scalability constraints, allowing traditional sectors to grow more rapidly. This has in turn led to increased demand for labour in service industries (e.g. financial services, education, health care, etc.), and has had a positive effect in manufacturing. The first wave appears to have helped household incomes to grow in some countries, and has facilitated social inclusion through increased access to information, government services, entertainment content, etc.

The second wave has ushered in new services and applications such as Internet information searches, electronic commerce, distance education and collaborative businesses such as Uber and Airbnb. This 'innovation effect' has increased labour demand in occupations in digital services and collaborative businesses, while eroding low and middle-skill jobs through automation.

The third wave will increase productivity levels and promises to benefit social welfare, particularly in relation to several Sustainable Development Goals related to public services, including health and education. Speculative evidence only has so far emerged as to any disruptive effects on labour. However, there is universal agreement that, as with initial waves of innovation, automation will favour better educated, more highly trained workers. It is vital to consider policy remedies that will maximize the benefits of automation while limiting negative outcomes.

The policy challenge going forward: the digital transformation resulting from all three waves is so all-encompassing that sector-specific strategies are no longer applicable. Governments need to build cross-institutional links fostering collaboration between education, ICT, industrial promotion, science and technology to devise and jointly implement policies. In addition, future public policy has to extend beyond traditional domains (taxation, competition, and digital literacy) to include new areas such as privacy protection, cybersecurity, and must foster trust and enhanced customer experience. It is clear that the challenges for policy-makers are significant, but so are the benefits for citizens. Mitigating any potential disruptions remains key.

Source: ITU, GSR-17 Discussion Paper, *Social and economic impact of digital transformation on the economy*

---

of policies ranging from telecoms to computing to adoption of the Internet and electronic commerce.

Finding 2: Economic impact of digitization is guided by a 'return to scale' effect

The same model was used for OECD and non-OECD countries to test for a 'return to scale' effect to see if the economic contribution of digitization increases at higher development stages.

Results show that the impact of the digital ecosystem is higher on more advanced economies than on developing countries. Thus, an increase of 1 per cent in the CAF Digital Ecosystem Development Index yields an increase of 0.14 per cent in per capita GDP for OECD countries, but yields only 0.10 per cent (see Figure 8) in non-OECD countries. In other words, the higher the economic development, the stronger the contribution of the digital ecosystem on economic growth.

Figure 7: CAF Digital Ecosystem Development Index
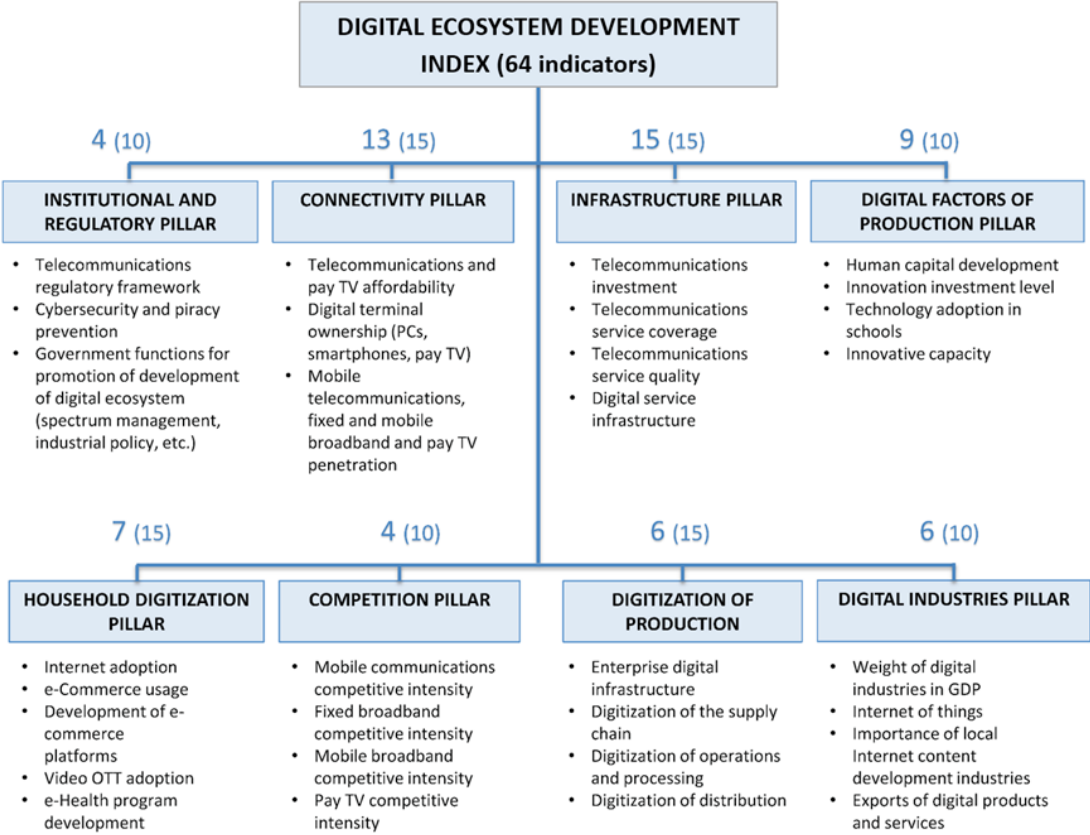
Source: Katz and Callorda (2017)

Figure 8: Economic impact of digitization, by grouping, 2004-2015
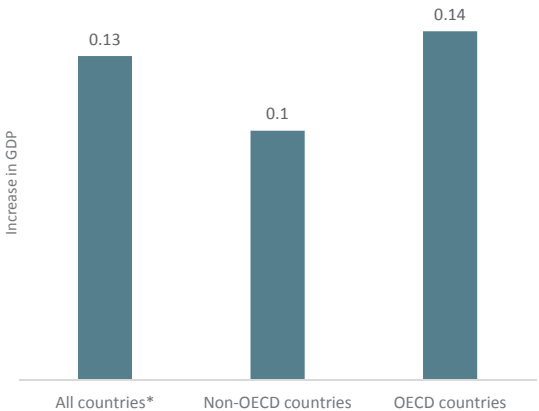
*Note: Based on a sample of 75 countries with population higher than 5 million and with GDP higher than USD5 000.
Source: ITU

As expected, the capital formation is positive and significant although this metric varies considerably across social, demographic and economic settings.

Digitization has a disproportionately high impact in developed economies compared to developing ones. Labour's contribution to GDP is also consistent and significant. The quality of labour is crucial – a higher proportion of skilled labour generates higher economic growth; however, this finding is largely accepted.

Finding 3: As well as contributing to GDP growth, digitization also impacts labour and total factor productivity

A different model was built to test the impact of digitization on economic variables such as labour productivity and total factor productivity. Using this model, we found that an increase in the ecosystem development index of 1 per cent yields an increase of 0.26 per cent in labour productivity and 0.23 per cent in total factor productivity.

2.3. ICT policy and regulatory frameworks impact market growth for digital services

Our previous work has underlined the strong correlation between ICT regulation and the take-up of ICT. Our analysis of mobile broadband adoption trends (showcased in the Global ICT Regulatory Outlook 2017 report) demonstrated the central role of good regulatory frameworks – with countries in the fourth generation of regulation (G4) significantly outperforming all others.[13]

As part of our latest econometric study, we explore the link between ICT Regulatory Tracker (a metric of the maturity of national ICT regulatory frameworks) and the CAF Digital Ecosystem Development Index (a metric of the growth of the digital economy, from 2007 to 2015). The underlying premise is that higher regulatory performance is directly related to the development of the digital economy. Beyond measuring the correlation between both metrics, we developed a model with lagged variables to account for the fact that regulation needs time to become effective and have impact. Finally, we converted the variables to logarithms to test causality of change in values of both metrics.

It is worth nothing that the two metrics do not track the same ecosystem: one focuses on ICTs and the other on digital development, which goes beyond traditional ICTs. This matching of metrics provides insights into the relationship between current, traditional ICT regulatory frameworks and fast-growing digital markets. For consistency, we recalculated the CAF Digital Ecosystem Development Index without its regulatory and competition pillars, as including these could create a high chance of co-linearity with the ICT Regulatory Tracker.[14]

Our analysis provides further evidence of how regulatory and institutional factors drive digital ecosystem growth. An increase of 10 per cent in the ICT Regulatory Tracker yields a positive increase in the CAF Digital Ecosystem Development Index of 0.348 per cent at least a year after regulation has been adopted, which builds up over time. In a nutshell, there is a proven correlation between ICT regulation and digital development; however, one can argue that the overall figure is relatively low. This finding

is consistent with the testing model, which recognizes the partial overlap of the two main metrics used. Moreover, this is an important avenue for regulators to explore since it shows clearly that even mature, advanced ICT regulatory frameworks might not yet have a significant or positive impact on the development of the digital economy. To have impact, targeted regulatory strategies should address the growing pains of digital markets.

To further test the relationship between the regulatory and digital ecosystem indices, a set of alternative correlations and causality was explored across the two metrics (see Tables 3 and 4). As a result, it is possible to pinpoint areas where ICT regulation is in strong interplay with digital development.

What the table tells us – the main highlights:

- An increase in the ITU ICT Regulatory Tracker values (with and without the competition pillar) is positively and significantly correlated with an increase in the CAF Digital Ecosystem Development Index, as well as with every one of its pillars.

- The **connectivity of digital services** is significantly correlated with the level of advancement of ICT policies and regulations – particularly the competition and market power regulatory set-up (*coefficient 0.80 and 0.68 respectively for the Tracker with and without the competition component, and 0.61 for the competition component alone*).

- **Digital factors of production** are directly and positively influenced by the maturity of ICT regulatory frameworks (*coefficient 0.77 and 0.64*) and by ICT competition frameworks in particular (*coefficient 0.62*).

- Policy and regulation also drive **household digitization** (*coefficient 0.72 and 0.60*).

- The cross-cutting analysis of the two metrics suggests the importance of the regulatory frameworks for the **development of infrastructure for digital services** (*coefficient 0.63 and 0.57*).

- On the other hand, **digital competitive intensity** does not unequivocally result

Table 3. Correlations between ITU ICT Regulatory Tracker and CAF Digital Ecosystem Development Index pillars

Pillars	ITU ICT Regulatory Tracker	ITU ICT Regulatory Tracker (w/o competition component)	Regulatory authority component	Regulatory mandate component	Regulatory regime component	Competition framework component
CAF Digital Ecosystem Development Index	0.5109 (0.0277) ***	0.4353 (0.0246) ***	0.3565 (0.0427) ***	0.3600 (0.0271) ***	0.3429 (0.0155) ***	0.3637 (0.0266) ***
Infrastructure of digital services	0.6394 (0.0434) ***	0.5769 (0.0378) ***	0.4649 (0.0629) ***	0.4767 (0.0400) ***	0.4294 (0.0241) ***	0.4141 (0.0405) ***
Connectivity of digital services	0.8058 (0.0538) ***	0.6764 (0.0479) ***	0.5791 (0.0802) ***	0.5484 (0.0515) ***	0.5811 (0.0299) ***	0.6067 (0.0497) ***
Household digitization	0.7179 (0.0375) ***	0.6030 (0.0337) ***	0.5478 (0.0590) ***	0.5189 (0.0367) ***	0.4521 (0.0219) ***	0.5094 (0.0363) ***
Digitization of production	0.3214 (0.0396) ***	0.2956 (0.0345) ***	0.1785 (0.0523) ***	0.2384 (0.0358) ***	0.2388 (0.0236) ***	0.1777 (0.0360) ***
Digital competitive intensity	0.3076 (0.0343) ***	0.2563 (0.0304) ***	0.1851 (0.0462) ***	0.1832 (0.0312) ***	0.1988 (0.0203) ***	0.2397 (0.0301) ***
Development of digital industries	0.3419 (0.0377) ***	0.3011 (0.0330) ***	0.2370 (0.0523) ***	0.2584 (0.0342) ***	0.2191 (0.0229) ***	0.2384 (0.0341) ***
Digital factors of production	0.7688 (0.0472) ***	0.6403 (0.0422) ***	0.5025 (0.0721) ***	0.5386 (0.0454) ***	0.5151 (0.0271) ***	0.6228 (0.0430) ***

***, **, * significant at 1%, 5% and 10% critical value respectively
Note: The values in blue have correlations higher than 0.60 (strong correlation).

Source: ITU

from traditional competition frameworks. In other words, for digital players, the level of openness in the ICT sector might not be the measure of openness in the digital ecosystem. Furthermore, the level playing field in the broader digital ecosystem is not necessarily a reality or even a possible option as different dynamics play out in digital markets. By extension, this finding suggests that digital players are at a competitive advantage if digital services/platforms are unregulated.

- The **development of digital industries and digitization of production** remains significantly and positively correlated to the maturity of regulatory frameworks – however, the strength of the correlation is weaker than for other key components (*coefficient around 0.3*).

- What's more, one cannot detect in this analysis a component of the ICT Regulatory Tracker that has higher importance than the rest when correlated with the CAF Digital Ecosystem Development Index and its pillars. Growth in the components of the ITU ICT Regulatory Tracker go hand-in-hand with an improvement across *all pillars* of the digital ecosystem.

- All this suggests that new policies and regulations need to be developed, or replace existing ones, to increase their impact on the development of the digital ecosystem.

Table 4: Strongest correlations between the ICT Regulatory Tracker and the CAF Digital Ecosystem Development Index

ITU ICT Regulatory Tracker	CAF Digital Ecosystem Development Index
All pillars	Development of infrastructure of digital services
All pillars Tracker w/o competition pillar Competition pillar alone	Connectivity of digital services
All pillars Tracker w/o competition pillar	Household digitization
All pillars Tracker w/o competition pillar Competition pillar alone	Digital factors of production

Note: Results here are significant at 1% and with correlations higher than 0.60 (strong correlation).
Source: ITU

A second set of regressions using the same metrics shows that the maturity of ICT regulatory regimes in particular (proxied by that component of the ICT Regulatory Tracker) appears to be the main path of impact of digital ecosystem development (proxied by the eponym index) (see Table 5).

This analysis indicates that the regulatory regime pillar always has a positive and significant impact on every single pillar of the CAF Digital Ecosystem Development Index.[15] This could indicate that the actual set of policies and regulations in place has higher impact on digital development than the mandate or existence of the regulatory authority.[16]

Indirectly, although rather intuitively, this in turn suggests that what matters is the regulatory framework and its capacity for enforcement rather than the nature – and mandate – of the regulator: it's not *who*, but *how and what* that matters most. While regulatory authorities can be the driving force of efficient market facilitation, policy-makers can also be effective in policy implementation and regulation-making.

This finding does not undermine the importance of an empowered, autonomous regulator (or regulators) as being able to maximize the positive impact of regulation, its coherence and strategic foresight. In an ideal situation, a separate, well-capacitated and funded regulator with a broad mandate can be a guarantee for these capabilities.

Table 5. Impact of the ICT Regulatory Tracker components of the CAF Digital Ecosystem Development Index pillars

	Digital ecosystem Development Index	Infrastructure of digital services	Connectivity of digital services	Household digitization	Digitization of production	Digital competitive intensity	Development of digital industries	Digital factors of production
Regulatory authority component	-0.1646 (0.0507) ***	-0.2209 (0.0806) ***	-0.2255 (0.0992) **	-0.1743 (0.0743) **	-0.1974 (0.0765) **	-0.0746 (0.0669)	-0.1162 (0.0777)	-0.3123 (0.0907) ***
Regulatory mandate component	-0.0899 (0.0463) *	-0.0980 (0.0736)	-0.3433 (0.0906) ***	-0.0084 (0.0679)	0.0000 (0.0698)	-0.1927 (0.0610) ***	0.0831 (0.0710)	-0.0934 (0.0828)
Regulatory regime component	0.4207 (0.0244) ***	0.5253 (0.0389) ***	0.7966 (0.0479) ***	0.4983 (0.0359) ***	0.2701 (0.0369) ***	0.2983 (0.0322) ***	0.2011 (0.0375) ***	0.6356 (0.0438) ***
Constant	3.1659 (0.0978) ***	2.7548 (0.1558) ***	3.0748 (0.1914) ***	2.6408 (0.1434) ***	3.3221 (0.1476) ***	4.0243 (0.1297) ***	2.7272 (0.1499) ***	2.6227 (0.1750) ***
Observations	656							
R-squared	0.4730	0.3599	0.4188	0.4189	0.1476	0.1589	0.1271	0.3947

***, **, * significant at 1%, 5% and 10% critical value respectively
Note: The values in blue have correlations higher than 0.60 (strong correlation).
Source: ITU

Endnotes

1   Back in 2011, Ericsson famously projected the number of connected devices to reach 50 billion by 2020, https://www
    .akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices
    .pdf. In the absence of a consistent definition of a 'connected device' (although many have tried to define it), there is no
    real way of knowing whether this forecast will be achieved.

2   This section is based on the econometric work and expands on the findings of the 2018 ITU Study on *The economic
    contribution of broadband and digital transformation and the impact of policy on the rate of digitization: econometric
    modelling*: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDR-2018-PDF-E.pdf

3   ITU, The economic contribution of broadband, digital transformation and ICT regulation, September 2018: www.itu.int/
    treg, ITU Trends in Telecommunication Reform 2014, Chapter 1, and Global ICT Regulatory Outlook 2017, itu.int/go/
    outlook

4   ITU, *The economic contribution of broadband and digital transformation and the impact of policy on the rate of
    digitization: econometric modelling*, September 2018: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDR-2018
    -PDF-E.pdf

5   The CAF Digital Ecosystem Development Index was developed with funding from CAF Development Bank of Latin
    America. Data can be found in Observatorio CAF del Ecosistema Digital at:scioteca.caf.com/handle/123456789/1059

6   itu.int/go/tracker

7   Education is defined as the World Bank indicator: School enrollment, tertiary (% gross). Ideally, the indicator should be
    workforce with tertiary education; however, this indicator is only available for a few countries and would reduce the
    number of countries to run the model by 70%.

8   The analysis of influence of control variables might require further analysis.

9   A word of caution: considering that this is a structural model based on a system of equations, the results of intermediate
    equations are inputs for the final result. In that sense, the coefficients of intermediate steps are results that should not
    be considered general conclusions.

10 This is particularly relevant for markets undergoing high growth, while it may not be the case for saturated markets.

11 Katz, R. and Callorda, F. (2018). "Accelerating the development of Latin American digital ecosystem and implications for
    broadband policy", Telecommunications Policy 42, pp. 661-681.

12 See list of countries in Appendix A

13 ITU *Global ICT Regulatory Outlook 2017*: https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Outlook/2017.aspx

14 See the original study for all model structure and results: ITU, *The economic contribution of broadband, digital
    transformation and ICT regulation,* September 2018: https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/FINAL
    _1d_18-00513_Broadband-and-Digital-Transformation-E.pdf

15 The regulatory regime component includes indicators such as type of licences provided to offer telecommunications
    services, obligations to publish interconnection offers by operators, monitoring of quality of service, infrastructure
    sharing for mobile operators permitted and/or mandated, unbundled access in local loop, spectrum secondary trading
    allowed, and number portability.

16 While the first two components of the ITU ICT Regulatory Tracker can have a negative sign, the coefficient of regulatory
    regime and regulatory mandate is always bigger and positive.

3. The state of ICT regulation

3.1. Worldwide trends

The state of ICT regulation worldwide is very much 'in flux'. Countries' approaches are converging on some topics and diverging on others and regulatory practices vary significantly.

In last year's Global ICT Regulatory Outlook 2017, we explored the evolution of ICT regulatory trends over the preceding decade. We set out the ITU concept of 'generations' of ICT regulation – now widely shared – analysing prime evidence and charting possible ways forward (see Figure 9).

Our findings hold true. The rise of G4 regulation has proved unstoppable. By the end of 2017, a third of countries had climbed aboard the bandwagon – no longer an exclusive club – of fourth generation regulators (see Figure 10, upper graph). In just ten years, G4 has become the gold-standard for every ICT regulator.

As regulation evolves worldwide, we discern three tiers of regulators, nearly equal in number:

- The highest tier – fourth-generation – is made up of achievers who have moved along the wave of the Fourth Industrial Revolution, have stood their ground to protect consumer interests, have opened up markets and are advancing investment for social and economic goals.

- The middle tier – third-generation – has been moving ahead, pushing limits and markets towards more adaptive, competitive regulatory regimes.

- The low tier grouping – first and second generation of regulators – is both losing ground and shrinking in number. Countries neither appreciate nor benefit from a lack of advancement in their market structure and regulatory instruments. In another ten years, the near-extinction of this tier seems likely. The progress and sophistication of ICT regulation is in effect a powerful statement of development ambitions and no country can afford to miss the considerable opportunity represented by an increasingly open and vibrant market.

Reviewing the top countries in 2017, there is little surprise. Italy tops the table with an overall score of 97.3, stealing the trophy from Ireland by a small margin (see Table 6). Europe largely leads the way, with only two non-European countries in the top ten, and five non-European countries in the top 25 (see Table 6). Overall, in broad terms,

ICT Regulatory Tracker data	Score breakdown/Gs
2007-2009: data for 187 countries	G1: [0; 40)
2010-2013: 188 countries	G2: [40; 70)
2014: 189 countries	G3: [70; 85)
2015-2017: 190 countries	G4: [85; 100]

Source: ITU

Figure 9: Generations of ICT regulation – conceptual framework

G3
Enabling investment, innovation and access
Dual focus on stimulating competition in service and content delivery, and consumer protection

G4
Integrated regulation
Led by economic and social policy goals

G2
Opening markets
Partial liberalization and privatization across the layers

G1
Regulated public monopolies
Command & control approach

G5
Collaborative regulation
Inclusive dialogue and harmonized approach across sectors

Source: ITU

Figure 10: Evolution of regulatory frameworks, worldwide, 2007-2017

Generations of ICT regulation, worldwide

State of maturity of ICT regulatory frameworks, worldwide, 2007 and 2017
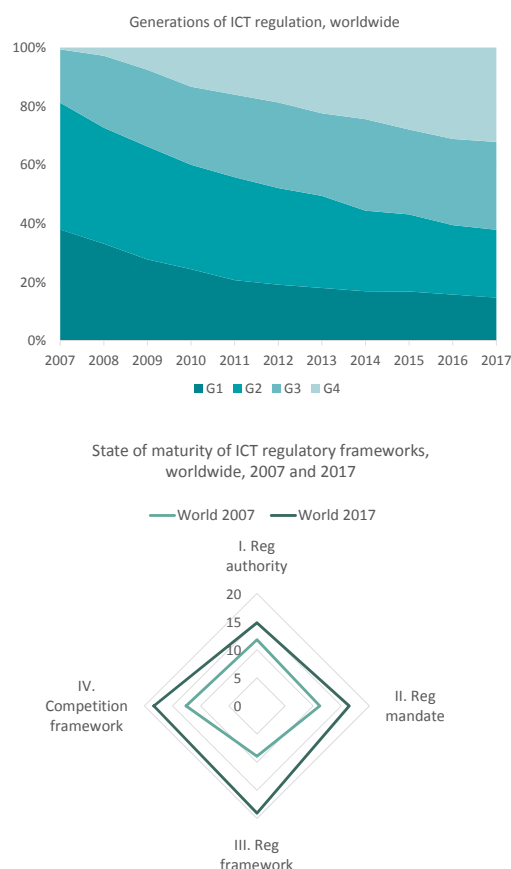
Note: The bottom chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points). Source: ITU

Europe rises impressively to the challenges of the digital economy with sound regulatory regimes, including veterans such as Portugal and Belgium as well as new entrants such as Latvia. Australia is the highest ranked non-European country, at eighth in the table. Latin America is the second most-represented region, featuring the Dominican Republic, Mexico and Brazil. Oman closes out the honorary top 25 country rankings to reflect the ambition of the Arab region in revamping much of their regulatory toolbox. Oman is also the only non-European new entrant in the world top 25 in 2017.

The 2017 ranking of the ICT Regulatory Tracker also reveals an improvement in the level of

Table 6: ICT Regulatory Tracker 2017, Top 25

Rank	Country	Score
1	Italy	97.3
2	Ireland	97
3	Finland	95
3	Lithuania	95
3	Malta	95
3	Portugal	95
3	Romania	95
8	Australia	94.5
8	Turkey	94.5
10	Norway	94
11	Greece	93.3
12	Croatia	93
12	Montenegro	93
14	Dominican Rep.	92.7
15	Hungary	92.5
15	Switzerland	92.5
17	Mexico	92
17	Belgium	92
17	Poland	92
17	Slovenia	92
21	Brazil	91.5
21	Latvia	91.5
23	France	90.5
23	Germany	90.5
25	Oman	90.3

Region	Countries in World top 25
Africa	0
Americas	3
Arab	1
Asia-Pacific	1
CIS	0
Europe	20

Source: ICT Regulatory Tracker 2017, itu.int/go/tracker

regulatory maturity across all regions (see Table 7). The regulatory divide persists, however, between Europe where four in five regulators have reached G4, or the fourth generation of ICT regulation, and the other regions. The Americas follow behind with 40 per cent and in Arab States 20 per cent of countries have reached G4. In Africa, Asia-Pacific and CIS, only around ten per cent of countries are in the most advanced generation of regulation, G4.

Table 7: G4 countries, worldwide, 2017

Region	G4 Countries	Score/%
Africa	Malawi	86.0
Africa	Kenya	87.5
Africa	Uganda	86.0
Africa	Ghana	88.3
Africa	**4**	**9%**
Arab States	Oman	90.3
Arab States	Saudi Arabia	90.0
Arab States	Morocco	88.5
Arab States	Bahrain	87.3
Arab States	**4**	**19%**
CIS	Georgia	90.0
CIS	Moldova	90.0
CIS	**2**	**17%**
Asia-Pacific	Malaysia	90.0
Asia-Pacific	Australia	94.5
Asia-Pacific	Singapore	89.0
Asia-Pacific	Pakistan	89.0
Asia-Pacific	**4**	**11%**
Europe	Greece	93.3
Europe	Ireland	97.0
Europe	Switzerland	92.5
Europe	Montenegro	93.0
Europe	Poland	92.0
Europe	Lithuania	95.0
Europe	Italy	97.3
Europe	Croatia	93.0
Europe	Turkey	94.5
Europe	Malta	95.0
Europe	Finland	95.0
Europe	Romania	95.0
Europe	Norway	94.0
Europe	Portugal	95.0
Europe	Hungary	92.5
Europe	Belgium	92.0
Europe	Slovenia	92.0

Region	G4 Countries	Score/%
Europe	Slovakia	90.0
Europe	United Kingdom	89.3
Europe	Iceland	88.0
Europe	Germany	90.5
Europe	Sweden	89.0
Europe	Netherlands	87.5
Europe	Denmark	87.7
Europe	Austria	89.5
Europe	Cyprus	87.0
Europe	Bosnia and Herzegovina	86.0
Europe	Spain	86.0
Europe	France	90.5
Europe	Estonia	87.0
Europe	Serbia	85.5
Europe	Albania	85.0
Europe	Latvia	91.5
Europe	**33**	**78%**
Americas	Dominican Rep.	92.7
Americas	Bahamas	88.8
Americas	Panama	86.0
Americas	Mexico	92.0
Americas	Chile	90.0
Americas	Saint Lucia	86.0
Americas	Ecuador	87.0
Americas	Trinidad and Tobago	85.3
Americas	Brazil	91.5
Americas	Peru	87.0
Americas	Argentina	90.0
Americas	Honduras	88.0
Americas	United States	88.5
Americas	Canada	85.5
Americas	**14**	**41%**
WORLD	**61**	**32%**

Source: ICT Regulatory Tracker 2017, itu.int/go/tracker

What does the ICT Regulatory Tracker do?
The Tracker pinpoints the changes taking place in the ICT regulatory environment. It facilitates benchmarking and the identification of trends in ICT legal and regulatory frameworks. The Tracker does not measure the quality, the level of implementation or the performance of regulatory frameworks in place, but records their existence and features. It helps track progress and identify gaps in regulatory frameworks, making the case for further regulatory reform towards achieving a vibrant and inclusive ICT sector.

For details, see the note on methodology and the annexes at the end of the report

3.2. Major regulatory trends

The past decade has seen considerable evolution of ICT regulatory frameworks. Regional disparities persist and both the pace and direction of change vary among countries. However, we discern major trends emerging over the past ten years based on the evidence provided by the ICT Regulatory Tracker. Large groups of countries have aligned their regulatory approaches in key areas – often based on the successful experiences of peers – and these have helped shape ICT regulation over the past decade.

Trend 1: National broadband plans dominate, replacing traditional universal service/access policies [▼]

Since 2007, the number of countries with a broadband plan have more than quadrupled to 155. That broadband both boosts the economy and facilitates social inclusion is today irrefutable. Policy-makers have raised broadband on their development and political agenda, opening the door for future technologies to reach everyone, everywhere – and approving the considerable investment needed to make this happen. The number of broadband plans has now reached a plateau however as policy attention shifts to new frontiers ranging from 5G to IoT and AI.

Trend 2: Spectrum reform unfolding [▲]

Spectrum reform has been ubiquitous, seeking to capitalize on spectrum as a means of achieving economic policy goals in view since the advent of 2G communications. Along with maturing 3G and 4G technologies, regulators have introduced more scrutiny over mobile operators and service providers. Forty-seven regulators are now entrusted with an exclusive spectrum monitoring and enforcement role. At the same time, regulators have also introduced flexible, adaptive regulatory practices. Of note, 106 countries have since 2007 allowed band migration while 42 have introduced spectrum trading. At least 90 countries have reallocated their digital dividend spectrum as a result of the analogue-to-digital migration, of which almost 90 per cent reallocated to mobile services. These developments have laid the groundwork for initial and subsequent 5G launches, their infrastructure requirements and the services that flow over them.

3: Tackling market dominance and competition [▲]

The past decade has seen a newly diverse face of ICT market player emerge – from independent tower companies to mobile virtual network operators (MVNOs) to digital platforms. The mainstream idea that regulation should provide a level playing field for all players is eroding; however, more practically, regulators have been shifting their focus from providing unified regulatory requirements and market conditions for all to targeting unfair use of market power. No fewer than 95 countries have adopted a legal concept of dominance or significant market power (SMP) since 2007, of which 91 have specific criteria to determine dominance or SMP. Over the same period, almost 60 countries have opened their mobile broadband markets to competition and 53 countries have liberalized their international gateways. These regulatory changes have helped amplify digital inclusion worldwide and have enabled the advent of digital platforms.

Trend 4: Infrastructure sharing [=]

Infrastructure sharing has been the mantra of many regulators – and market players – since the global financial crisis in 2007-08. Arguably, infrastructure sharing and open access have been key elements of most strategies to promote affordable broadband access.[1] Since 2007, infrastructure sharing has been mandated in an additional 76 countries, and co-location or site sharing has been mandated in 83 more. Forty-six countries have introduced regulation permitting infrastructure sharing for mobile operators over the past decade. With IoT on the horizon, sharing practices will multiply, from passive to active to spectrum sharing, and will involve a wide array of technologies and regulatory practices.

Trend 5: The growing importance of quality of service and experience [=]

A main factor driving the adoption of new technologies is quality of service and experience. If a service is unreliable, it will likely fail to become mainstream. Efficient regulatory tools and broad regulatory mandates in the area of quality of service and experience have helped drive the success of digital services. Almost 80 countries have introduced requirements for quality of service (QoS) monitoring since 2007, while in more

than 60 countries the ICT regulator has been in charge of QoS obligation measures and monitoring over the same period. Moreover, the quality of service of mobile broadband services is a 'make-or-break' condition for the introduction of digital services, from mobile money to e-health services.

Trend 6: VoIP [▼]

VoIP (voice over Internet Protocol) has been one of the most successful digital applications to date. Several options exist for handling VoIP – but have all been on the same part of the regulatory spectrum. Blocking the use of VoIP services on a permanent basis has proven neither desirable nor completely enforceable. In 2017, 156 countries allow individual users to use VoIP with roughly half of them (76) moving to authorize it over the past decade. Around 30 countries still ban VoIP – and most do not plan to allow it in the foreseeable future.

Trend 7: Number portability [▲]

Mobile has become the main medium of communication for many consumers over the past ten years. An important factor in enhancing mobile competition and reducing consumer prices has been number portability. The number of countries where mobile number portability is neither required nor available to consumers has almost halved, from close to 140 to 76. Although fixed number portability is lagging behind mobile, over 40 countries have either authorized or enforced this over the decade.

Trend 8: Converged regulatory structures [▲]

As observed in last year's Global ICT Regulatory Outlook report, the purview of the ICT regulator has evolved and expanded over the past decade. Converged regulatory structures have become common, growing from roughly one-third in 2007 to over 70 per cent in 2017. Sixty-eight ICT regulators have new oversight of broadcasting (radio and TV transmission), and close to 50 oversee IT.

Increasingly, ICT regulators address content of electronic communication or media services. Since 2007, over 45 ICT regulators oversee broadcasting content, and 35 Internet content. It is worth noting, however, that more government ministries are in charge of media and Internet content than

separate regulatory agencies – over 100 ministries are responsible for media and broadcasting content and almost 60 ministries are responsible for Internet content.

Trend 9: Simplified and converged licensing regimes [▲]

Operating licences are key to buoyant digital markets, and leaving the door open to operators and service providers has been effective in boosting competition and helping establishment of new business models. Over 60 countries have introduced unified licences or general authorization regimes over the period. Looking for alternative and complementary solutions for connectivity and service provision, some 50 new countries have introduced licence-exempt regimes for spectrum since 2007. This has enabled the global take-up of public – and often free – Wi-Fi systems, and will further pave the way for 5G.

Trend 10: Regulatory process is opening up [▲]

Driven by new market dynamics and social expectation, ICT regulators have begun to consult with market players and broader ecosystem stakeholders. Public consultations prior to major decisions have become mandatory in over 55 countries over the past decade. Regulatory processes have themselves become more open and collaborative. Regulators are considering innovative, out-of the box regulatory solutions such as regulatory sandboxes for enterprises wishing to test an emerging technology or innovative service without being bound by all the regulations that would normally apply as well as "start-up and experiment" interfaces to support start-ups, enterprises and communities in their experimental initiatives[2]. Regulators have become more responsive and accountable to their constituencies, and consumer appeals to regulatory decisions are now allowed in some 50 countries.

Collaborative regulation has been steadily gaining momentum, federating peer regulators from across the industry in addition to market players (see section 4.5). A cycle of successful regulatory reform is likely to perpetuate itself on the back of the growth of new technologies and the social and economic phenomena they engender.

Table 8: Top 10 regulatory reforms 2007-2017

Trend/indicators	2007 (countries)	2017 (countries)	Δ 2007-17	Country examples
1. National broadband plans have replaced traditional universal service/access policies linking broadband to economic growth and social good				
• National plan that involves broadband	36	155	119	Afghanistan, Bahrain, Slovenia, South Africa
2. Spectrum reform has been ubiquitous seeking to capture the value of spectrum for achieving development policy goals and, more recently but even more intensely, preparing the ground for 5G				
• Regulator in charge of spectrum monitoring and enforcement	• 98	• 145	• 47	Dominica, Mexico, Suriname, Tanzania
• Band migration allowed	• 30	• 139	• 109	
3. Tackling market dominance and competition				
• Legal concept of dominance/ SMP	• 43	• 141	• 98	Armenia, Costa Rica, Oman, Zambia
• Criteria used in determining dominance/ SMP	• 41	• 135	• 94	
• Level of competition in IMT (3G, 4G) services	• 98	• 158	• 60	
• Level of competition in international gateways	• 88	• 144	• 56	
4. Infrastructure sharing				
• Infrastructure sharing for mobile operators permitted	• 115	• 164	• 49	Benin, Brunei Darussalam, China, TFYR Macedonia
• Infrastructure sharing mandated	• 43	• 122	• 79	
• Co-location/site sharing mandated	• 38	• 124	• 86	
5. Quality of service regulations have set high standards for consumer protection				
▢ Quality of service monitoring required	86	166	80	Grenada, Liberia, Montenegro, Nepal
6. VoIP has become a mainstream service				
• Individual users allowed to use VoIP	77	156	79	Antigua and Barbuda, Iran, Lesotho, Myanmar
7. Moving towards converged regulatory structures				
ICT Regulator in charge of:				
• Broadcasting (radio & TV transmission)	• 49	• 117	• 68	Croatia, Lithuania, Malawi, Nicaragua
• Broadcasting content	• 17	• 62	• 45	
• Internet content	• 6	• 41	• 35	
• IT	• 25	• 72	• 47	
8. Mobile number portability has become the norm, fixed following behind				
• Number portability required from mobile operators and available to consumers	28	85	57	Cabo Verde, Greece, Honduras, India
9. Simplified and converged licensing regimes				
• Unified licences/ general authorization	• 64	• 114	• 50	Bahamas, Fiji, Guatemala, Sudan
• License exempt	• 2	• 52	• 50	
10. Regulatory process is opening up				
• Public consultations mandatory before major regulatory decisions are made	• 84	• 143	• 59	Kyrgyzstan, Liberia, Romania, Uganda
• Appeals to the decisions of the regulator are allowed	• 117	• 169	• 52	

Source: ITU, ICT Regulatory Tracker 2007-2017

3.3. Each region is unique

Regional trends provide key insights into patterns of progress towards better regulatory frameworks for the ICT sector. The following is a bird's-eye view of the six regions, with a focus on i) what has changed and ii) where to expect further change.

Africa in 2017

- There is a tight regulatory 'race' involving eight countries occupying the top 5 rankings (see Table 9). Only a three-point difference separates the top country from fourth place. This top group is equally spread across the third (G3) and the fourth generation (G4) of ICT regulation.

- Four countries are part of the 61-strong, global G4 contingent. It has taken Africa a mere ten years to nurture these regional champions, since Uganda first attained G4 status in 2009.

- Ghana and Kenya keep their leading positions in the region although their scores remain unchanged since 2015.

- The region is home to countries in all stages of regulatory maturity and the 65-point discrepancy between the highest and lowest scoring country is large. Half of the countries are of G1 and G2 status combined, while the other half is of combined G3 and G4 status.

Table 9: Top 5 Africa, 2017

		Score	Generation	Rank
1	Ghana	88.3	4G	41
2	Kenya	87.5	4G	45
3	Malawi	86.0	4G	52
3	Uganda	86.0	4G	52
4	Botswana	84.0	3G	63
4	Burkina Faso	84.0	3G	63
4	Cabo Verde	84.0	3G	63
5	Tanzania	80.0	3G	81

Source: ICT Regulatory Tracker, itu.int/go/tracker

- The evolution of Africa's scores tracks world averages, and in fact ranks above averages of Arab States, Asia-Pacific and CIS.

- Eight of ten countries are split across G2 and G3 status. Within these categories is where the most rapid regulatory evolution is happening, with 10 per cent graduating from G2 to G3 over the past four years.

- Africa is the region where regulatory frameworks have most evolved over the past ten years. 3G countries have increased in number from five to 40 per cent in ten years. In 2007, more than half of Africa were of G1 status – in 2017, only four LDCs remain in this lowest tier. Their scores reveal much remains to be done to advance to G2: considerable support will be required to ensure these countries move ahead on their journey towards meaningful regulatory reform.

Figure 11: Evolution of regulatory frameworks, Africa, 2007-2017
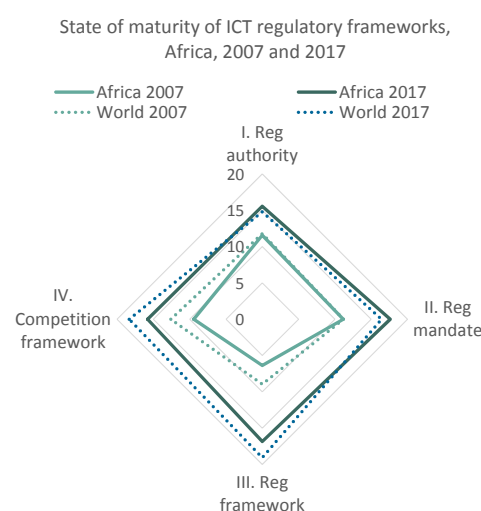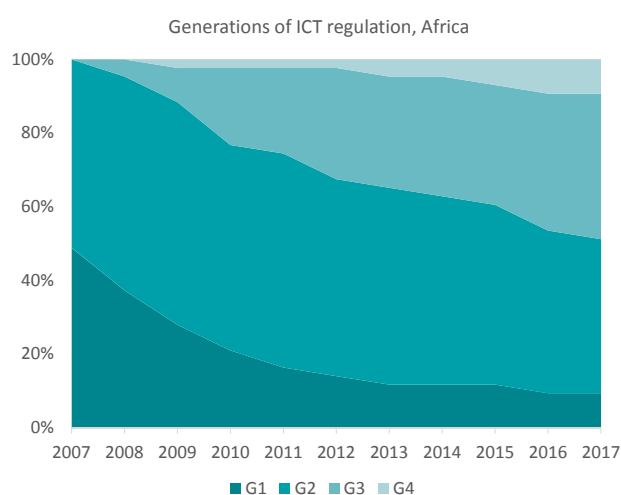
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

Americas in 2017

- The leader within the region is the Dominican Republic, which is also the second-highest scored non-European country (see Table 10). Mexico, also in the world top 25, trails the Dominican Republic by a single point of the ICT Regulatory Tracker. Six countries rank as top 5 in the region – of these, five are from Latin America, trailed by the Bahamas, a Caribbean State. No Americas country was part of the worldwide top 5 in 2007 and none was of G4 status.

- Fourteen countries have attained G4 status. The region has experienced the strongest growth in the average scores between 2007 and 2017, with current scores above the world average, and growth has been more homogeneous than in other regions such as Africa and Asia Pacific.

- Less than a third of countries are of combined G1 and G2 status, compared to nine out of every ten countries in 2007.

Table 10: Top 5 Americas, 2017

		Score	Generation	Rank
1	Dominican Rep.	92.7	4G	14
2	Mexico	92.0	4G	17
3	Brazil	91.5	4G	21
4	Argentina	90.0	4G	26
4	Chile	90.0	4G	26
5	Bahamas	88.8	4G	38

Source: ICT Regulatory Tracker, itu.int/go/tracker

- Less than a third of countries are of G3 status – an area which has evolved at a dynamic pace. Since 2010, 20 per cent of countries in the region have moved from G2 to G3, although the pace has now slowed and there has been little movement since 2015. Notably, however, 40 per cent of the countries have graduated from G3 to G4 since 2010 and three of the remaining countries are close to achieving G4 status.

Figure 12: Evolution of regulatory frameworks, Americas, 2007-2017
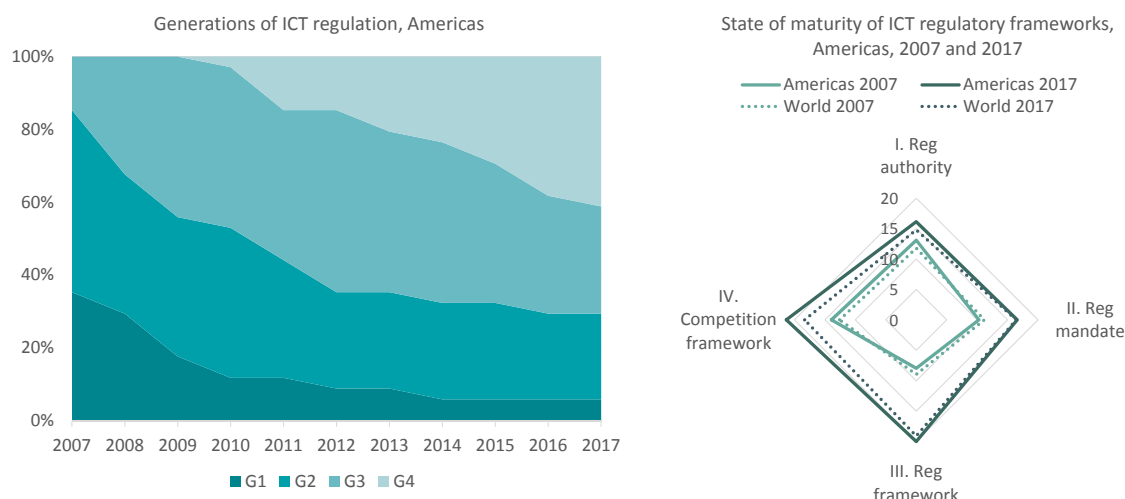
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

Arab States in 2017

- The region is led by Oman, the only Arab State in the world top 25, ahead of Saudi Arabia by a marginal difference (see Table 11). One of every five Arab States – four in total – was of G4 status as of 2017, while four more are within four points of attaining G4 status.

- Progress up the 'generation ladder' has been slower than in most other regions, although the pace is likely to accelerate over the next two years with major reforms in the pipeline in a number of Arab States.

- Notably, 60 per cent of countries are of G3 and G4 status – in 2007, only 10 per cent of countries had attained G3 status while none had attained G4 status.

Table 11: Top 5 Arab States, 2017

		Score	Generation	Rank
1	Oman	90.3	4G	25
2	Saudi Arabia	90.0	4G	26
3	Morocco	88.5	4G	39
4	Bahrain	87.3	4G	47
5	Egypt	84.3	3G	62

Source: ICT Regulatory Tracker, itu.int/go/tracker

- Most of the movement in the region has resulted from G2 countries leaping to G3 and, to a lesser extent, from G3 countries moving up to G4.

- The number of G1 countries has almost halved since 2007; however, a quarter of all Arab States remain in G1 – some with scores as low as 3 points in the ICT Regulatory Tracker.

Figure 13: Evolution of regulatory frameworks, Arab States, 2007-2017
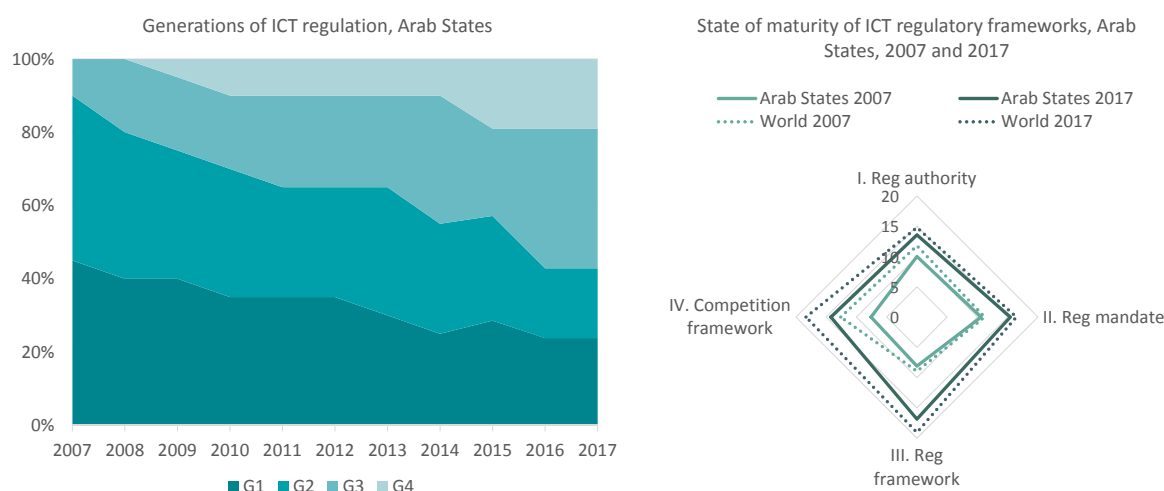
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

Asia-Pacific in 2017

- Australia tops the Asia-Pacific top 5 (shared by six countries) while placing eighth in the world ranking – and also features as the highest-ranked non-European country (see Table 12).

- Only four countries – one in ten – have attained G4 status, a performance comparable to the figures for Africa. No new countries have attained G4 status since 2012.

- In terms of average annual scores, Asia-Pacific and Arab States follow a similar pattern with scores at around ten points below the 2017 world average.

- With the exception of Africa, Asia-Pacific presents the most diverse range of countries in terms of regulatory maturity.

- Globally in 2007, almost half of the countries in the region were of G1 status and only 8

Table 12: Top 5 Asia-Pacific, 2017

		Score	Generation	Rank
1	Australia	94.5	4G	8
2	Malaysia	90.0	4G	26
3	Pakistan	89.0	4G	35
3	Singapore	89.0	4G	35
4	Hong Kong, China	82.8	3G	71
5	Thailand	82.3	3G	73

Source: ICT Regulatory Tracker, itu.int/go/tracker

per cent were G3, while none had attained G4 status. In 2017, the region splits equally between G1 and G2 combined on the one hand, and G3 and G4 combined on the other.

- Looking more closely at sub-regions, some divergence appears. While in East Asia and the Pacific a third of the countries are of G1 status, South Asia has none and over half of the countries are of G2 status. A third of South Asian countries are G3 status, compared to close to 40 per cent in the rest of the region.

Figure 14: Evolution of regulatory frameworks, Asia-Pacific, 2007-2017
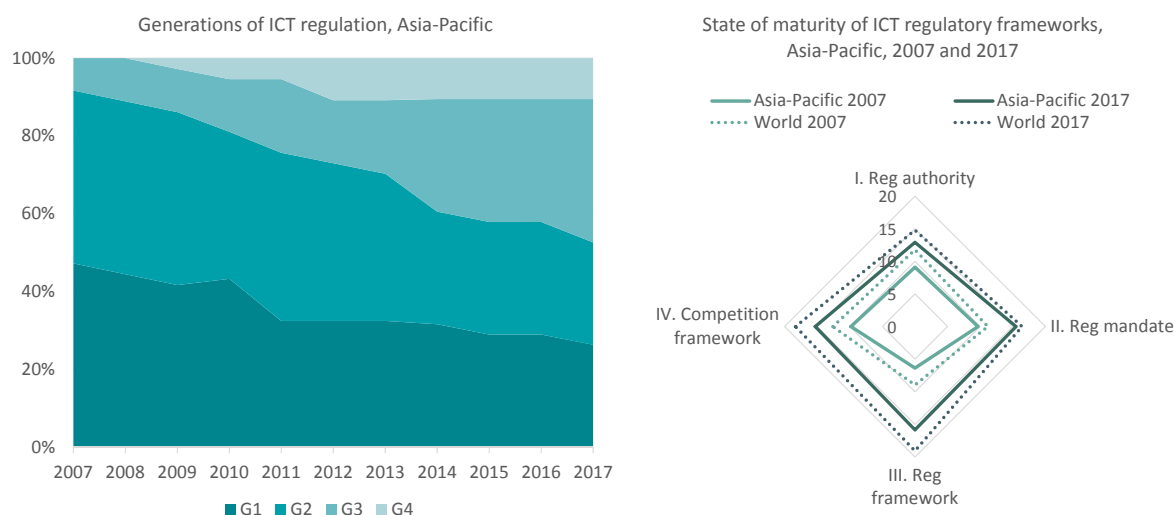
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

CIS in 2017

- Georgia and Moldova[3] top the CIS ranking and stands out as the only G4 countries in the region (see Table 13).

- CIS is the only region featuring a G2 country in its top 5.

- Despite the relatively small number of countries in the region, disparity of regulatory maturity is particularly marked. While the top CIS countries place at 26th in the world ranking, the fifth stands at the 133rd world spot, with a G2 status.

- The region has made steady progress since 2007. Eleven of 12 countries were either of

Table 13: Top 5 CIS, 2017

		Score	Generation	Rank
1	Georgia[56]	90.0	4G	26
1	Moldova[56]	90.0	4G	26
3	Armenia	83.5	3G	67
4	Kyrgyzstan	74.5	3G	98
5	Azerbaijan	62.3	2G	133

Source: ICT Regulatory Tracker, itu.int/go/tracker

G1 or G2 status in 2007 and boasted a single G3 country. In 2017, four countries have progressed to G3 and G4 status.

- Overall, the evolution of regulatory frameworks in CIS is moving at a slower pace, with average annual scores since 2007 consistently below the world average.

Figure 15: Evolution of regulatory frameworks, CIS, 2007-2017
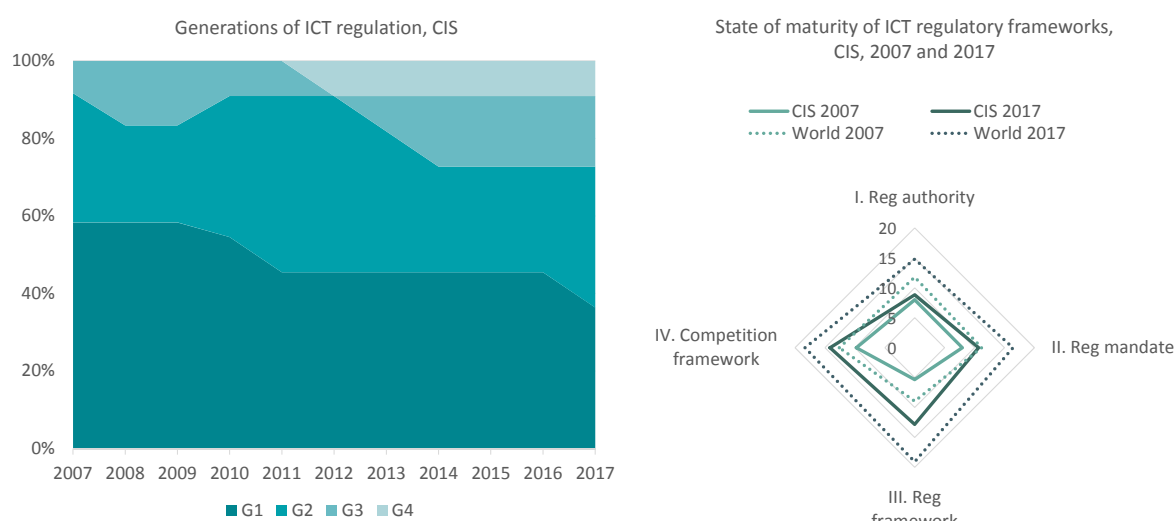
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

Europe in 2017

- Italy tops both European and world rankings, with a score of over 97 points in the ICT Regulatory Tracker (see Table 14). The European top 5 is effectively the world top 5. Last year's champion, Ireland, moves to an honourable second spot with an unchanged score.

- Europe was the first region to produce a G4 regulator, Belgium, the first and only country in the world to have attained this status in 2007. Since then, Europe has been the cradle of the largest G4 community, with no fewer than 43 G4 regulators in 2017 – four of every five European regulators are G4 regulators.

- The annual average scores of Europe have been consistently the highest globally since 2007. Nevertheless, the gap between European annual average scores and the world averages has halved from over 40 per cent in 2007 to close to 20 per cent in 2017.

- Regionally-coordinated regulatory reform over the past 20 years have provided fertile ground for the transformation and maturing of European regulations and for a steady,

Table 14: Top 5 Europe, 2017

		Score	Generation	Rank
1	Italy	97.3	4G	1
2	Ireland	97.0	4G	2
3	Finland	95.0	4G	3
3	Lithuania	95.0	4G	3
3	Malta	95.0	4G	3
3	Portugal	95.0	4G	3
3	Romania	95.0	4G	3
4	Turkey	94.5	4G	8
5	Norway	94.0	4G	10

Source: ICT Regulatory Tracker, itu.int/go/tracker

inclusive advance towards G4 status across the region.

- Six G3 countries, mostly Eastern European, are advancing towards G4 status – five of which are within four points of attaining G4 status.

- Three countries remain at G1 status, while no country is of G2 status. Apart from Andorra which is planning to create a separate regulator, the remaining G1 countries are unlikely to join the ICT regulation generation race, since their limited market size will not justify onerous regulatory reforms.

Figure 16: Evolution of regulatory frameworks, Europe, 2007-2017
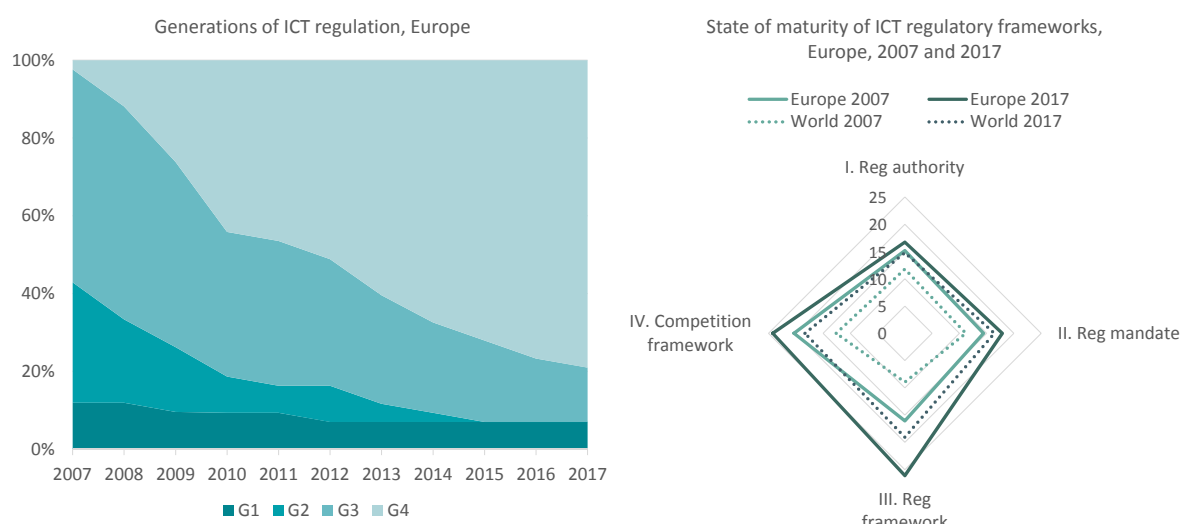
Note: The right chart shows the evolution of the average scores of the ICT Regulatory Tracker, per pillar (in points).
Source: ICT Regulatory Tracker, itu.int/go/tracker

Endnotes

1   GSR09 Best Practice Guidelines on infrastructure sharing: https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/consultation_contributions/GSR09_BestPractice_E.pdf

2   GSR-18 Best practice guidelines on new regulatory frontiers to achieve digital transformation, https://www.itu.int/net4/ITU-D/CDS/GSR/2018/documents/Guidelines/GSR-18_BPG_Final-E.PDF

3   Georgia, Moldova and Ukraine joined the Europe region in 2018

4. Policy and regulatory trends

'Communicare' in Latin means 'to share' while the Latin for regulation means to lead as well as control through adherence to rule. Both qualities – sharing and leading – are moving increasingly centre-stage for regulators worldwide.

The history of telecommunications, Internet and augmented digital media reflects a journey towards sharing, a celebration of shared ideas, triumphs and disappointments. The essential need to share has driven technological innovation across time and geographies.

Has regulation helped in the journey? Until the new millennium and the digital era, the nature of regulation had very much been about command and control. Its nature has seen significant evolution nowadays – and the nature and quality of leadership have become central to regulation. Today's regulation has also become a process, embracing collaboration and shared reflection of the complexities at hand.

The following sections throw light on how policy and regulatory approaches have evolved and examine the main challenges. The analysis builds on unique and authoritative ITU data about regulatory practices across Member States. It charts the road ahead in finding the right balance for every market and consumer group. It is not intended to provide a comprehensive view – nor does it define any one approach as 'correct'. Our aim is to make a measured, authoritative and evidence-based contribution to important public discourse on high-profile regulatory issues, informing and helping guide decision-making in fast-changing digital markets.

4.1. The regulator

In earlier years ICT regulators were watchdogs, gatekeepers and arbiters. Their role has evolved to that of facilitator and partner in shaping ICT and digital markets. The job of a modern-day regulator involves a degree of Socratic questioning: is it best to have or not to have certain regulations – and best for whom? What regulations will lead most

Figure 17: ICT regulators, by region, 2017

Telecom/ICT regulators, by region, 2017

Telecom/ICT regulators, by region, 2017

Region	%
Europe	93%
CIS	94%
Asia & Pacific	86%
Arab States	72%
Americas	45%
Africa	86%

Pie chart: Africa, 41; Americas, 32; Arab States, 18; Asia-Pacific, 30; CIS, 4; Europe, 39

Remit of the ICT regulator, worldwide, 2017

ICT-centric Multi-sector Converged* countries
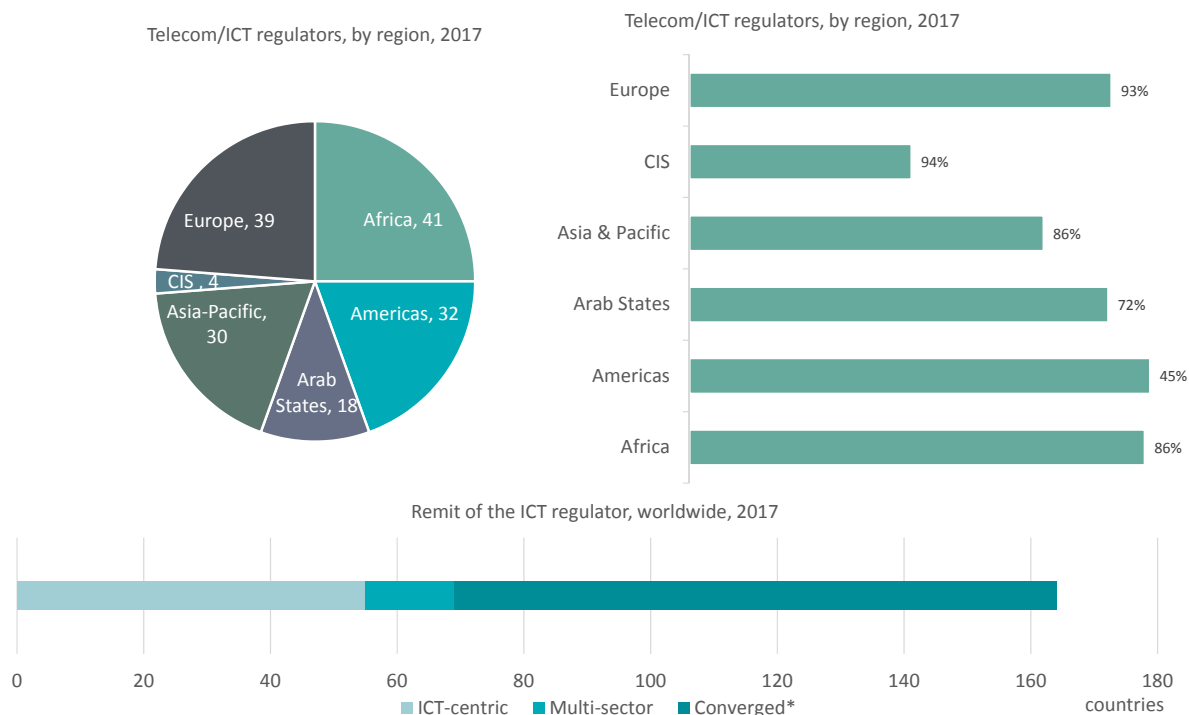
Notes:
1) Total: 164 regulators (2017)
2) Data for 190 countries and economies based on the ICT Regulatory Tracker 2017.
3) The values correspond to the number of regulators per region.
4) Converged refers to a regulatory mandate including broadcasting transmission and/or broadcasting content.
Source: ITU

Figure 18: Power profile of the ICT regulator, 2017

ICT regulator autonomous in decision-making, worldwide, 2017

ICT regulator has enforcement power, worldwide, 2017

Sanctions or penalties imposed by the regulator, worldwide, 2017

12%, No

87%, Yes

21%, No

79%, Yes

9%

6%

85%

■ Heavy sanctions   ■ Light sanctions
■ No sanctions
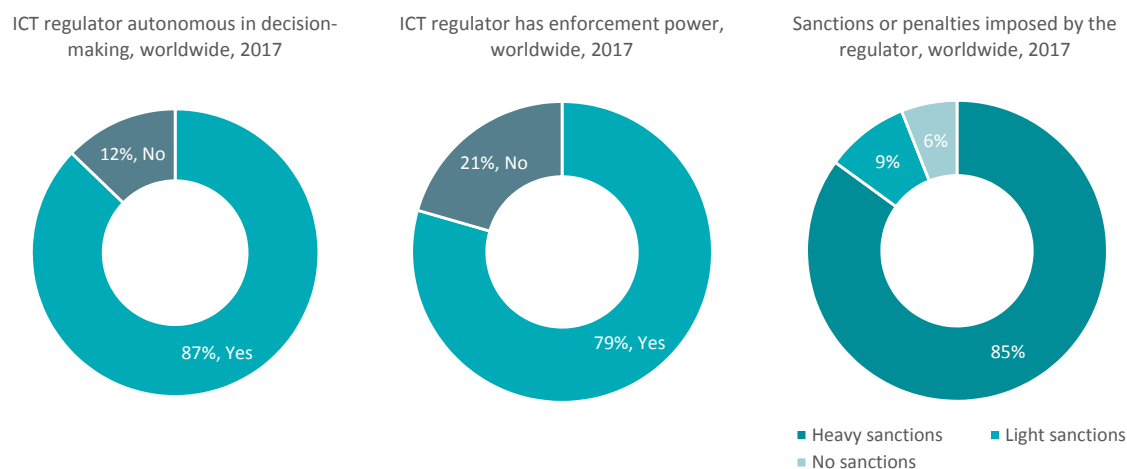
Source: ICT Regulatory Tracker, itu.int/go/tracker

effectively to social and economic goals? What shelf life should regulations have? The eyes of market players and consumers are on regulators for guidance, consent and protection. They have become the sherpas of the digital transformation and guardians of its growing pains.

ICT regulators worldwide number 164 at the end of 2017, and the trend of creating new, separate regulatory agencies seemed to have reached a plateau. Only eight regulators have been created between 2007 and 2017, with not a single new regulator in 2017. However, a new wave is coming. The National Communication Authority of Somalia[1] and the Nauru Communications Authority[2] were established in 2018. In Niger, a new law regulating electronic communications was adopted in 2018 along with a new law establishing the Regulatory Authority for Electronic Communications and Post (Autorité de Régulation des Communications Electroniques et de la Poste, ARCEP).[3] A handful of countries is in the process of being established or are planning to establish a regulator. Azerbaijan, Ethiopia, Micronesia, Myanmar, the State of Palestine, Seychelles and Tonga are all on their way to establishing a separate regulator.[4] Thus, Africa is set to become the first region where every country has a separate ICT regulator.

Roughly nine out of ten countries in the Americas, Africa, Arab States and Europe have a separate regulator as of 2017 (see Figure 17). Asia-Pacific is the probable growth area for the coming decade, with nine countries yet to establish a regulator. CIS is the only region where a majority of countries

retain the ICT regulatory role within the sector ministry itself.

As of 2017, only a third of all regulators deal solely with the traditional ICT sector. Six of every ten are 'converged regulators' with additional responsibility for broadcasting, and in some cases having a remit that extends to Internet content. Outside the ICT sector, fewer than one in ten regulators oversee multiple sectors, from energy to roads, and the creation of such regulators hasn't gained much traction beyond the initial wave that occurred in early 2000.

An emerging – and intensifying – trend over the past decade has been the move towards the 'converged regulator'. As technological convergence sweeps the sector, regulatory coherence must extend beyond the limits of traditional ICT to encompass a range of market players and digital services, albeit with both positive and negative implications.

For example, in Zimbabwe, the country has merged media and communications watchdogs to create a single converged regulator[5] combining the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) with the Broadcasting Authority of Zimbabwe (BAZ). In 2018, Vanuatu also moved to give a broadcasting and media mandate to TTR, the ICT regulator, and will host the 2019 ITU Global Symposium for Regulators (GSR).

Regulators' names also evolve to reflect their changing mandate and scope. The Telecom Regulatory Authority of India (TRAI) will become the Digital Communications Regulatory Authority of India (DCRAI), while the Telecom Commission – the Department of Telecommunications' (DoT's) highest decision-making body – will be renamed as the Digital Communications Commission (DCC).[6]

Originally simple extensions of sector ministries, ICT regulators have come a long way over the past 20 years, extending their remits as well as their powers. As of 2017, three of every four regulators are autonomous in their decision-making, with 43 regulators (more than a quarter of all regulators) acquiring the power of enforcement since 2007 (see Figure 18).

Today, almost all regulators have power of enforcement and the mandate to impose sanctions ranging from monetary fines to removal of officials (see Figure 18). Only ten regulators worldwide are still to be given an enforcement mandate. Eight of every nine regulators can impose heavy sanctions, and one in ten only light sanctions as of 2017.

Increasing importance of the ICT regulator's role

Clearly, the role of ICT regulator has grown significantly in stature and authority. As the pace of convergence and interconnectedness of ICTs across national economies accelerates further, the ICT regulator is engaging with new issues, increasingly acting across sectors and generally forging a more extensive, more challenging and more influential role.

Looking at digital services (see Figure 19) broken down into infrastructure, service delivery and content, the ICT regulator is the dominant figure, with highest operational capacity and outreach:

• Nearly 90 per cent of countries worldwide have established a separate ICT regulator for ICT infrastructure and services.

• In a quarter of all countries, they also regulate content (either for broadcasting or media in general, or over the Internet).

• Although sector-specific regulators (such as energy and spectrum regulators) or other overarching agencies (such as competition and consumer protection authorities) are equally well-established, their purview remains limited to no more than two of the three core areas of

Figure 19: Regulatory ecosystem for digital services

• 📱 ICT regulator
• 🔒 Data protection regulator
• 🌐 National committee
• 🛒 Consumer protection
• ((•)) Broadcasting regulator

• 💰 Financial regulator
• 🧍 Energy regulator
• 👥 Competition regulator
• ▮▮▮ Spectrum regulator
• 🛡 Cybersecurity
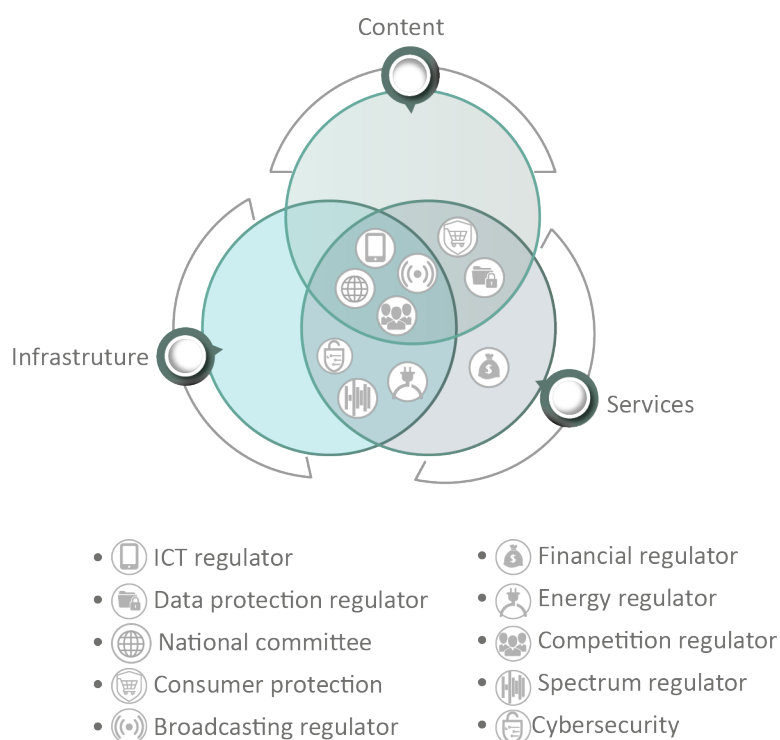
Regulators involved in the digital ecosystem, worldwide, 2018

Category	Value
ICT	164
Competition	131
Consumer protection	94
Data protection	98
Financial	173
Broadcasting	92
Spectrum management	21
Internet	14
Energy	143
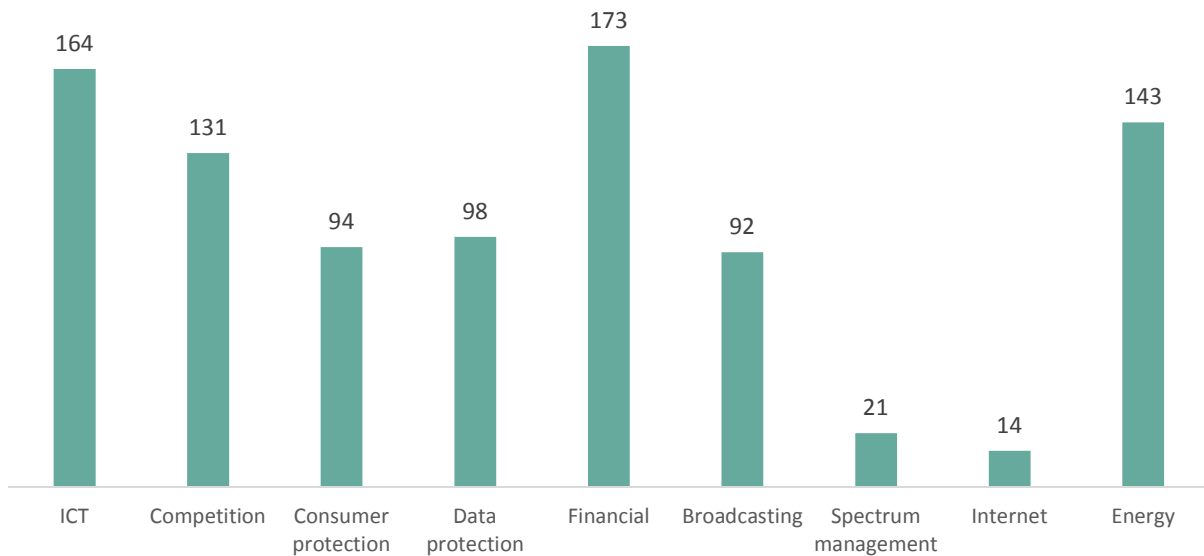
Source: ITU

the digital ecosystem – infrastructure, services and content.

- The ICT regulator outweighs other regulators in terms of institutional capacity, with two-thirds of countries having a competition authority and a financial regulator, while all types of regulatory agencies are functional in less than half of all countries.

- Arguably, the ICT regulator has considerable convening power and is of relevance to other national regulators in every country.

- ICT regulators have a unique mandate to tackle thorny, cross-cutting, cross-industry and transnational issues of the digital economy

– and an imperative to collaborate with peer regulators to come up with high impact, coherent regulatory responses.

In Australia, Burkina Faso, Colombia and Poland, consumer protection and competition issues are handled by a single congregated regulator, part of a wider trend of institutional convergence. Such overarching agencies tend to absorb sector-specific or multi-sector agencies such as the ICT regulator. The trend is not yet global but does involve multiple regions. This is the case for a few European agencies (Denmark, the Netherlands) as well as in East Asia and the Pacific (New Zealand) and the Caribbean (Trinidad and Tobago). This trend will continue, given the pervasiveness of digital technologies in all walks of life.

4.2. Policies for digital

ICT policies have formed the bedrock for regulators and both have evolved together to address market failures and to respond to social demands and expectations. And the spectrum of policy goals has widened significantly over the past three decades (see Figure 20), ranging from ensuring everyone can have access to a fixed phone within walking distance right through to capturing the potential of AI for the digital transformation of societies. While most digital policies currently focus on stimulating investment in broadband networks and connecting uneconomic areas, a fast-growing community of countries is looking ahead and gearing up for 5G, IoT and AI – and beyond.

Digital policy frameworks are currently dominated by ICT-centric policies, such as classic telecom universal access and service (UAS) policies, ICT policies and broadband plans. Broadband plans outnumbered UAS policies by almost 30 per cent, reaching 155 in 2017 (see Figure 21). A third of countries worldwide have adopted ICT accessibility policies for persons with disabilities, redefining digital inclusion. UAS policies and broadband plans have now reached a plateau; very few countries have adopted new such policies since 2012, while accessibility policies are on the rise. There is likewise a clear trend towards more holistic approaches to harness the benefits of the digital economy.

Proliferation of national broadband plans

National broadband plans have been trending in popularity since the last world financial crisis in 2008-09, until recently. In 2017, eight out of ten countries worldwide (or a total of 155) had a broadband plan of some sort and the trend is consistent across all regions (see Figure 22). Europe has been the trendsetter and leader as virtually all European countries today are tooled up with a set of targeted broadband policy principles. In Africa, the Americas and Asia-Pacific, around 80 per cent of countries have a plan, close to the world average.

The proportion in Arab States is slightly lower, around 70 per cent, and the approaches taken vary. In Bahrain, the TRA regulates the sector in accordance with the national telecom plans, while in Saudi Arabia and UAE, regulators implement broader national policies (e.g., the Saudi Vision 2030 and the UAE Vision 2021).[7]

CIS countries come last, mainly because of the small size of the region, with roughly two-thirds of countries with a plan. More than a dozen countries are planning to adopt a plan, including Afghanistan, Bosnia and Herzegovina, Moldova, Somalia and Tonga; however, many of them will likely have a different spin than the current – and diminishing – wave of reactive broadband plans.

As an upgrade to existing UAS polices or broadband plans, a number of regulators have recently upgraded their UAS definitions or terms of service. One example is the Slovenian telecom regulator, AKOS, which included 4 Mbps

Figure 20: Changing focus of ICT policies

Access to fixed/ mobile/internet
- UA
- US

Broadband investment, access & use
- ICT master plans
- Broadband plans
- NGN/NGA strategies

Digital integration
- Digitization, automation
- Digital transformation
- Smart cities
- ICT accessibility

Digital enablers
- 5G
- IoT
- AI
- DFS
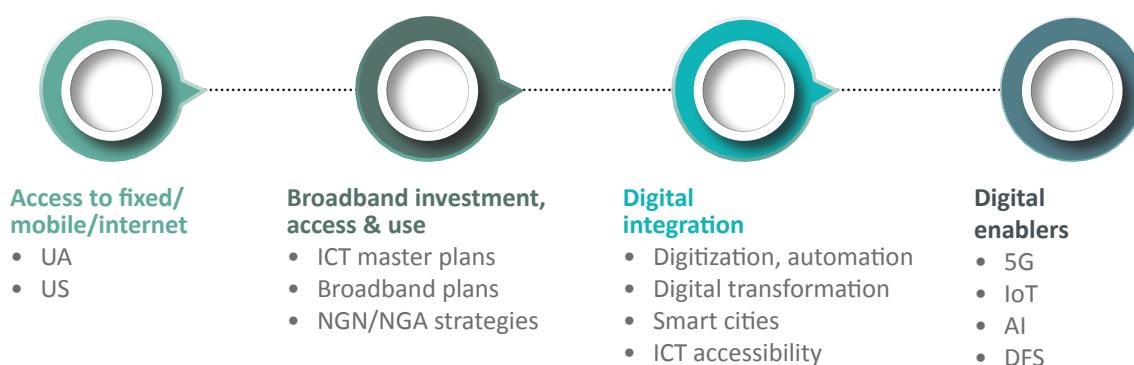
Note: UA = Universal access; US = Universal service; NGN/NGA = Next generation networks/ access; IoT = Internet of things; AI = Artificial intelligence; DFS = Digital financial inclusion

Source: ITU

Figure 21: ICT-centered polices, worldwide, 2017
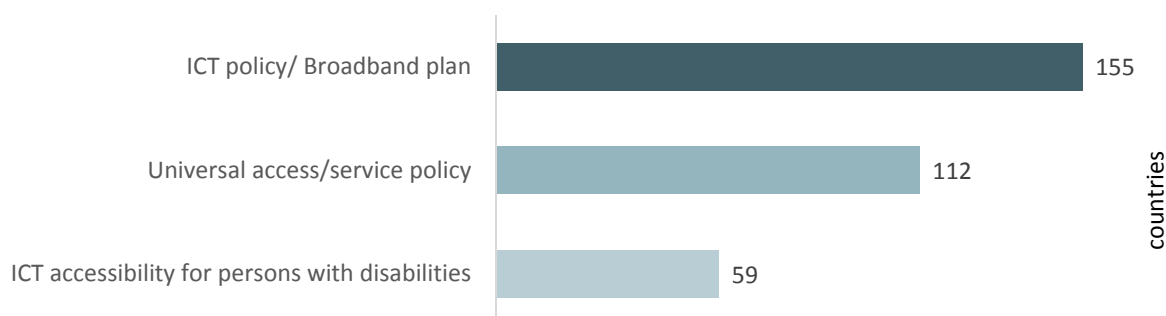
Source: ITU

broadband in the scope of the universal service obligation (USO) in 2018.[8] The USO broadband obligation is technology neutral and can be provided using fixed, fixed-wireless and satellite broadband access.

A new generation of digital policies is coming of age

This new generation reflects a holistic view of economy and society, with policies that address the digital ecosystem as a macrocosm for development, economic transformation and growth. They focus on the interplay between digitization and social and economic order and impacts on governments, national and global businesses, communities and individual citizens. These policies also incorporate interdependence and integration of digital across industries and cultures, while recognizing the transnational flows of digital data, services and content. The current rapid (and sparsely documented) trend in this regard is the adoption of national policies focusing on digital enablers, from the fast-approaching 5G to the more equivocal blockchain and robots. Some new examples of such policies include:

• National Productive Plan of Argentina;

• China Manufacturing 2025;

• Digitising European Industry Strategy for EU countries;

• Industrie du Futur in France;

• Industrie 4.0 in Germany;

• Make in India;

• Manifattura Italia in Italy;

• New Robot Strategy in Japan;

• National Strategy for Blockchain in Kenya;

• Manufacturing Innovation 3.0 in the Republic of Korea;

• National Technology Initiative in Russian Federation;

• Industria Conectada 4.0 in Spain.[9]

We expect the current twin trend to dominate over coming years, helping to push through policies with a more general focus on digital transformation on the one hand, and with focus on a specific enabler on the other.

Current, revised and fresh spectrum policies are thriving as a proxy for digital enablement. Unlike most other policies, virtually all countries have spectrum policies. In the EU, efforts are under way to harmonize radio spectrum in the 3.4-3.8 GHz and 26 GHz bands to facilitate the deployment of 5G in Europe as set out in the 5G roadmap.[10] Constantly seeking an enabling policy environment for the launch of 5G services, ARCEP France has issued new policy principles to reallocate frequency for 5G spectrum bands, and is writing new obligations into operators' licences.[11]

A spectrum of policies and regulatory frameworks

The digital economy has evolved under varied policies and regulatory frameworks. And while today's digital economy is booming, a unified and

Figure 22: National broadband plans adoption, worldwide, 2017

National policy, strategy or plan involving broadband, by region, 2017

% of countries per region having a national policy, strategy or plan involving broadband, 2017

Europe, 41
Africa, 33
CIS , 7
Americas, 27
Asia-Pacific, 32
Arab States , 15

Region	%
Africa	95%
Americas	64%
Arab States	84%
Asia-Pacific	71%
CIS	79%
Europe	76%
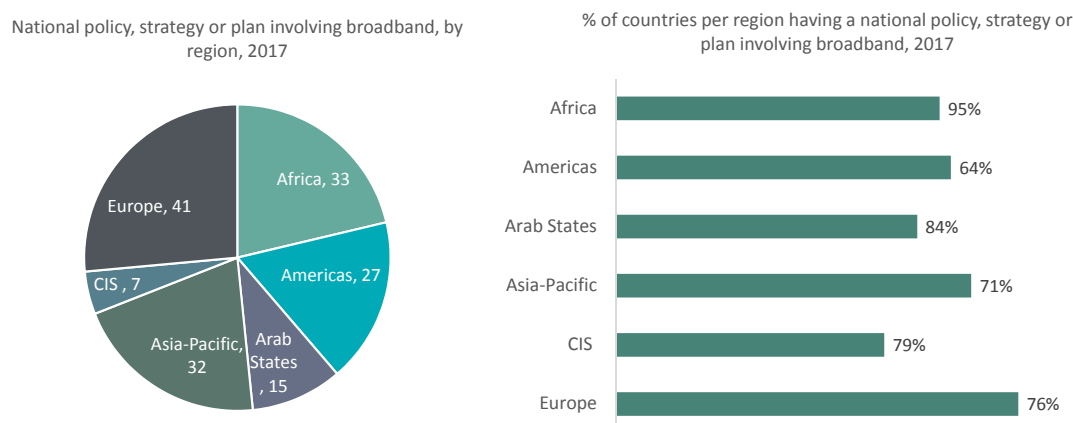
Total 2017: 158 countries, 82% of all countries

Note:
1) A national broadband plan or strategy typically includes: a plan, strategy or policy specific to broadband; digital plan, agenda, strategy or policy; ICT plan, strategy, or policy; or a communication plan, strategy, or policy.
2) The figures in the pie chart (left) correspond to the number of countries with a national broadband plan in each region.
Source: ITU, ICT Regulatory Tracker 2017: itu.int/go/tracker

strategic tech-for-good vision is conspicuously absent. Individual countries are pursuing individual courses and there is little consensus on an optimal policy approach. The wide spectrum of policy approaches in use is staggering (see Figure 23):

- **Wait and see**. Some countries are taking a prudent wait-and-see approach on response to the contentious issues currently shaking the unfolding digital economy, such as net neutrality and cloud computing. Other issues, such as conduct on digital platforms, remain largely unaddressed at policy level until recently. The time has come for clarifying the roles and responsibilities of market players vis-à-vis governments and consumers – and the volume of policies in this area is growing rapidly, with regional patterns emerging (see the discussion on digital platform regulation in Section 4.4). Also needed are policies that address the Internet of Things and digital apps. The volume of specific policies, for example in regard to ICT counterfeiting, is steadily growing – although not fast enough to counter negative impacts of counterfeit devices on consumer protection and well-being.

- **Aligned with national policy and priority**. In some key areas, most countries are aligned with a national policy. Aspirations for broadband investment have generated many national broadband plans worldwide. Similarly,

national tables of frequency allocation are bringing order to wireless broadband practices in line with national priorities – while dispute resolution frameworks are building confidence in markets and have equipped governments to handle disputes in a non-traditional, digital environment.

- **Absence of policy or framework**. There have been varied responses to major trends related to deep-seated issues which have emerged in the telecom era. Current levels of foreign ownership policy are significantly below expectations in the context of 20-year old multi-lateral trade in telecoms agreements (GATS). And in regard to VoIP, a technology that has been hugely empowering for ICT users, the absence of an explicit regulatory framework in many countries can be seen as a regulatory loophole. Similarly, the lack of an ICT consumer protection framework and of cybersecurity policy in many countries is a cause of concern (see also the discussion on consumer protection in section 4.3 and data protection in section 4.4).

Figure 23: Recent evolution of policy and regulatory frameworks, worldwide, 2012-2017
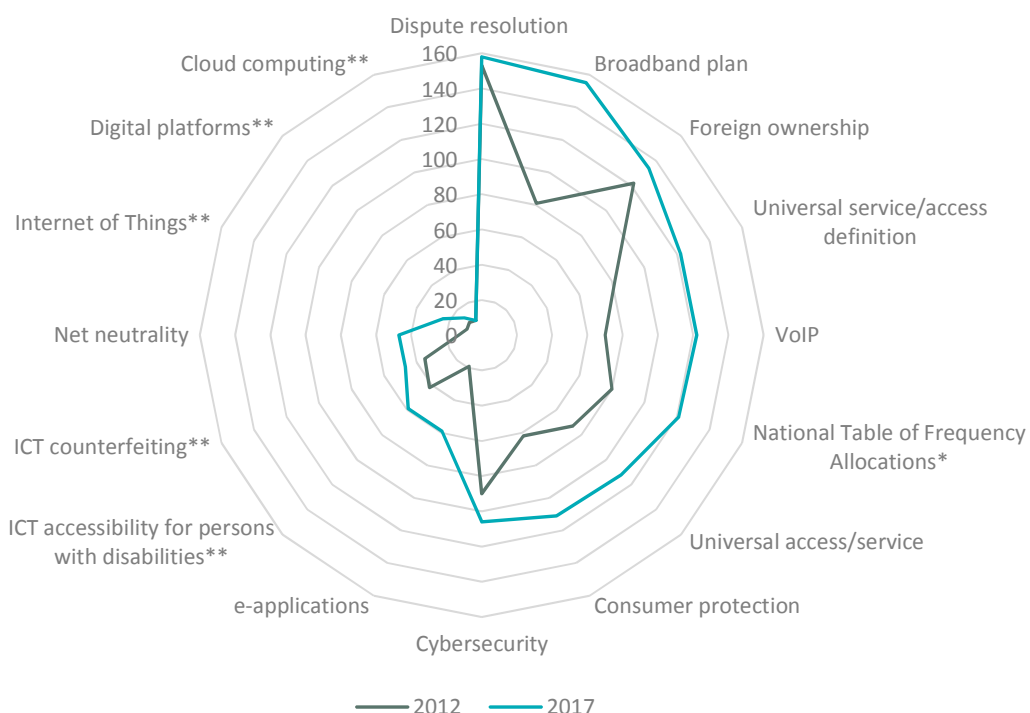
Note: *2013 instead of 2012 data; **2015 instead of 2012 data
Source: ITU

Piecemeal policies and their impact

A lack of coherence results from piecemeal policies and regulatory frameworks in a converged, digital environment. It produces gaps and contradictions which can either neutralize policy benefits or create confusion, undermining trust in government policies and the market. Piecemeal policies can also disincentivize entry into markets, undermine respect for rules and lead to non-enforcement.

The current trend towards more holistic, progressive digital policies will likely accelerate the maturing of the digital economy and the achievement of larger economic and policy goals, driven by the growing awareness and evidence of the important impact of digital technologies on the economy (see section 2.1).

4.3.   Regulation as usual – or is it?

The regulatory landscape presents a mixed picture. Many pillars of ICT regulation are also at the core of regulators' efforts in enabling the digital economy. And while many longstanding issues are multi-faceted and complex, new issues are emerging and challenging regulators to formulate viable regulatory responses. This section goes on to look at some major areas where this is the case: competition, licensing, consumer protection, infrastructure sharing and spectrum.

Developments in the field of competition

Competition is a central regulatory issue in shaping the digital economy. But may we assume that the digital economy is a competitive economy? The marketplace for ICT services is far from perfectly competitive and is more concentrated than telecom markets were, before the pervasive digitization of the last ten years. Many services that define the digital economy rely on product differentiation, innovation, brand identification or advertising. Competition in digital markets also works differently and can produce unexpected effects – both positive and negative. Competition policies need to rise to the challenge of the interplay of digital platforms, telcos, new species of network operators and the variety of players in the digital ecosystem. There is also the need to consider that services offered by global online service providers do not fall within the traditional definitions in such regulation, meaning that they are outside the scope of sector specific regulation and can sometimes escape competition law scrutiny altogether, due to the characteristics of their business model.[12]

Who's regulating competition in ICTs and the digital economy?

In the core ICT sector, the ICT regulator is in charge of competition in three-quarters of countries worldwide, either exclusively or in collaboration with the competition authority (see Figure 24). In Egypt, telecom services are classified as public utility and are largely exempt from the direct application of competition law. Hence, NTRA is responsible for competition in the ICT sector.[13] Likewise, the Singapore Competition Act excludes sectors governed by sector-specific competition laws, such as telecom, energy and media.[14]

In one-third of countries worldwide, the ICT regulator and the competition authority handle competition issues together. In the US, FCC, the ICT regulator, and the Federal Trade Commission, the competition authority, have independent and concurrent jurisdiction; however, their mandates do not perfectly coincide. Also, FCC and the Department of Justice each have independent authority to examine likely competitive effects of proposed transactions, but FCC's competitive analysis under the public interest standard is broader. In Oman, there are separate laws for regulating the competition of goods and services and TRA, the ICT regulator, works on common issues with the Ministry of Commerce and Industry.[15] The Vietnam Competition Authority has power to enforce competition law across industries and coordinates with the Authority of Telecommunications of Viet Nam (VNTA) for issues related to ICT and digital markets.

Figure 24: Who is in charge of competition in the ICT sector?, worldwide, 2018
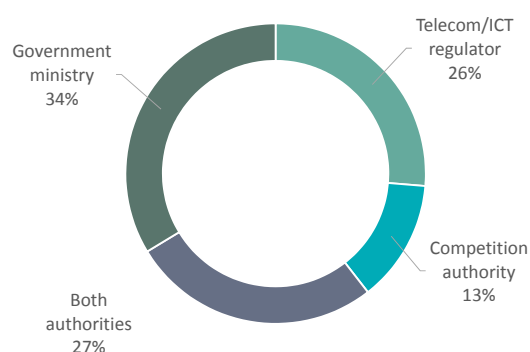
Source: ITU

In one-fifth of countries worldwide, the competition authority alone is responsible for the promotion of competition and the enforcing competition rules, either because of the lack of an ICT regulator or jurisdiction. New Zealand has taken a holistic approach, which moves away from sector-specific regulators and regulations and relies entirely on competition policy, with access to bottlenecks being subject to the essential facilities doctrine. The Ministry of Business, Innovation and Employment elaborates competition law while the Commerce Commission ensures that the telecom market is operated under the Telecom Act 2001.[16] In Mali, AMRTP, the ICT regulator, does not have mandate related to competition[17] and the competition authority handles issues related to the ICT sector on an exclusive basis.

In some countries, there is a clear division of responsibilities between the ICT regulator and the competition authority. In Iceland, the ICT regulator is responsible for wholesale markets and the competition authority – for retail markets. In Cyprus and Norway, the competition authority has jurisdiction over the ex-post cases in the ICT sector, while the ICT regulator has jurisdiction in the *ex-ante* competition regulation.

In a handful of countries, multi-sector regulators oversee a range of national markets, including ICT and digital services markets. In Barbados, BFTC is the utility regulator, competition authority and consumer protection agency and in the Netherlands, the Authority for Consumers and Markets, is charged with competition oversight, sector-specific regulation of several sectors, and enforcement of consumer protection laws.[18]

Some sub-regional organizations, notably COMESA, have developed Directives that member countries transpose into their national legislation. In Comoros, the Ministry of Trade is in charge of competition and applies COMESA's competition rules.

It is worth noting that there are still countries where no institution is appointed to deal with competition and no competition law has been enforced. This is the case of the Maldives[19], Solomon Islands[20] and Suriname. Only a few countries still have only state-owned monopolies engaged in ICT markets, making competition arbitration irrelevant. In a handful of countries, such as Antigua and Barbuda and Belarus, it

is a government ministry that is in charge of competition.

How competitive are digital services, from a legal perspective?

Core telecom markets that have reinvented themselves digitally have reached a high level (80 per cent) of competition (see Figure 25, right graph), driven by the interplay between digitization, new business models and digital policies. Anecdotally, the levels of legally permissible competition in fixed and mobile broadband markets are nearly identical, although mobile-broadband penetration is four times higher than fixed-broadband penetration – a discrepancy explained by fewer business models for fixed broadband providers, more restrictive regulatory policies applied, and higher investment needs. Competition in markets for leased lines mirrors fixed-line markets, a trend dating back to the analogue era. International gateways have the lowest level of competition, with a quarter of countries still operating under monopoly international facilities. A third of countries worldwide retain a state-owned fixed-line incumbent – exclusively responsible for fixed-line and fixed-broadband services provision. From the 69 countries with a state-owned incumbent in 2007, only five have moved towards privatizing their state-owned incumbent as of 2017.

The goal of achieving universal competition across geographies remains a challenge. Markets for digital services in 20 per cent of countries

Figure 25: ICT market structure, worldwide, 2017

Level of competition in the main ICT market segments

Ownership of the fixed-line incumbent

34%, State-owned
24%, Private
42%, Mixed ownership

■ Monopoly   ■ Partial competition   ■ Full competition
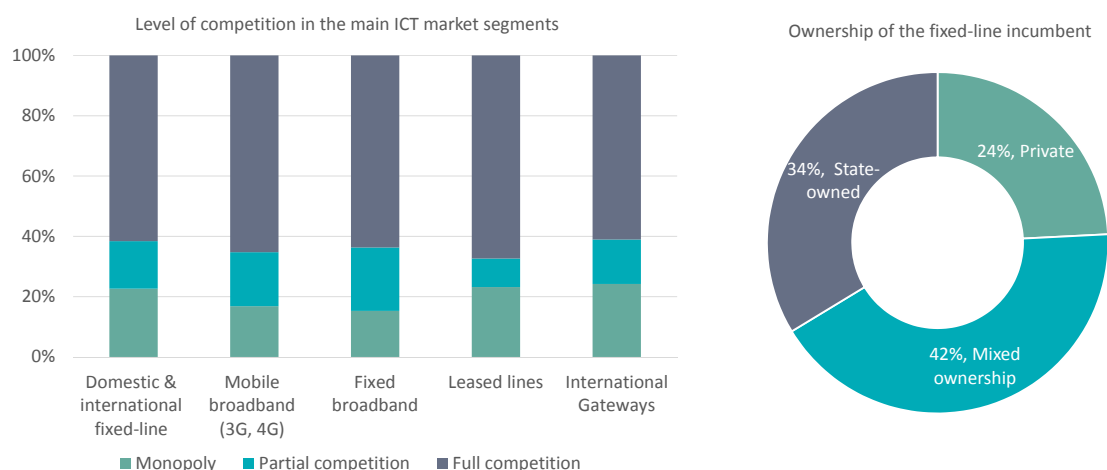
Source: ITU

worldwide have yet to open up to competition. With digital development recognized as a driver of sustainable development and vibrant economies, more effort is needed to address competitive gaps and stimulate competitive dynamics for millions of people (see Figure 25).

Foreign ownership

Foreign ownership is a key means of enabling investment and boosting innovation in digital markets. Foreign capital flows across national borders make it possible to tap into additional resources much needed for the development of national digital markets – in tune with decentralized models for digital service delivery and the explosion of transnational data flows. This enhances competitiveness, especially in countries lacking developed financial markets. Seven out of every ten countries have allowed foreign ownership in core market segments for digital services (see Figure 26). For facilities-based and domestic service operators, the worldwide averages are a little higher; for Internet Service Providers (ISPs) and value-added service providers averages are some percentage points lower.

While the pattern is consistent across market segments (see Figure 26 above), this is not the case across regions (see Figure 27). In terms of facilities-based competition, Europe allows foreign

ownership in over 90 per cent of countries while in Africa, only 60 per cent do so. In Europe, 90 per cent of countries also allow foreign capital to flow into spectrum-based operators, which paved the way for 3G and 4G, and will do so for 5G. In CIS, the proportion of countries doing so is half this rate – as it is in regard to international service operators. Looking at foreign participation and ownership in ISPs, engines of the digital economy, above half of countries in Africa allow it compared to 80 per cent in Europe.

Market dominance: thorny issue

Globally, three-quarters of countries worldwide have adopted a definition of significant market power for the ICT sector. Ninety per cent of countries in Europe now have such a definition while less than 60 per cent of countries in Asia-Pacific have done so (see Figure 28).

One-quarter of countries worldwide do not yet have a definition of dominance. One-fifth of countries have a definition without specific criteria, and a further one-fifth have a definition based on a single criterion (see Figure 28) – from an enforcement perspective, such 'half-way houses' are tantamount to having no definition. Digital services have challenged existing market definitions. They are often provided by converged or unregulated market players across national

Figure 26: Foreign ownership in the ICT sector, by segment, worldwide, 2017
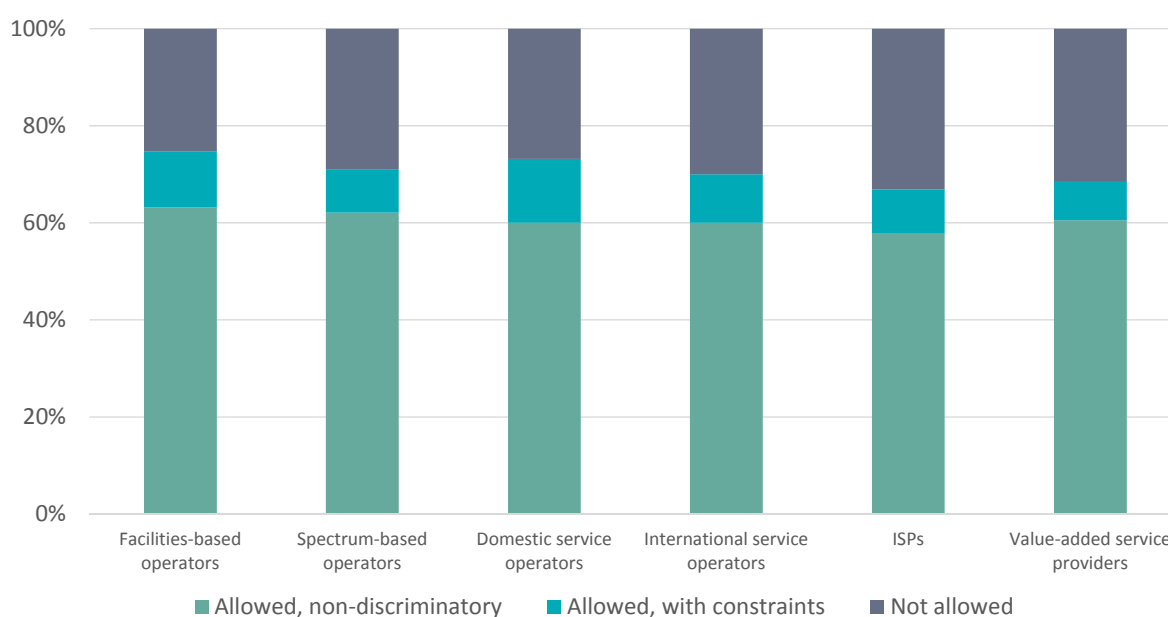
Source: ITU

Figure 27: Foreign ownership allowed, by market segment, percentage of countries per region, 2017

Facilities-based operators, by region, 2017

Africa	Americas	Arab States	Asia-Pacific	CIS	Europe
62%	88%	61%	68%	54%	93%

International service operators, by region, 2017

Africa	Americas	Arab States	Asia-Pacific	CIS	Europe
58%	85%	52%	65%	45%	88%

Spectrum-based operators, by region, 2017

Africa	Americas	Arab States	Asia-Pacific	CIS	Europe
58%	82%	57%	68%	45%	90%

ISPs, by region, 2017

Africa	Americas	Arab States	Asia-Pacific	CIS	Europe
55%	79%	66%	57%	45%	81%

Note: Percentages correspond to the proportion of countries per region allowing foreign ownership.
Source: ITU

borders; all of these factors make analysis of market dominance very complicated. A single criterion definition or one with no defined criteria will fail to pinpoint specific aspects in assessing players' real market power. Only one-third of countries worldwide have a clear framework for assessing market power for ICT – and by extension digital services – equipped with a legal definition of SMP and multiple criteria.

Figure 28: Legal concept of dominance and criteria used for determining SMP, worldwide, 2017

- No legal concept, 25%
- SMP defined, multiple criteria, 33%
- SMP defined, single criteria, 19%
- SMP defined but no criteria, 21%
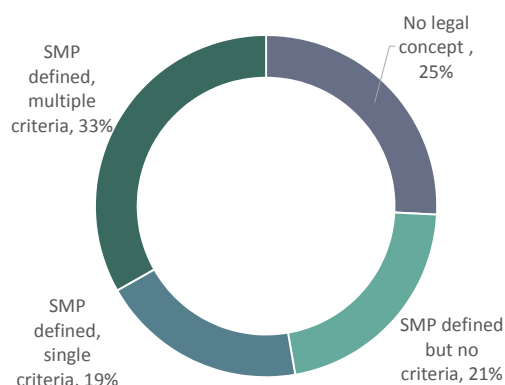
Source: ITU

Beyond the structure and granularity of the rules of competition frameworks, new issues related to the focus of such rules have arisen. Digital markets are evolving so rapidly that competition analysis cannot be based solely on traditional measures of concentration risks and invoking regulation before the markets have had time to settle and potential market power has solidified. The interpretation of concentration measures must be done with caution since the market is still developing and, in many cases, market shares have risen and fallen dramatically over a short period. It has become more difficult to establish general rules for behaviour that should be applied in the regulatory environment, as well as for the choice of remedies or incentives. Commercial strategies in the digital economy are more complex and an in-depth case-by-case assessment, also taking in account trans-border and cross-sectoral aspects, should play a greater role in determining regulatory response. This may mean a greater reliance on general competition policy or a change in the nature of regulatory obligations, making them more competition-policy like.[21]

Top 3 trends in competition

1.   Deregulation:

This is accelerating in mature broadband markets. Deregulation of broadband markets continues in European countries. Where competition is considered strong enough to sustain viable markets for digital services, administrative formalities have been lifted. In many cases though, deregulation may be coupled with additional requirements in related areas, such as infrastructure sharing.

What happened in 2018

- Austria: The ICT regulator, RTR, has deregulated leased lines with traditional interfaces.

- Hungary: The ICT regulator, NMHH, has deregulated geographic areas covering 20 per cent of Hungarian households. NMHH also includes cable networks in its definition of the wholesale broadband market.

- Ireland: The Commission for Communications Regulation, ComReg, is set to lift regulation of wholesale broadband access in urban areas accounting for almost half of households. At the same time, it will require Eircom Limited to provide access to virtual unbundling and duct-sharing on an equivalence of inputs (EoI) basis.[22]

Deregulation isn't unequivocally seen as the ultimate regulatory tool to unlock investment flows. In early 2018, the European Competitive Telecommunications Association (ECTA) suggested that competition rather than deregulation drives investment, and competition must prevail in the quest for telecoms investment.[23] Following the same market philosophy, the Belgian regulator, BIPT, has maintained regulation on broadband and broadcasting – cable operators will have to offer wholesale broadband access and access to their digital TV platform while the national fixed-broadband operator will have to offer multicasting. These measures will allow alternative operators to offer triple-play services over cable and DSL.[24]

2.   Market reviews

A number of countries in different regions are moving towards a review of broadband markets, and more are planning to do so in the coming year. Supporting European countries and equipping ICT regulators, the European Commission has published the draft of guidelines on market analysis and the assessment of significant market power (SMP Guidelines[25]). The SMP Guidelines set out principles for national regulators when intervening in ICT markets, and provides structured advice to regulators on how to conduct their markets and analyse SMP according to current European regulations.

What happened in 2018

- **New Zealand:** The Commerce Commission (Comcom) released a study of mobile telecommunication markets in New Zealand as part of a broader review of mobile markets in New Zealand. The study explores potential future developments in the supply of mobile services such as 5G and e-SIMs, and their impact on competition and market outcomes in New Zealand.[26]

- **Oman:** The Telecom Regulatory Authority (TRA) is carrying out a review of the telecom market in Oman, identifying constraints to competition with a view to preventing abuse of dominant position by operators.[27]

- **Uganda:** the Uganda Communications Commission (UCC) has opened a public consultation based on an extensive study of the wholesale access markets for Short Message Service (SMS) and Unstructured Supplementary Service Data (USSD) services in the country. One of the threshold questions for an analysis of market conduct under Ugandan law was whether the MNOs are likely to hold 'dominant positions' in the wholesale markets for SMS and/or USSD access. Ultimately, the consultation has been focusing on how commercial, legal and regulatory policies and practices relating to the SMS and USSD channels affect and are likely to affect the development of mobile financial services in Uganda.[28]

- **UK:** Ofcom, the ICT regulator, has published two draft statements setting out its

assessment of competition within the wholesale broadband access (WBA) market, and determining whether any telecoms provider has "a position strong enough to influence market outcomes". It also sets out the regulatory instruments designed to protect competition in those areas where it has determined that wholesale competition is not effective. Both of the regulator's draft statements have been submitted to the European Commission (EC) for comment.[29]

Enforcement of competition rules: competing for a monopoly position… no means no

As stated in *GIRO 17*,[30] enforcement continues to be central in regulating the digital economy. The weight of regulatory policies is shifting towards to *ex post* review of actual market behaviours. These behaviours have been scrutinized and have earned both rebukes and significant fines – with each new court case bringing a new record. This trend impacts market players from all backgrounds, from traditional players, telcos and MNOs, to digital platforms. European countries, large States and the European Union are the main litigators, sending a clear signal to market players that established competition rules will be enforced, even in the context of much expected investment in fixed broadband and 5G infrastructure.

What happened in 2018: traditional players

- **Chile:** The national Supreme Court has ruled in favour of consumer rights group, Corporacion Nacional de Consumidores y Usuarios, Conadecus, upholding its complaint that Movistar, Claro and Entel had engaged in anti-competitive practices in the process of bidding for 700MHz spectrum in 2014. The resolution found that the trio had not respected the 60MHz cap on spectrum holdings and required them to return the amount of spectrum that they won via the tender. The Department of Telecommunications (Subsecretaria de Telecomunicaciones, Subtel) was ordered to ensure 'timely compliance' with the ruling and adopt necessary measures to carry it out. Finally, if Subtel wishes to review the spectrum cap, it must do so through a consultation process with the anti-monopoly regulator, the Antitrust Tribunal (Tribunal de Defensa de la Libre Competencia, TDLC).[31]

- **Italy:** Agcom, the communications regulator, has opened consultation on commitments offered by Telecom Italia in a broadband antitrust probe. The incumbent telecom operator submitted a number of commitments to address concerns about a possible abuse of dominance in the Italian high-speed broadband market.[32]

- **EU:** The EU Court of Justice has confirmed a EUR127 million antitrust fine on Orange Polska. The judgment dismissed Orange's argument that its investment should have been recognized as mitigating circumstances when setting the level of the fine. In 2011, the Commission found Orange Polska guilty of a constructive refusal to provide access to its WBA and LLU products.[33]

- **Norway:** Telenor Norge has been fined NOK788 million (USD97 million), the largest ever levied, by the Norwegian Competition Authority (Konkurransetilsynet, KT) for abusing its dominant position in the domestic mobile market by creating barriers for the development of a third mobile network in Norway, in what it termed "a serious infringement of competition law".[34]

- **Switzerland:** The Federal Communications Commission, ComCom, is unable to organize virtual unbundling because the necessary legislation does not exist. For this reason, ComCom had to reject a corresponding application from Sunrise even though virtual access to the subscriber line could stimulate competition. Within the scope of the ongoing revision of the Federal Telecommunications Act, however, Parliament has the possibility of introducing an obligation to grant technology-neutral and virtual access to the network of a dominant market operator in view of enhancing competition and digital services to consumers.[35]

Digital platforms have moved centre-stage in terms of controversy and the attention of enforcement authorities, most prominently in Europe. Recent developments are defining an emerging regulatory paradigm and setting out norms for anti-competitive practices in digital services markets (see also section 4.4).

Regulators and enforcement agencies are concerned about natural monopoly situations of digital platforms leading to widespread market power and an accompanying willingness to lose money over long periods to 'buy' the prospect of a future monopoly position.[36] Regionally limited regulatory decisions and large fines will not resolve issues related to market power assessment and pro-trust practices of digital platforms. It may be time to turn back the clock and revisit – or reinvent – ex ante competition policies as a collaborative process. Regulators and enforcement agencies, on the one hand, and digital platforms, on the other, need to build trust and collaboration in the area of regulatory policies. The options at hand are many; the approach to regulating digital platforms needs to evolve and a 'safe place' for open discussion needs to be created. This is both a responsibility and an opportunity that competition, consumer protection and ICT regulators can take on in the coming years. Such a move will lead to the emergence of new regulatory models more adapted to the digital ecosystem – and more suited to healthy competition in digital markets.

What happened in 2018: digital platforms

- **Netherlands:** the Authority for Consumers and Markets (ACM) launched market study into mobile app stores and looking to understand better what influence app stores have on the selection of apps by end-users.[37]

- **EU:** Google was fined a record EUR4.34 billion fine by the European Commission for leveraging its Android operating system while abusing its dominance. The Commission found that Google imposed anti-competitive restrictions on Android device manufacturers and mobile network operators (MNOs) in order to cement its dominant position in general Internet search. The appeal ruling of the EU General Court is pending on the European Commission's June 2017 Google Shopping decision, in which the company was fined a record EUR2.42 billion.[38]

- **EU:** The European Commission has been collecting data on the power of large digital companies focusing on concentration trends, margins, firm entry and exit. Key areas of focus will be (i) how big data should be treated in the context of merger control and to what extent they can confer market power; (ii) the follow-up from the e-commerce sector enquiry, continued enforcement against pricing restrictions, geo-blocking in online distribution channels; and finally (iii) algorithms or decision-making software at the core of many digital products. To the extent algorithms can be used to monitor competitors' prices and adapt price, this can raise competition concerns.[39]

- **France:** The French Minister of Finance has filed a complaint against Apple and Google to the Paris Commercial Court over app store concerns.[40]

- **Germany:** The German national competition authority has formally informed Facebook of its preliminary legal assessment, confirming that Facebook's data collection and processing policy could qualify as an abuse of dominance. A final decision is expected in late 2018.

- **UNCTAD:** UNCTAD Secretary-General Mukhisa Kituyi has stated that a regional network of competition and consumer protection agencies, such as COMPAL in Latin America, could lead the way in soft development of laws to tame the abusive power of dominant players in the global digital economy, which can translate into national legislation. This would allow to better shield markets and people in the growing digital economy, where products and services flow across borders and jurisdictions.[41]

Developments in the field of licensing

Who's in charge of licensing operators and ICT service providers in the digital economy?

Facilitating and upholding a competitive marketplace is no easy task in the digital economy. Challenges range from getting the right number of market players (neither too many nor too few), to making choices on the terms and conditions of authorizations for monitoring their compliance – and the job requires many skills played out across varied areas of expertise.

In six of every ten countries the ICT regulator assigns and auctions licences, and drafts licence conditions (see Figure 29). The sector ministry is in charge of licensing in a further quarter

of all countries. Multiple institutions share responsibilities in fewer than one of every ten countries, where ministries issue licences while the ICT regulator carries out auctions and formulates recommendations. In a handful of countries (especially countries torn by prolonged armed conflicts), no entity is responsible for licensing.

Figure 29: Who's in charge of licensing worldwide?, worldwide, 2017
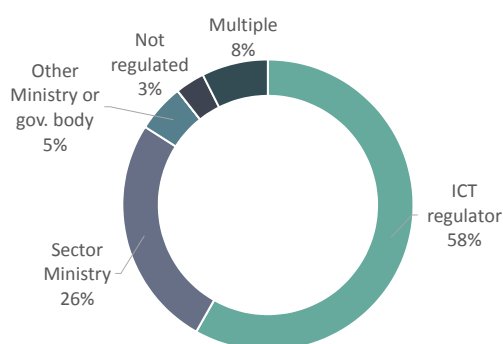
Source: ITU

Over the past decade, we have seen a clear transfer of responsibility from telecom/ICT ministries to separate ICT regulators. This is driven by the sustained trend of strengthening regulatory mandates and institutional capacity to handle complex and demanding challenges.

What kind of licences?

The digital economy is an open economy – as reflected clearly by today's licensing frameworks worldwide. Six of every ten countries worldwide have significantly opened their licensing regimes and now operate either unified licences or general authorizations. One in ten apply multi-service licences (see Figure 30, left chart). One-third of countries create delays and additional challenges to market entry by continuing with individual service licences. On a positive note, the number of countries under a first-generation (G1) licensing regime has halved since 2007.

In the area of spectrum allocation and assignment, over one-quarter of countries worldwide have created a regulatory framework for licence-exempt spectrum (see Figure 30, right chart). This figure shows impressive growth, up from only one per cent of countries a decade ago.

Some countries are experimenting with new approaches to licensing with the goal of fostering innovation and enabling continued investment. In France, ARCEP has come up with an inventory of new tools including 5G pilot projects interface, start-ups and experiments interface, the regulatory sandbox and the free frequencies site[42].

- The 5G pilot projects interface enable all players in the 5G value chain to learn about specific use cases and future challenges of next-generation technologies under real-life conditions while allocating frequencies to interested players for the purpose of full-scale deployments and obtaining feedback concerning the design of future spectrum allocations.

- The start-ups and experiments interface will support start-ups, enterprises and communities in their experimental initiatives.

- A regulatory sandbox approach enables companies wishing to test a given technology or innovative service to do so without being bound by all the regulations that would normally apply.

- A free frequencies site is dedicated to providing information on bands subject to general authorization, reporting on quality of service issues in these bands and informing IoT stakeholders of available bands.[43]

Digital era needs both global and local approaches

The regional harmonization of regulatory frameworks for licensing continues – progress on the journey towards a global approach for licensing operators and service providers in a global digital world. Innovative models are needed to respond to the global nature of platforms and players. Building on examples from the satellite industry and MVNO regulation could provide a useful starting place.

Licensing regimes for the digital era also need to encourage local development, by creating incentives for local greenfield businesses, or through integrating such clauses in licensing conditions.

Developments in the field of consumer protection

Consumers are a main driver in the digital economy and have the power to make or break digital business. Consumers are however vulnerable: with user data fueling business models and routinely monetized, business integrity towards consumers has been sorely tested. In this context, the role of regulatory agencies is paramount in protecting consumers, defending their rights and raising awareness about all aspects of their digital experience.

Governments are very much aware of these issues as digital services increasingly extend into all walks of life.

Our data shows:

- 96 per cent of countries worldwide have a regulatory agency mandated to protect consumers in the area of ICT services – extended in many cases to other services such as mobile money (see Figure 31).

- In four of every ten countries worldwide, the ICT regulator is exclusively in charge of consumer protection, and a government consumer protection authority exclusively handles consumer protection in other sectors.

- In a minority of countries (only one in ten), the sector ministry is tasked solely with protecting ICT consumers.

- In 2 per cent of countries, self-regulatory practices rather than formal regulation are the norm, and no regulatory focal point exists for ICT consumer protection in a further 2 per cent of countries.

Good ICT consumer protection legislation is a key regulatory framework underwriting the safe expansion of digital services. Since 2007, the number of countries with such legislation has doubled, rising to 118 as of 2017 (see Figure 32). A dozen countries are also planning to adopt a new consumer protection framework in the coming years or are actively working on it.

Handling consumer complaints and educating ICT consumers are two main roles for the ICT regulator, bringing them face to face with the

Figure 30: Licensing framework for ICT services, worldwide, 2017

Who is in charge of licensing?

Multiple 8%
Not regulated 3%
Other Ministry or gov. body 5%
Regulator 58%
Sector Ministry 26%

Types of licences provided, worldwide, 2017

Service-specific only, 31%
Unified/ General authorization, 60%
Multi-service, 8%

Licence-exempt spectrum available, worldwide, 2017

Yes, 27%
No , 72%
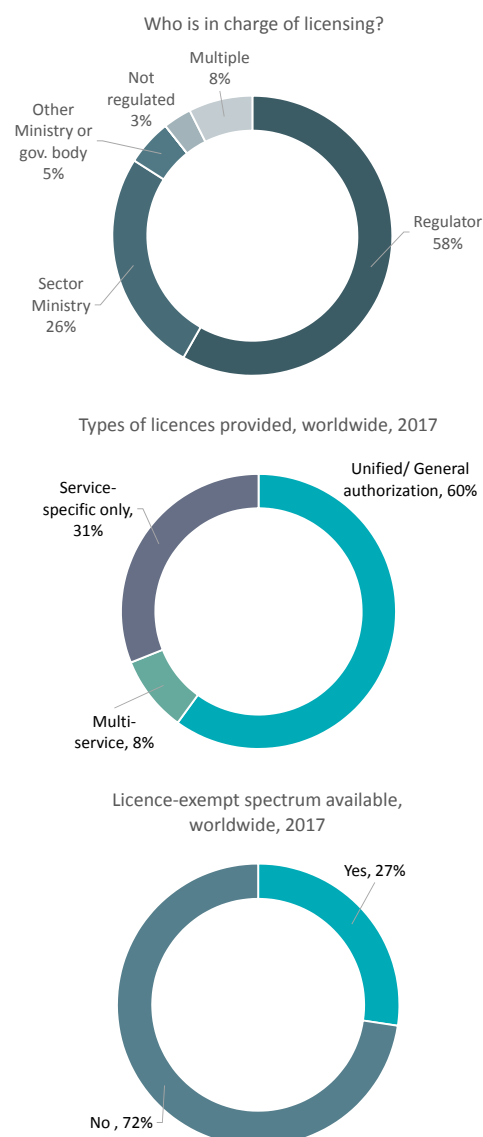
Source: ITU

complex issues related to digital services – a role few other market stakeholders are willing and able to take on. Virtually all ICT regulators play the role of trusted advisor and advocate of ICT consumers – and around 100 of them are responsible for pro-actively defending consumer rights. The growing numbers of litigations and the complexity and opacity of digital service bundles will necessitate further enhancement of regulatory mandates.

Surprisingly, only one in two ICT regulators is responsible for providing comparative tariff information, and not many agencies have acquired this mandate over the past decade. This is mainly

Figure 31: Who is in charge of consumer protection?, worldwide, 2017

Multiple 17%

Not regulated 2%

Operators 2%

Other Ministry or gov. body 26%

ICT regulator 43%

Sector Ministry 10%
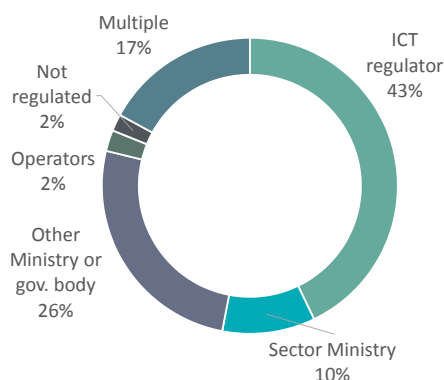
Source: ITU

because private sector players manage tariff comparison websites efficiently.

One interesting institutional trend – and impacting more than 100 countries – is the inclusion in the regulator's mandate of promoting consumer

protection. Different countries have different practices. In some, individual consumers along with consumer associations are invited to provide comments during public consultations on regulatory documents. In others, consumers are routinely surveyed on topics such as the quality of their Internet connection or the billing of their mobile services. In others, consumer associations are seen to be core to the process. In 2018, for example, ACMA replaced individual consumer representatives with consumer organizations[44] to deliver more consistency and transparency, and enable information to be more readily shared between networks.[45] Many countries run community or national consumer awareness programmes to advocate for increased access and responsible use of new technologies.

Many regulators think innovatively – Ofcom in the UK, for example, takes user questions on Twitter and respond with a tweet and a posting of the Q&A on their website.[46] In Kenya, CCK (now CA) have a code of conduct for consumers

Figure 32: Consumer protection framework, worldwide, 2010 and 2017

Telecom/ICT consumer protection legislation

200
150
100
50
0

Regulator responsible for comparative tariff information

Regulator responsible for consumer complaints

Regulator responsible for defending consumer rights

Regulator promoting consumer participation in their activities

Regulator responsible for consumer education

—— 2010 —— 2017
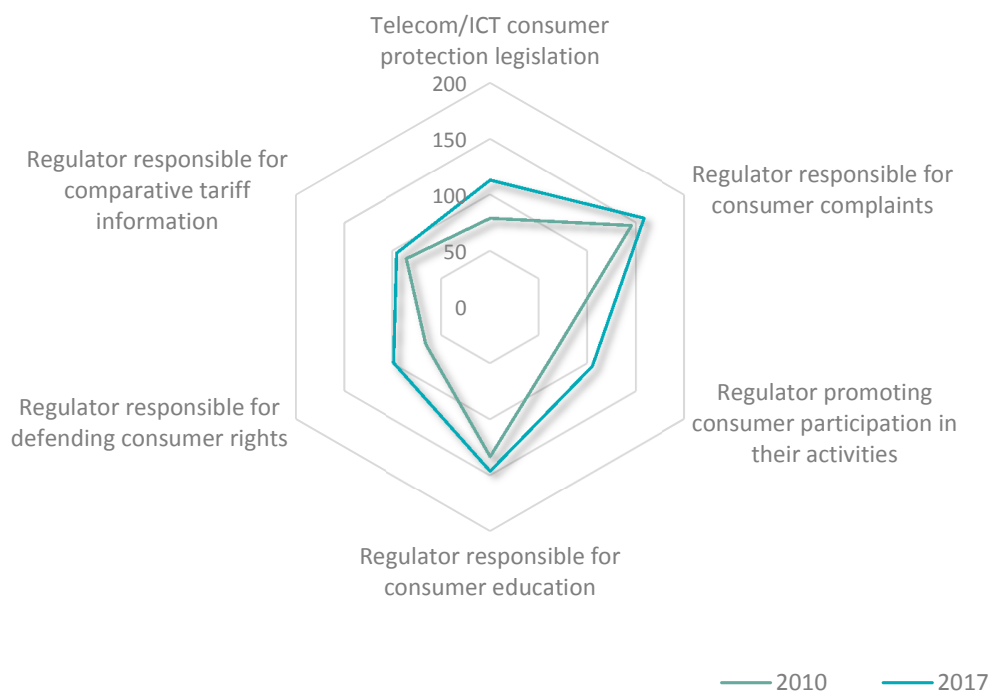
Source: ITU

Figure 33: Quality of service framework, worldwide, 2017

Quality of service monitoring required

No
13%

Yes
87%

Operators subject to quality of service monitoring, worldwide, 2017

countries

Any operator or service provider	Mobile cellular operators	Incumbent	Dominant or SMP operator/s	Universal Service/Access operator/s	Other	Network operators
69	60	45	43	41	22	19
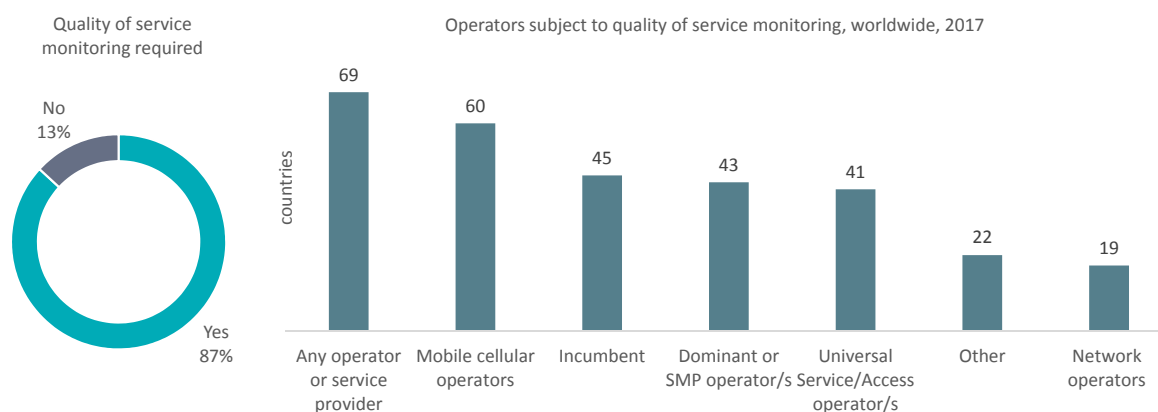
Source: ITU

giving them rights but also entrusting them with responsibilities, like reporting faults when they occur so that quality of service can be monitored.[47] In France, ARCEP has introduced 'Regulation by data' to leverage the power of digital online services. Two ARCEP projects are core to this approach: maps available at the site 'monreseaumobile.fr' enable users to compare coverage and quality of service of mobile networks while the reporting platform 'J'alerte l'Arcep' enables every user to trace malfunctions in links with operators. ARCEP also runs a 'crowdsourcing' ecosystem for measuring Internet quality.[48]

There is opportunity to move towards more collaborative regulation, enhancing the participation of consumers and associations in the decision-making process, and for example crowdsourcing ideas and experiences. As big data tools become more readily available, polling large populations can be a powerful source of market data and an almost real-time indicator of competitiveness and fairness in regard to digital services. Such data could also identify new issues, could inform new regulations, or could lead to the withdrawal of existing ones.

Quality of service and experience

Quality of service and experience (QoS/E), especially for services delivered online, can make or break a business – but they have also a marked impact on consumers. They have evolved from being a technical issue handled by ICT regulators into a pillar of consumer protection in digital markets.

In almost nine in ten countries worldwide, QoS monitoring is required (see Figure 33) and there is little variation across the regions. This is good news for consumers using services in sound regulatory frameworks – mostly light-touch. QoS monitoring effectively ensures service providers comply with established norms and deliver on consumer satisfaction.

QoS monitoring varies across countries. While the majority still have a differentiated approach (targeting only certain profiles of service providers), over a third of countries consistently apply QoS monitoring to all operators and service providers – and this trend is growing despite technical complexity in monitoring some Internet services. It is fair to note, however, that digital platforms are in general not addressed given their nature and absence of national point of presence. Digital platform services could nevertheless fall under net neutrality regulations and benefit from generally free access to Internet capacity and unaltered QoS delivered to their consumers. Quality of service and experience for digital platform services will therefore remain a major area for ICT regulators to explore in a broader social and economic context.

Mobile and fixed services are monitored equally in more than three-quarters of countries worldwide. Internet services are a major focus of QoS/E monitoring in two-thirds of countries. Legacy regulations in some countries still specifically target interconnection (for telephony and Internet) as well as services like pay phones. The latter may well lose the use rate they hitherto enjoyed as low-cost mobile services and shared-use schemes

proliferate, and therefore will likely be less relevant in consumer protection frameworks.

Surprisingly, only 15 per cent of countries apply a harmonized approach to QoS monitoring for all regulated services (see Figure 34). Such an approach might be useful in establishing a single benchmark and blueprint for regulatory treatment of substitute online services in particular – and more regulators might be interested in a level playing field revamp of their regulatory frameworks for QoS/E in the coming years.

Developments in the field of infrastructure sharing

The 2008 Global Symposium for Regulators (GSR), entitled "Six degrees of sharing", was the first major effort in ITU to explore regulatory and policy-sharing measures that developed and developing countries can implement to ensure that all people are connected to ICT networks offering affordable broadband services.[49] The discussions revolved around the various aspects of infrastructure sharing in the telecom/ICT sector.[50]

We have revisited the original categories (see Figure 35) as follows:

- Passive and active sharing cover both mobile and fibre (backbone, backhaul or edge) networks;

- International sharing covers sharing international gateways and submarine cable

landing stations, and international mobile roaming regulation as a form of regulatory sharing or harmonization;

- Spectrum sharing to promote broadband wireless access technologies involves both sharing practices amongst MNOs and between MNOs and MVNOs;

- Functional separation of legacy fixed-line networks is considered sharing as long as the infrastructure and service provision arms belong to the same operator while operating under a business agreement;

- End-user sharing refers to sharing devices and applications as well as user-generated content and the access to digital platforms for sharing data and content and offering services and products.

The sharing options can be used alone or in combination, mixing and matching regulatory initiatives to achieve desired policy objectives. Some of the high-level principles enshrined in the GSR 2008 Best Practice Guidelines are highlighted in Box 5.

Infrastructure sharing practices have become more common in the aftermath of the global financial crisis 2008-2009 and their modalities have significantly expanded.

Figure 34: Services subject to quality of service monitoring, worldwide, 2017
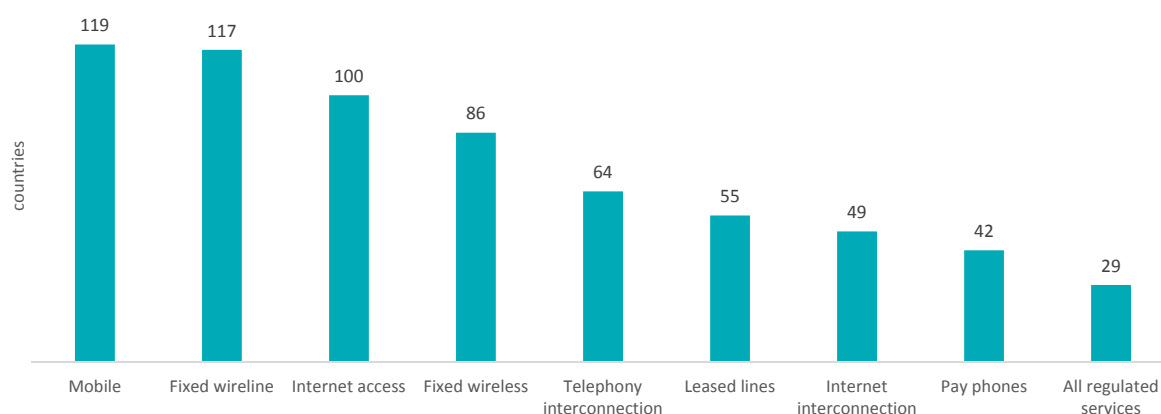
Source: ITU

Figure 35: Six degrees of sharing

01 Passive infrastructure sharing

02 Active infrastructure sharing

03 Spectrum sharing

04 International sharing

05 Functional separation

06 End-user sharing
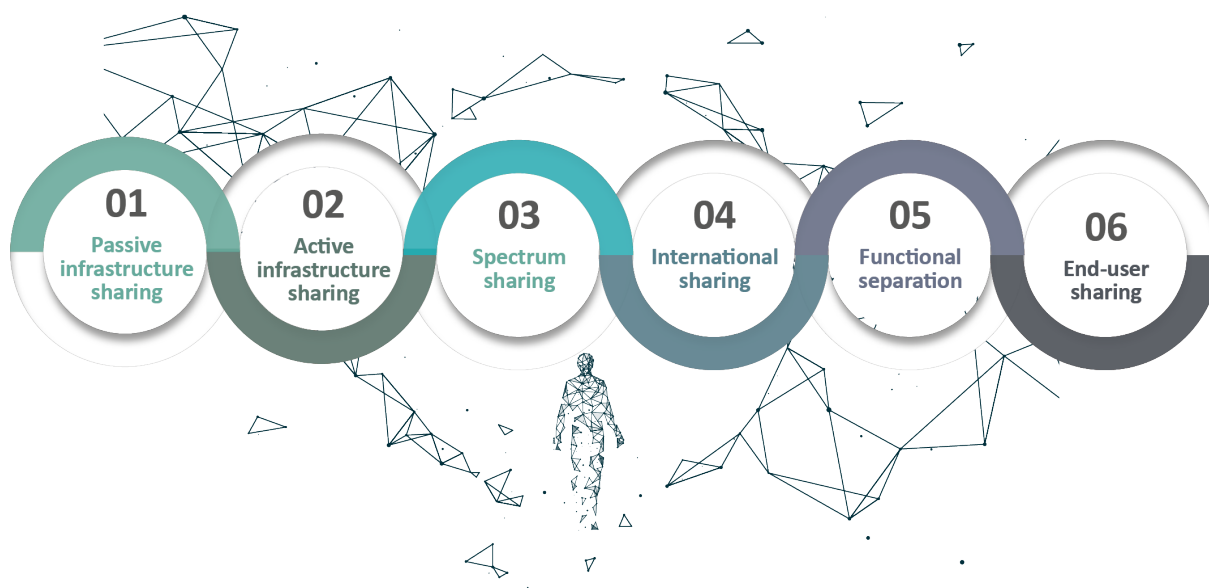
Source: ITU

Passive vs. active infrastructure sharing

Passive and active infrastructure sharing have been the most widely regulated types of sharing. ICT regulators have adopted a myriad of regulations with the aim of stirring markets, creating opportunities and reducing prices for ICT services – ranging from tolerating to explicitly permitting sharing to mandating it. Today, six of every seven countries worldwide permit infrastructure sharing; two of every three mandate it, compared to two of every five in 2010 (see Figure 36). Over 50 per cent of countries allow unbundled access to the local loop – the least preferred infrastructure sharing option.

Spectrum sharing

Spectrum sharing – less controversial than spectrum trading – has powered new partnerships and helped optimize available spectrum and deriving higher economic value from assigned spectrum bands. Europe is the only region where the majority of countries (or three-quarters) have removed regulatory barriers to spectrum sharing while a third of countries across all other regions have allowed it (see Figure 37, right graph).

Six of every ten countries worldwide still do not allow spectrum sharing (see Figure 37, left graph), driven by concerns regarding competition and altered market dynamics. With the advent of 5G

services, spectrum sharing is likely to become much more common in the coming years.

International sharing

Data flows across borders and regulatory frameworks – along with people, goods, services and currencies. And yet, nation States have jurisdiction only over their respective economies. Measuring the economic value of data flows remains challenging, although it is universally acknowledged that this value is considerable. Governments and private enterprise strive to capture this and convert it into tangible benefits for all, the benefits of sharing globally. Regulatory policies have been spreading across regions, creating incentives, shaping positive behaviour and clarifying the obligations of market players. Such policies are becoming more common and patterns are beginning to emerge.

However, regulation remains disproportionately underdeveloped to address the issues thrown up by international data flows – nor are enforcement agencies adequately equipped to address them. All the while, new regulatory areas are taking shape alongside established, traditional fields.

For sharing to happen at the international level, physical and virtual facilities need to be shared, with commercial terms of sharing agreed. Two key

Box 5: GSR 2008 Best Practice Guidelines on infrastructure sharing

"We, the regulators participating in the 2008 Global Symposium for Regulators, have identified and proposed best practice guidelines for innovative infrastructure sharing and open access strategies to promote affordable broadband access.

- **Appropriate regulatory framework:** We recognize the need for an appropriate regulatory framework fostering broadband access including Internet, to enable the development of infrastructure-based competition, in addition to service-based competition, and the emergence of new innovative players at the national level.

- **Competition and investment incentives:** We recognize the potential benefits of infrastructure sharing, whether mandatory or optional, in situations where competition and investment incentives are not undermined, bearing in mind the need to safeguard competition and investment incentives. We recognize that offering of shared facilities must not be biased towards any specific service provider or types of services.

- **Conditions for sharing and interconnection:** Regulators recognize that infrastructure sharing can only take place on a neutral, transparent, fair and non-discriminatory basis and that interconnection frameworks can ensure that all licensed operators are granted the right to interconnect as well as encourage the sharing of essential facilities and guarantee that network security and quality of service are not compromised.

- **Establishing an infrastructure sharing one-stop-shop:** Establishing a one-stop-shop would facilitate the coordination of trenching and ducting works between telecommunication service providers as well as between telecommunication service providers and those of other utilities. Regulators recognize the key role local authorities could play in fostering the deployment of broadband access and development of competition and the importance of close cooperation to simplify administrative proceedings and ensure timely response to requests for infrastructure sharing.

- **Sharing with other market players and industries:** Regulators also recognize that sharing should be encouraged not only within the boundaries of the telecommunications/ICT and broadcasting industry, but together with other infrastructure industries (such as electricity, gas, water, sewage, etc.) as well. In the context of technological development, joint infrastructure building (with other market players and with other industries) may be encouraged, providing for timed, organized opportunities for access to ducts and conduits (for example, for the joint laying of fibre) to distribute the cost of civil works among service providers and reduce the inconvenience for traffic in towns and cities. This would also provide for a positive environmental (including aesthetic) impact, in particular by reducing the number of mobile masts and towers.

- **Sharing of regulatory practices:** Regulators recognize the need for an appropriate level of international and regional harmonization to ensure that best practice regulatory policies on sharing are widely spread, and regional organizations have an important role to play in this regard. This is even more important in areas where a specific regulatory issue has a significant cross-border effect and thereby cannot be tackled by a national regulator."

Source: ITU, Extract from the GSR 2008 Best Practice Guidelines on infrastructure sharing

Box 6: ICT and Broadcasting Infrastructure Sharing Guidelines of the Communications Regulators' Association of Southern Africa (CRASA)

High-level principles:

1. Regulatory framework should address all aspects of infrastructure sharing and apply to all sector participants

2. All types of sharing should be permitted so long as competition is not adversely affected

3. All sector participants have the right to request to share infrastructure that has been mandated for sharing

4. All sector participants when requested are obliged to negotiate sharing of their (mandated) infrastructure

5. Operators designated as having SMP in a passive or active infrastructure market are required to publish a reference offer approved by the NRA

6. Commercial terms for infrastructure sharing should be transparent, fair/economic and non-discriminatory

7. Approval process for new infrastructure should be timely, effective and should encourage infrastructure sharing

8. Dispute resolution process should be cross-sector, documented, timely and effective

9. Infrastructure sharing regulatory framework takes into account the national broadband plan, USF policy and future technology development

Source: Based on the ICT and Broadcasting Infrastructure Sharing Guidelines prepared by ITU for the Communications Regulators' Association of Southern Africa (CRASA), 2016.

Figure 36: Infrastructure sharing framework, worldwide, 2010 and 2017
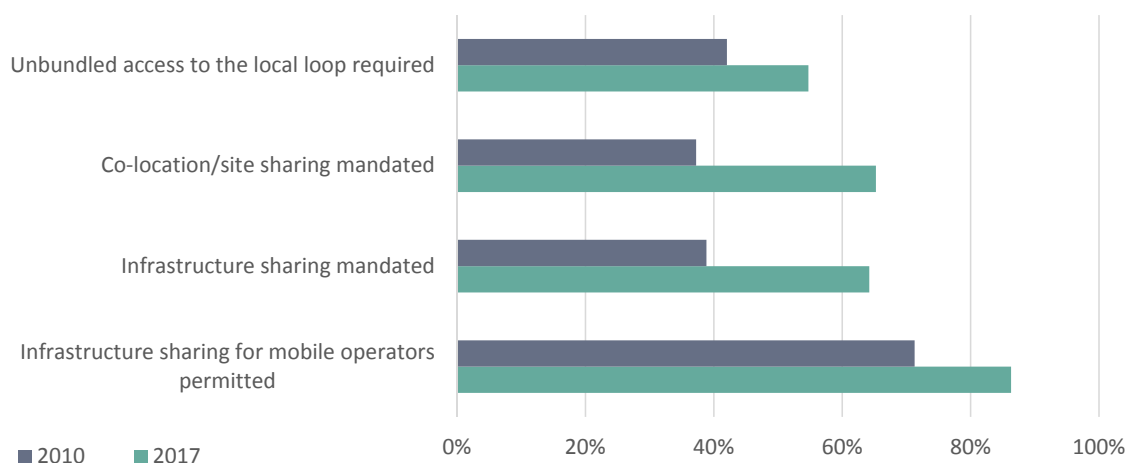
Source: ITU

Figure 37: Spectrum sharing framework, worldwide, 2017

Is spectrum sharing allowed? by region, 2017

Africa 8%
Arab States
Asia & Pacific
CIS
Europe 16%
The Americas 6%
Not allowed 58%

Spectrum sharing allowed, by region, 2017

Legend: ■ Yes ■ No

Region	Yes	No
Africa	15	28
Arab States	7	14
Asia & Pacific	11	27
CIS	3	8
Europe	31	12
The Americas	12	22
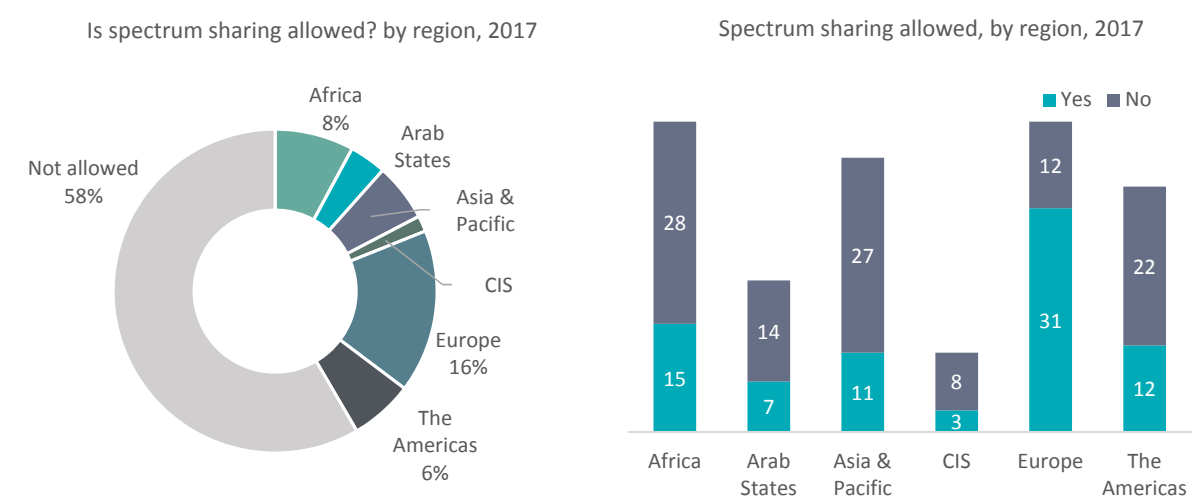
areas in this regard are submarine cable landing stations and international gateways.

Liberalization of international gateways has allowed countries Internet access and has enabled international connectivity for digital and Internet-driven services. Over the past decade, while countries with a monopoly gateway have halved in number, a quarter of countries worldwide still limit international access (see Figure 38). Half of all Arab States still operate a monopoly international gateway as do a third of CIS countries. These figures compare with fewer than one-tenth of European countries. One in six countries have only partially liberalized their competition framework for international gateways, a proportion that has remained stable through the period of strong Internet adoption since 2007. Nevertheless, three in five countries today have an open framework

for international sharing, laying the groundwork for a global digital economy.

The explosion of data needs triggered by the digital transformation has opened the way to mass deployment of international fibre infrastructure worldwide. Nevertheless, there are still a large number of population centres, particularly in developing countries, which remain unconnected by fibre while many others are only connected by high-cost or unreliable fibre links. The wide variety and large number of factors in the affordable connectivity equation underscore the need for an integrated approach to provide continuous affordable access to international fibre infrastructure.

Figure 38: Status of international gateway/s, worldwide, 2007 and 2017

2007

Open 33%
Monopoly 52%
Partially liberalized, 13%

2017

Monopoly 24%
Open 61%
Partially liberalized 15%
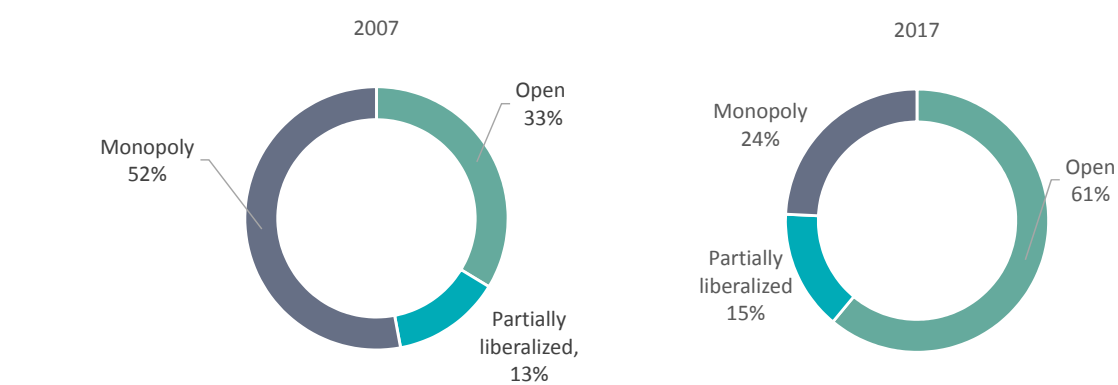
Functional separation: breaking up is hard to do

Functional separation is one of the most drastic remedies available to a regulator. It has enormous implications for the incumbent as well as for the regulator in charge of its implementation and enforcement.[51] Functional separation is a last-resort remedy to address anti-competitive and discriminatory behaviours by national fixed-line incumbents.

Accounting separation – softer and less controversial – remains more prevalent than functional separation. It has nevertheless been losing ground over the past years (see Figure 39, left graph). In contrast, the high-impact, more costly and irreversible functional separation has also gained momentum, with over 60 countries worldwide applying it to dominant operators – an increase of 100 per cent since 2007.

The rationale for this approach is the imperative to facilitate the provision of broadband services by ensuring competitor access to bottleneck assets. This seems to hold true as the number of MNO network infrastructure sharing deals has increased significantly over the past decade (see Figure 39, right graph), making it possible to develop new business partnerships. A related trend growing and taking shape is the positioning of independent tower companies as a privileged partner in network sharing deals.

It will be of value to explore a new form of functional separation for digital platforms in response to growing evidence of anti-competitive behaviours at the global level, which handicap small market players in particular. While the idea is tempting, implementation and enforcement aspects of functional separation at the international level are likely to be beyond the powers and resources of any existing agency – national or international.

End-user sharing: to stream or not to stream?

End-user sharing of devices and applications falls outside the scope of regulation and is driven by practicality, cost and the additional value arising from shared use.

With regard to user-generated content sharing, regulators from various sectors have sought to engage with its implications – while others have stayed away. End-user sharing is the most heterogeneous type of sharing and one of the most complex and challenging for many reasons including:

- Complex general constructs dependent on culture, tradition, politics and background (such as freedom of expression, privacy and ethics);

- Universally recognized scourges (such as online harassment and bullying);

Figure 39: Network sharing requirements and practices, worldwide, 2010-2017

Operational separation of dominant/SMP operator required by law, worldwide

Active network-sharing agreements announced (cumulative)
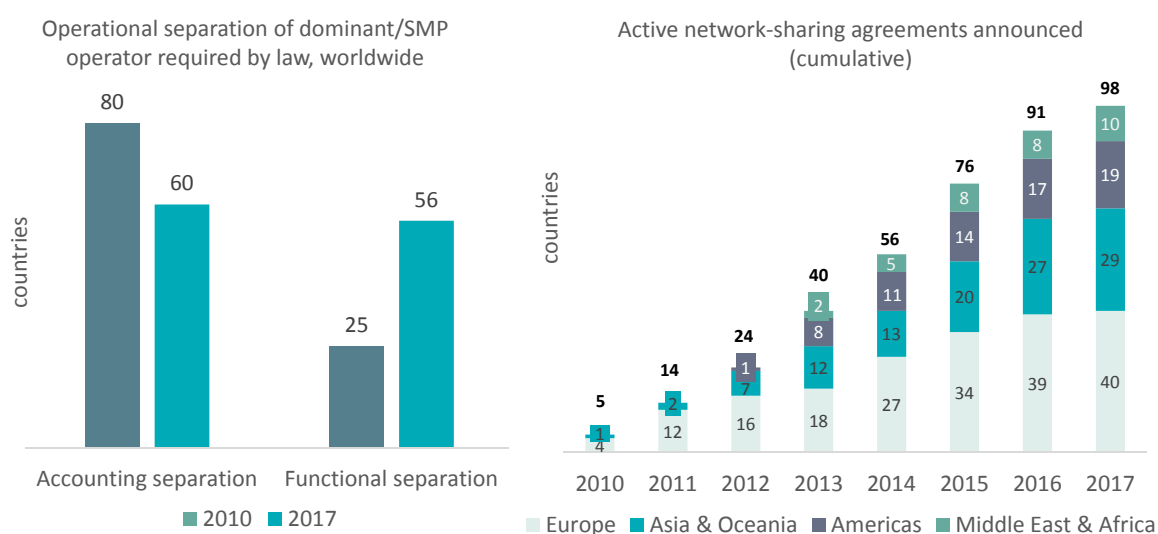
Source: ITU (left graph) and McKinsey (right graph)

Figure 40: Who regulates Internet content?, worldwide and by region, 2017

worldwide, 2017

Regulator 22%

Not regulated 48%

Sector Ministry 30%

by region, 2017

■ ICT regulator ■ Sector ministry ■ Not regulated
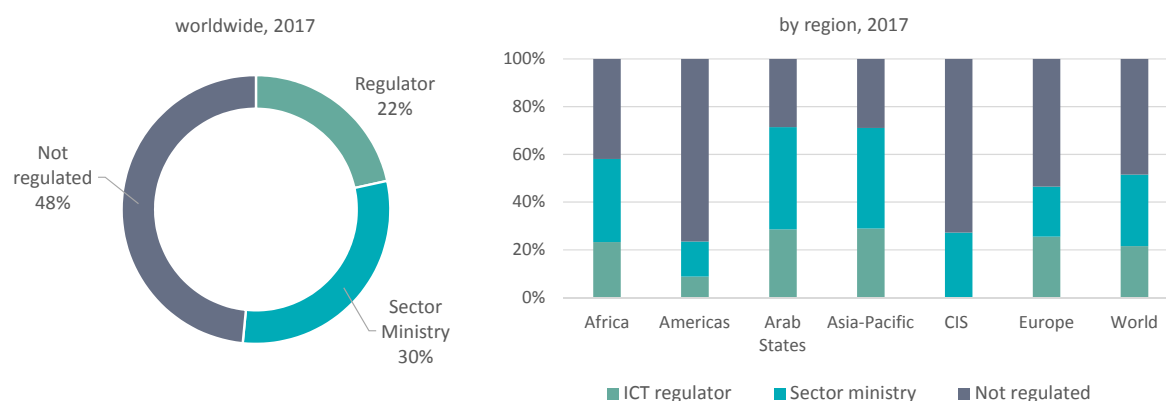
Source: ITU

- Technical questions related to the physical access to digital platforms for sharing (such as the legal status of zero-rated service offers and VoIP).

What is unique to the sharing of user-generated content – and Internet content in general – is the necessity of self-regulatory frameworks for all digital platforms. As a real-time, worldwide arena for broadcasting the best and the worst of human ideas and behaviours, digital platforms have the heavy burden to stream – or not – user-generated content. Motivation for removing content posted on platforms have varied between ethical and enforcement requirements on one hand, and self-promotion and platform growth, on the other. For many, current self-regulatory practices have not performed satisfactorily, and constitute

a 'missing link' in the regulatory framework chain. While self-regulation, in this case, can be a valuable complementary solution to more formal regulation, it is likely to prove ineffective at best and counterproductive at worst, when the sole form of regulation on the playing field.

Currently, half of countries worldwide do not regulate Internet content at all (see Figure 40, left chart) and more government ministries than regulators have charge of content in the other half. The actual case for Internet content regulation is unclear in many jurisdictions and no sound framework exists. Cultural, political and ethical dimensions are different in every country and it is difficult to agree on a guideline for handling complex cases of convergence and cross-border disputes.

Figure 41: Regulatory framework for VoIP, worldwide, 2017

Individuals allowed to use VoIP, worldwide, 2007-2017

	2007	2017
No	59%	18%
Yes	41%	82%

■ Yes ■ No

Regulatory treatment of VoIP, worldwide, 2017

Allowed, 108

Banned, 27

Closed, 22

No Framework, 33
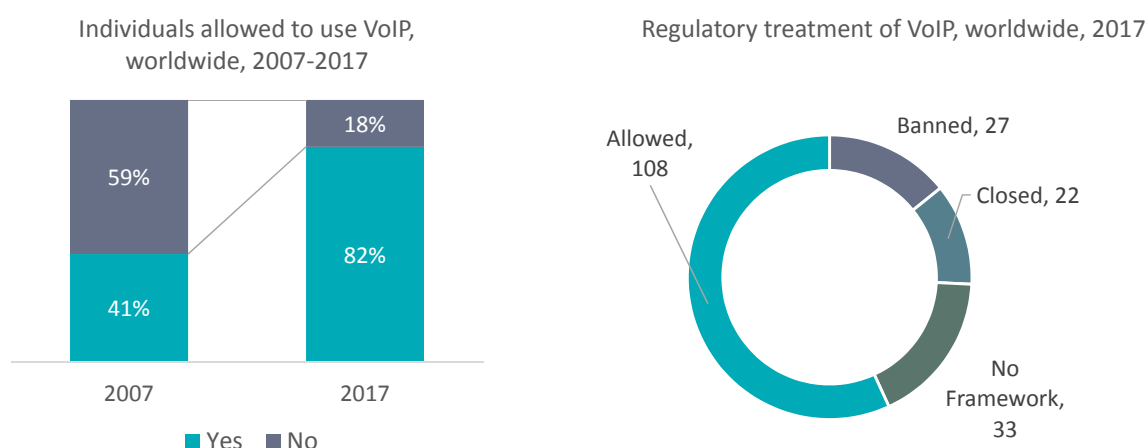
Note: "Closed" means that wholesale IP voice is permitted, but retail VoIP is banned, as well as cases where only the incumbent is licensed to provide VoIP .

Source: ITU

In the Americas and CIS, four of every five countries do not regulate Internet content, while in Africa four in ten do not have regulatory oversight over it (see Figure 40, right graph). In Europe, half of all countries do not have national policies on Internet content. However, the harmonized regional approach provides policy guidance and allows for borrowing regulatory practices and precedent-based court decisions in the resolution of disputes and complaints.

From a consumer perspective, enhancing ex ante regulatory requirements and designing more stringent enforcement are plausible options. The questions are many, however, ranging from which regulatory bodies should lead in enforcement, to how to ensure a consistent approach to global flows of data across borders.

VoIP and its many variants is one of the most global digital phenomena. Seen as an early milestone in national digital ecosystems, the regulatory treatment of VoIP has been uneven. Many countries explicitly legalized VoIP services soon after they became popular. Many countries, nevertheless, have no regulations on VoIP, treating it like any other communication service. Overall, VoIP has been allowed in more than 80

per cent of countries worldwide (see Figure 41). Counterintuitively, it is still banned in 34 countries, and only four countries are planning on legalizing VoIP in 2018-2019 – Afghanistan, Gabon, Kuwait and Liberia.

Developments in the field of spectrum

Radio spectrum has been at the heart of digital transformation – without it, the world as we know it would not be the same. Imagine a world without mobile networks, where only those with a fixed connection could make voice calls or access Internet and where connectivity on the move is not possible. At least 3.2 billion people would not have access to Internet and at least 6.8 billion people would not have voice communications. The digital connected world simply would not exist.

Fortunately, it does! Technologists, investors and policy-makers have done a great deal to leverage the benefits and value of spectrum. They have done much to unlock its potential and open new avenues for service provision, content dissemination and ultimately, social and economic development.

Figure 42: Regulatory mandates in spectrum management, worldwide, 2017
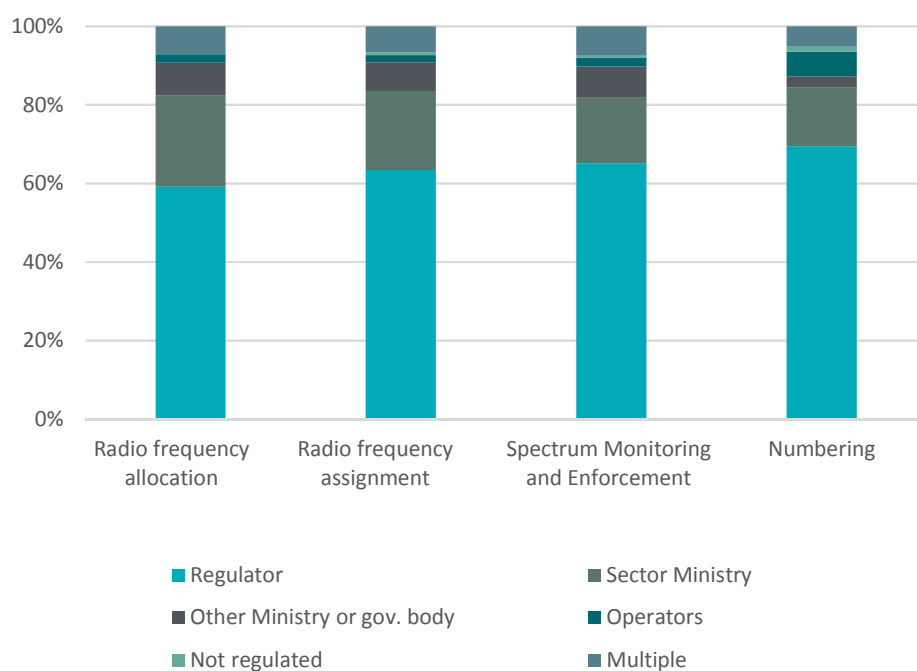
Source: ITU

Figure 43: Spectrum licensing practices, worldwide, 2017

Technology-neutral spectrum licences, worldwide, 2017

No 40%
Yes, all 48%
Yes, some 12%

Licence-exempt spectrum available, by region, 2017

Africa 16% | Americas 21% | Arab States 19% | Asia-Pacific 18% | CIS 36% | Europe 53% | World 27%
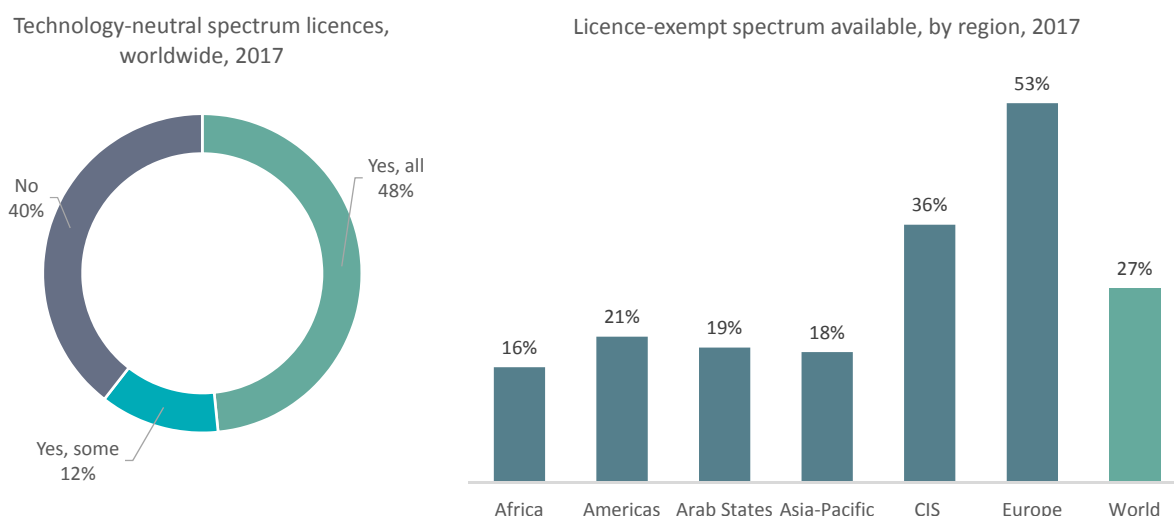
Source: ITU

Who deals with spectrum?

Managing spectrum is a core function for most ICT regulators worldwide (see Figure 42). Six of every ten regulators are exclusive spectrum administrators. In one of every ten countries, the regulator shares functions with the sector ministry. Ministries are unique spectrum managers in a further tenth of countries, strategically centralizing all functions at government level. On the other hand, separate spectrum agencies operate in a tenth of countries worldwide. In a handful of countries, as with licensing, spectrum is not managed at government level, and spectrum regulations are not enforced. In a few cases, operators are the only entities engaged in spectrum management for the purpose of their service provision. Such a set-up does not ensure high quality and reliability of service because of possible interferences or gaps.

Spectrum management practices

Regulatory responses to market development and the open arrangements for spectrum assignment have played an enabling role in the universal spread of mobile worldwide. What has allowed the strong, stable growth of mobile connectivity and the number of people connected? The use of technology-neutral licences has removed barriers to market entry and shortened the time-to-market for new services. At the end of 2017, almost half of countries worldwide used technology-neutral

spectrum licences (double the number of five years ago); a further tenth of countries have partially introduced them (see Figure 43, left graph). A large minority of countries, however – two in every five countries worldwide – still only issue technology-specific licences.

Following the trend of allowing more freedom for market players to manage spectrum among themselves, an increasing number of regulators have made available spectrum bands for licence-exempt use. The number of countries thus liberalizing their spectrum policies has leaped from a mere seven back in 2010 to over 50 as of 2017. Half of European countries and a third of CIS countries have established similar regulatory treatment for spectrum. In the other regions, the

Figure 44: Band migration allowed, by region, 2017

2007 | 2017

World | Europe | CIS | Asia-Pacific | Arab States | Americas | Africa

0% 20% 40% 60% 80% 100%
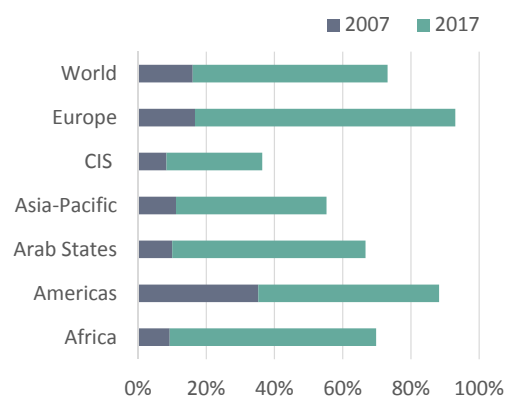
Source: ITU

Figure 45: Spectrum trading frameworks, worldwide and by region, 2017

Spectrum trading practices worldwide, 2017

Spectrum trading allowed, by region, 2017

licence-exempt spectrum is available in around 20 per cent of countries.

For established operators, band migration has allowed them to swiftly reconfigure available spectrum resources and launch new services. Consumers can benefit from technology innovation without additional delay for regulatory approvals as new services are integrated in existing spectrum management framework from the outset. The number of countries allowing band migration has exploded over the past ten years, from less than 20 per cent to close to 80 per cent of countries worldwide as of 2017 (see Figure 44, right graph). In some regions, such as in Europe and the Americas, the practice has been adopted

in 90 per cent of countries. CIS is the region with lowest adoption, standing below 40 per cent.

In-band migration, spectrum sharing and spectrum trading have been instrumental in distributing access and creating vibrant markets. Spectrum trading has generated a lot of debate over the past decade and is still limited to a minority of roughly one-third of countries worldwide (see Figure 45, left graph). Nevertheless, its adoption has quadrupled in a decade and has reached four in five European countries (see Figure 45, right graph). A third of the countries in the Americas region allow spectrum trading as does a fifth of Asia-Pacific countries. Other regions are taking a more cautious approach, relying mainly on

Box 7: The case for spectrum trading

Ronald Coase won a Nobel Prize in economics for the basic theory he developed for enhancing the efficiencies of spectrum management. He studied multiple cases where portions of valuable spectrum were underutilized because they were assigned to users who do not take full advantage of its potential under traditional spectrum assignment regulations.

He showed that the inability to buy and sell spectrum capacity led to economic inefficiencies and that better defining the property rights to spectrum would lead to social welfare-increasing outcomes. This led him to favor market-based mechanisms and spectrum auctions in particular as well as the right for the auction winners to resell, rent, or otherwise make deals that let them reallocate spectrum to its highest and best use.

band migration to encourage new dynamics and efficiencies in spectrum markets.

Overall, spectrum regulations – both at the national and international level – have proved robust. Spectrum regulation has been accorded high government priority and for most countries, it has generated solid foundations for the digital economy. It is clear, nevertheless, that spectrum policies will not ensure universal coverage of mobile, and mobile broadband in particular, in all areas. The importance of spectrum management practices will increase as 5G approaches. Will 5G policies now in the pipeline meet the challenges – and deliver mobile services to everyone, everywhere? Some of the issues are discussed below.

Harnessing 5G and the digital dividend

5G – demystifying the hype

According to ITU's recent report, *Setting the scene for 5G: opportunities and challenges, 2018,* expectations of 5G are high. Many assume it will deliver a transformative promised land – an improved end-user experience, new applications, new business models and new services riding swiftly on the back of gigabit speeds, improved network performance and reliability. 5G networks and services, standing as they do on the shoulders of successful 2G, 3G and 4G mobile networks, are forecast by independent economic studies to deliver very significant economic gains. The following section is an extract from the report.

What is 5G?

At the highest level, 5G is an opportunity for policy-makers to empower citizens and businesses. 5G will play a key role in supporting governments and policy-makers in transforming their cities into smart cities, allowing citizens and communities

to realize and participate in the socio-economic benefits delivered by an advanced, data-intensive, digital economy.

Opportunities

5G promises to deliver improved end-user experience by offering new applications and services through gigabit speeds, and significantly improved performance and reliability. 5G will build on the successes of 2G, 3G and 4G mobile networks, which have transformed societies, supporting new services and new business models. 5G provides an opportunity for wireless operators to move beyond providing connectivity services, to developing rich solutions and services for consumers and 5G is an opportunity to implement wired and wireless converged networks and integrate network management systems.

Commercial 5G networks are expected to start deployment after 2020 (see Table 15), as 5G standards are finalized.[52] By 2025, the GSM Association (GSMA) expects 5G connections to reach 1.1 billion, some 12 per cent of total mobile connections. It also forecasts overall operator revenues to grow at a CAGR of 2.5 per cent, to reach USD1.3 trillion by 2025.[53]

The high speeds and low latency promised by 5G will propel societies into a new age of smart cities and the Internet of Things. Industry stakeholders have identified several potential use cases for 5G networks, and the ITU-R has defined three important categories of these (see Figure 46):

1. Enhanced mobile broadband (eMBB) – enhanced indoor and outdoor broadband, enterprise collaboration, augmented and virtual reality.

2. Massive machine-type communications (mMTC) – IoT, asset tracking, smart agriculture, smart cities, energy monitoring, smart home, remote monitoring.

Table 15: Evolution of mobile networks.

	1G	2G	3G	4G	5G
Approximate deployment date	1980s	1990s	2000s	2010s	2020s
Theoretical download speed	2kbit/s	384kbit/s	56Mbit/s	1Gbit/s	10Gbit/s
Latency	N/A	629 ms	212 ms	60-98 ms	< 1 ms

Source: GSMA, OpenSignal, operator press releases, ITU

Figure 46: 5G usage scenarios
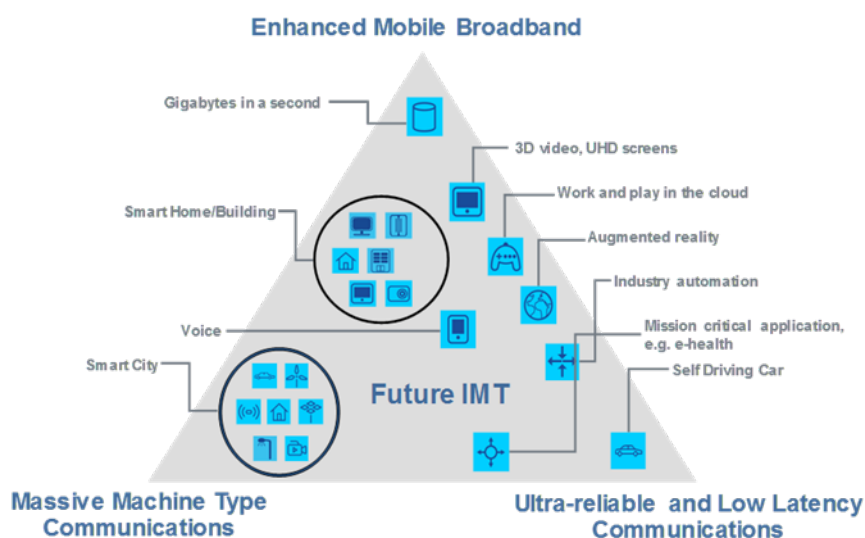
Source: ITU

3. Ultra-reliable and low-latency communications (URLLC) – autonomous vehicles, smart grids, remote patient monitoring and telehealth, industrial automation.

eMBB is expected to be the primary use case for 5G in its early deployments, according to wireless operators. eMBB will bring high-speed mobile broadband to crowded areas, enable consumers to enjoy high-speed streaming for in-home, screen and mobile devices on demand, and will allow enterprise collaboration services to evolve. Some operators are also considering eMBB as the last-mile solution in areas lacking copper or fibre connections to homes.

5G is also expected to drive the evolution of smart cities and IoT through the deployment of a considerable number of low-power sensor networks in cities and rural areas. The security and robustness built into 5G will make it suitable for public safety as well as for use in mission-critical services, such as smart grids, police and security services, energy and water utilities, and healthcare. Its low latency performance characteristics make it suitable for remote surgery, factory automation and the control of real-time processes.

5G's low latency and safety characteristics will play well in the evolution of intelligent transport systems, enabling smart vehicles to communicate with each other, and creating opportunities for connected, autonomous cars and trucks. For

example, an autonomous vehicle (AV) operated via a cloud-based, autonomous driving system must be able to stop, accelerate or turn when told to do so. Any network latency or loss in signal coverage preventing the message from being delivered could result in catastrophic consequences. However, wireless operators believe that AVs have a significant way to go before they come into service, despite ongoing pilots and trials.

More spectrum bandwidth will be required to deploy 5G networks (compared to 4G) to the high capacity requirements, increasing the need for spectrum. In consequence, the industry is making concerted efforts to harmonize 5G spectrum. ITU-R is coordinating the international harmonization of additional spectrum for 5G mobile systems development (Box 8). ITU's Standardization Sector (ITU-T) is playing a key role in producing the standards for the technologies and architectures of the wireline elements of 5G systems.

Policy-makers in governments and NRAs are encouraging early technology pilots to promote early investment in 5G networks and infrastructure, and to aid their understanding of 5G technologies (see Box 9).

In addition, the telecoms sector, comprising operators, vendors and research institutes, has been participating in 5G testbeds independently of NRA or government intervention (see Box 10).

Challenges

Despite the potential economic benefits, the industry remains cautious about the commercial case for investment in 5G. Given the significance of required investment, skepticism remains among some European operators over 5G hype and they question whether they can make money from it. These concerns are supported by the 5G Infrastructure Association (5GIA), an EU-backed body, and by senior telecom executives cautioning against premature 5G launch announcements.[54]

Many 5G announcements are 5G pilots and trials rather than full-scale commercial deployments. There is some way to go before the investment case for operators can be made robustly and before any large-scale commercial deployment can commence.

As an illustration, the estimated cost to deploy a small cell-ready 5G network – assuming fibre backhaul is commercially feasible – can range from USD6.8 million for a small city to USD55.5 million for a large, dense city.

Given the considerable CAPEX investment required in deploying 5G, operators face major challenges in making the investment case for 5G. Policy-makers will need to consider alternative investment models (for example PPPs, loans, challenge funds and investment vehicles) to ensure high upfront CAPEX costs are not a barrier for wireless providers.

Some examples of government intervention include a range of PPP programmes. These programmes can either be: i) publicly led, where the government builds and owns fibre networks, as in Qatar; or ii) privately led, where the government partly funds the development of fibre networks in partnership with the market, as in Germany.

Other approaches include offering grants to local authorities, as in the UK, to construct and upgrade passive assets (such as ducts, fibre networks, data centres, street furniture, etc.). Governments can also offer low-cost loans to operators in return for a guaranteed investment from the operators, as in Malaysia.

Where operators prefer to access capital from private markets, governments can set up investment funds in collaboration with established private sector fund managers to provide operators

Box 9: Government-led 5G initiatives

- The Government of the Republic of Korea, via the NISA, established 5G pilot networks at the 2018 Winter Olympics, providing futuristic experiences such as augmented reality-based navigation.

- A GBP17.6 million government grant has been awarded to a consortium led by the University of Warwick to develop a UK central testbed for connected autonomous vehicles (CAVs). Small cells will be deployed along a route through Coventry and Birmingham where the CAVs will be tested.

- The FCC (US) has encouraged applications from the research community for experimental licences for radio frequencies not granted or assigned, to promote innovation and research through experiments in defined geographic areas.

- The EC Horizon 2020 work programme (2018-2020) is promoting innovation in 5G involving the EU, China, Taiwan, China and the US. Activities include end-to-end testing of cross-border connected and automated mobility, and 5G trials across multiple vertical industries.

- The Federated Union of Telecommunications Research Facilities for an EU-Brazil Open Laboratory (FUTEBOL) is creating research that promotes experimental telecommunication resources in Brazil and Europe. FUTEBOL will also demonstrate use cases based on IoT, heterogeneous networks and C-RAN.

- The Russian Ministry of Communications concluded an agreement with Rostelecom and Tattelecom to create an experimental 5G zone in the hi-tech city of Innopolis.

Sources: https://goo.gl/JWFBCY (Korea Rep.), https://goo.gl/FnLZCd (UK), https://goo.gl/wNVZqs (US), https://goo.gl/iXkYQo (Europe), https://goo.gl/VNeDwn (EU-Brazil), https://goo.gl/4DySs2 (Russian Federation);
Additional information on the economic aspects of spectrum management can be found in Report ITU-R SM.2012; GSMA, 5G Spectrum Public Policy Position, 2016

with equity. This equity can then be used to support operator network expansion programmes.

Other PPP models for incentivizing investment in telecom networks do exist and have been written about extensively.[55]

Not all 5G deployments require government intervention. Some small cell and pre-5G deployments to date have been privately financed.

A viable business case for investment in 5G can be made for densely populated urban areas – always the most commercially attractive regions for operators. The business case for investing in 5G networks outside such areas is more challenging, especially in the early years of 5G deployment. As a result, rural and suburban areas are less likely to benefit from 5G investment, and this may potentially widen the digital divide.

As long as the investment case for 5G remains uncertain, industry and policy-makers should remain cautious and should consider enhancing the availability and quality of existing 4G networks in the run up to 5G. The need for 5G is not immediate. Policy-makers and operators should only consider deploying 5G networks where there is demand or a robust commercial case in favour of doing so.

Moving to 5G, key considerations

Where demand exists alongside high 5G deployment costs, policy-makers can use a range of legal and regulatory actions to facilitate 5G network deployment. These include:

- Supporting the use of affordable wireless coverage (e.g. through sub-1 GHz bands) to reduce the digital divide;

- Commercial incentives such as grants, or PPPs to stimulate investment in 5G networks, as identified above.

An overhaul of the regulatory, government and local authority approaches to digital policy is needed to boost the roll-out of 5G networks. Importantly, this includes ensuring affordable access to public assets thereby strengthening the commercial case to invest in small cell infrastructure and 5G spectrum.

The new ITU report highlights the following 16 key issues – and responses – for policy-makers to consider as they formulate strategies to stimulate investment in 5G networks (see Table 17). Together they represent powerful means of calibrating an overall approach across major aspects of migration and, where appropriate, embarking on a judiciously facilitated, accelerated transition to 5G.

Table 17: Strategies to stimulate investment in 5G networks - key considerations

1)	Investment case	Policy-makers may consider undertaking their own independent economic assessment of the commercial viability of deploying 5G networks
2)	4G network strategy	Until the case for 5G networks can be clearly made, policy makers may consider enhancing the availability of and boosting the quality of 4G networks
3)	Harmonize spectrum	NRAs may consider allocating/assigning globally harmonized 5G spectrum bands
4)	Spectrum roadmap	NRAs may consider adopting a spectrum roadmap and a predictable renewal process
5)	Spectrum sharing	NRAs may consider allowing sharing to maximize efficient use of available spectrum, particularly to benefit rural areas
6)	Spectrum pricing	NRAs may consider selecting spectrum award procedures that favour investment
7)	700Mhz spectrum	Policy-makers may consider supporting the use of affordable wireless coverage (e.g. through the 700 MHz band) to reduce the risk of digital divide
8)	Fibre investment incentives	Policy-makers, where the market has failed, may consider stimulating fibre investment and passive assets through PPPs, investment funds and the offering of grant funding, etc.
9)	Fibre tax	Policy-makers may consider removing any tax burdens associated with deploying fibre networks to reduce the associated costs
10)	Copper migration to fibre	Policy-makers may consider adopting policies/financial incentives to encourage migration from copper to fibre and stimulate deployment of fibre
11)	Wireless backhaul	Operators may consider a portfolio of wireless technologies for 5G backhaul in addition to fibre, including point-to-multipoint (PMP), microwave and millimeter wave (mmWave) radio relays, high altitude platform systems (HAPS) and satellites
12)	Access/sharing of passive infrastructure	Policy makers may consider allowing access to government-owned infrastructure such as utility poles, traffic lights and lampposts to give wireless operators the appropriate rights to deploy electronic small cell apparatus to street furniture NRAs may consider continuing to elaborate existing duct access regimes to encompass 5G networks allowing affordable fibre deployments
13)	Access costs	Policy-makers/NRAs may consider ensuring reasonable fees are charged to operators to deploy small-cell radio equipment onto street furniture
14)	Asset database	Policy-makers may consider holding a central database identifying key contacts, showing assets such as utility ducts, fibre networks, CCTV posts, lampposts, etc. This will help operators cost and plan their infrastructure deployment more accurately
15)	Wayleave (rights of way) agreements	Policy-makers may agree upon standardized wayleave agreements to reduce cost and time to deploy fibre and wireless networks
16)	5G test beds	Policy-makers may consider encouraging 5G pilots and test beds to test 5G technologies, and use cases, and to stimulate market engagement

Source: ITU, Setting the scene for 5G: opportunities and challenges, 2018

Digital dividend

This section is based on ITU, Digital Dividend: Insights for spectrum decisions, 2018 and self-reported data by ITU Member States as part of the 2017 ITU Telecommunication/ICT Regulatory Survey.

The essence of the digital dividend is to open the possibility of re-allocating a large part of the radio spectrum. Like any other spectrum allocation decision, it is about allocating scarce resources and the spectrum use of choice to be defined. In this sense, it is no different to what spectrum managers normally do. However, the implications of the digital dividend make it one of the most important spectrum decisions for years to come.

The bands identified for international mobile telecommunications (IMT) by WRC-07, WRC-12, and WRC-15 opened the possibility for each country to allocate them nationally as the first or second *digital dividend* for the mobile service. Because of interference, cross-border frequency coordination, preferably at regional level, is a pre-requisite for this purpose. A regional coordinated approach, by which all countries in a region jointly agree to use these bands in a consistent way is preferable.

As of the end of 2017, at least 90 countries worldwide reported to have reallocated digital dividend spectrum (see Figure 48, left graph).[56]

Box 11: What is the digital dividend?

The digital dividend is the spectrum that becomes available over and above that required to accommodate the existing analogue television services in a digital form in the UHF bands.

Technical specifications and details on this definition are available in Section 2.1 of Report ITU-R SM.2353-0.

Source: ITU

Figure 47: Digital dividend spectrum
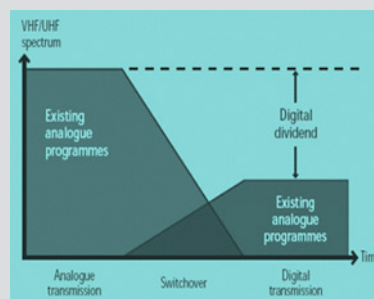
A large majority of European countries and a slim majority of Americas countries account for half of those. The other regions are still half-way through the reallocation of the digital dividend, partly because of the less advanced state of the analogue-to-digital transition. In three-quarters of those countries, spectrum has been reallocated to mobile services (see Figure 48, right graph). Broadcasting has reclaimed the digital dividend in only 5 per cent of countries, such as Afghanistan, Brunei Darussalam and Uruguay, although more may be following suit with the broader redeployment of this spectrum. In a few countries, some of the digital dividend was set aside for fixed wireless services or new and emerging mobile broadband services, for instance for pilot projects. Digital dividend spectrum been assigned or set aside for Public Protection and Disaster Relief

(PPDR) mobile services in at least 26 countries, such as Burundi, Finland and United Arab Emirates.

Allocating the 700 MHz and/or 800 MHz bands to the mobile service would still enable a large portion of the digital dividend to be allocated to television broadcasting in the remaining parts of the UHF band. This allocation however could result in the loss of channels that may already have been negotiated with neighbouring countries. Reconstituting these lost channels as a result of the above allocation to the mobile service and increasing their number to provide additional digital dividend for the broadcasting service is possible. This requires bilateral and possibly multilateral frequency coordination discussions with neighbouring countries.

Figure 48: Status of reallocation of the digital dividend spectrum, worldwide and by region, 2017

Countries having reallocated digital dividend spectrum, by region, 2017

Services to which the digital dividend has been reallocated, worldwide, 2017
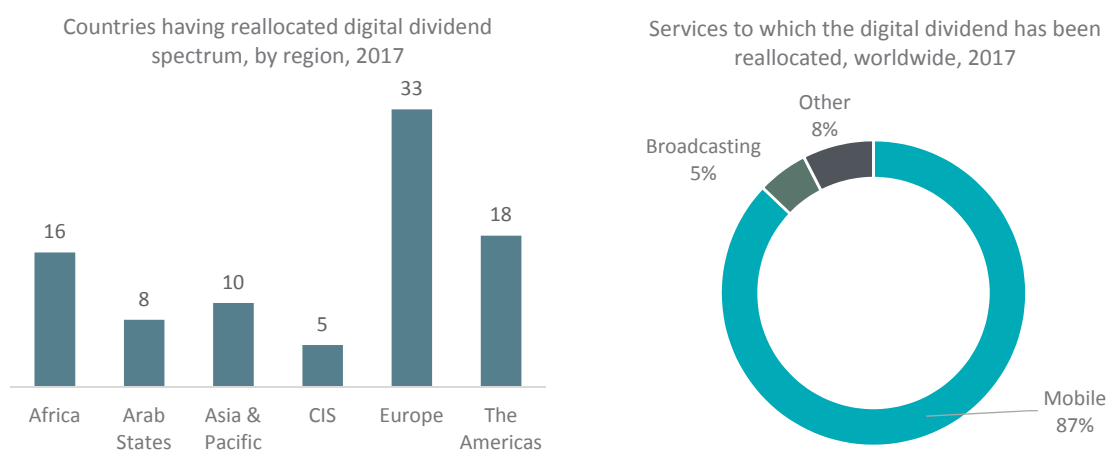
Source: ITU

Figure 49 provides an overview of selected countries regarding the allocation of the first and second digital dividend to mobile services. To date, the US is the only country to have allocated spectrum in the 600MHz band; the US is also the country having allocated the largest portion of digital dividend spectrum so far. Globally, more countries have allocated the digital dividend in the 700MHz than in the 800MHz.

Parts of the bands that may be allocated nationally to the mobile service are currently used in many countries by wireless microphones or military applications. Migration of these services therefore needs to be considered, which may have financial consequences that need to be addressed upfront.

A clear regulatory situation also needs to be established upfront in relation to the handling of possible interference into broadcasting receivers in cases where a base station of the mobile service is established and transmits on frequencies adjacent to those to be used by broadcasting. An improvement to the immunity of broadcasting receivers may also be helpful and is being sought through international standardization to facilitate such situations.

Spectrum licensing for the digital dividend

Licensing of the digital dividend spectrum entails one of the largest spectrum operations for the years to come. Recent decisions have given the opportunity for the introduction of new approaches related to the specifics of the UHF band.

Particular effort has been made to ensure that the licensing process for the use of the digital dividend by the mobile service is 'technology neutral'. The first countries assigning mobile licences in these bands, such as Germany, Sweden and the United States, have not stipulated technology standards or services to be deployed.

Although resolving incompatibility issues is not new for spectrum managers, having different 'unknown' systems being deployed in adjacent channels may complicate matters. Especially when due to great economic and political pressure, spectrum is released before all incompatibility issues are fully understood or resolved. In this light, the practical solution of the Swedish regulator (PTS) may prove an effective way for resolving these issues. In the licence conditions

Figure 49: Amount of spectrum allocated as part of the first and second digital dividend, per frequency band, selected countries, 2017
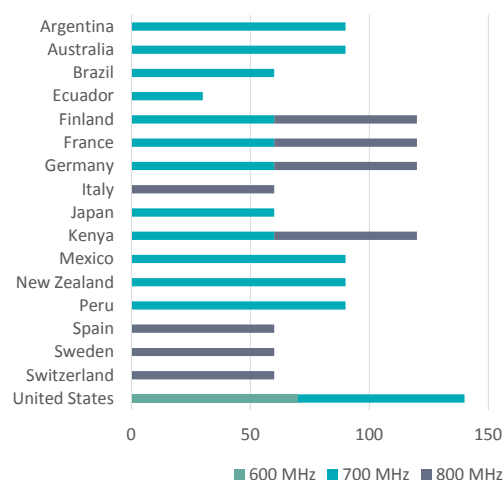
Source: ITU, Digital Dividend: Insights for spectrum decisions, 2018

it is stipulated that the new licence holders are responsible for resolving interference and have to establish a common entity in which they cooperate to resolve any problems that may occur.[57]

A similar approach was followed in the Netherlands when DVB-T was introduced and interference on cable networks was expected. At the time of launching the service, the magnitude of this problem could not be accurately estimated and an entity was established to resolve any interference problems. A similar discussion is now taking place in Europe on the interference of 800 MHz broadband wireless networks on cable networks.[58]

Lifting system or standard requirements can lead to complications and will require careful analysis. Some licence holders might gain competitive advantages, which may lead to market distortions. This may require spectrum managers to revoke spectrum from licence holders.[59] This is a measure with considerable impact and may hamper the objective to interfere as little as possible.

Next to advocating more flexible approaches to spectrum management, promoting more economic incentives for assigning the available spectrum has been discussed and applied over time. Given the focus on the economic value of the digital dividend, market based assignment tools have been increasingly applied in allocating and assigning the digital dividend. This in contrast

Box 12: Benchmarking on spectrum valuation

When allocating radio spectrum, economic, social, educational and cultural values of spectrum usage need to be evaluated carefully. In particular, the following issues need to be considered:

- **Exclusive spectrum allocations for specific services or users.** For example, the decision to set aside a part of the digital dividend for television broadcasting (for example for HDTV) needs to be motivated by the value (both economic and social) of such use. Allocating spectrum for exclusive services will always imply denying spectrum access for others services and users.

- **Use of auctions for spectrum licensing.** When auctioning spectrum it is common that a minimum bid price is determined. To do so, an assessment is needed of the possible migration costs (e.g. example to migrate the wireless microphone band) and cost for resolving harmful interference (e.g. wireless broadband on cable networks) to be covered by governments. Such costs need to be covered in the minimum bidding price.

- **A market-based or administrative incentive pricing (AIP) fee on spectrum licence holders.** Accurately assessing the value of the licence is important as a too low fee will not result in more spectrum efficiency and, reversely, an excessively high fee may result in a financial burden for the licence holder, especially when coverage obligations are also imposed.

Recent country experiences suggest that it is not always necessary to put a value to spectrum bands. For example, a country may decide to follow the EU recommendation and allocate the 800 MHz band for wireless broadband services (for reasons of spectrum harmonization) and assign the spectrum on the basis of a public tender.

When spectrum valuations need to be carried out, they should use a benchmarking approach to estimate a value or to validate the valuation on the basis of economic, cash-flow models. For example, in the US and Germany, the recent 700/800 MHz auctions delivered the actual market value for these bands. However, careful consideration should be given to the specifics of those auctions. One should compare geographical size, population of the country and from there the coverage area, as well as the licence conditions, number of competitors, legal framework and coverage obligations.

The two main approaches in valuating spectrum focus respectively on the economic value and the social value of spectrum. The first is also referred to as private value (which comprises the consumer and producer surplus) and corresponds to the value end-consumers place on the services minus the costs of producing this service. This also includes migration or spectrum re-farming costs and cost to avoid harmful interference. The social, educational and cultural value (also referred to as external value) represent the value of a service which groups of people attach to it and cannot be directly expressed in financial terms.

Source: ITU, Digital Dividend: Insights for spectrum decisions, 2018

whereby spectrum is assigned on the basis of technological considerations such as application type, spectrum efficiency and number of services (see also Box 12).

In recent digital dividend allocations and assignments, the following market (or economic value) based instruments have been applied, which are often interrelated:

- auctions;

- economic or administrative incentive pricing;

- licence trading.

Spectrum auctions have been applied for some years. The main advantage of auctions is that they are transparent, relatively simple and return economic value to society. A well-designed auction can reduce the risks of the 'winners curse'. The so-called simultaneous open multi-round auction is often applied, also in the latest spectrum auctions in the 700/800 MHz bands.

However, auctions should be applied with careful consideration in particular when licensing bidders from different industries, for example the television and mobile industry. In such a case, market distortions may occur and the results of the auction may be flawed. Free-to-air television service providers operate a different business model to mobile service providers.[60] The business model of free-to-air television service providers does not reflect consumer but advertiser value.

In addition, their individual bids cannot reflect network effects, that is to say the value of having a complete bouquet of services. One way to resolve such distortions is to avoid to auction service (or technology) neutral licences but licences with service stipulations.

In countries such as the UK, France, Australia and New Zealand, so called 'administrative incentive pricing' (AIP) regimes have been introduced. These pricing regimes are not based on costs but on economic value to make spectrum allocation more flexible and return this economic value to society. For determining the economic value of licences (i.e. the licence fee to be paid each period), complex models are used based on principles of 'next-best-alternative' or opportunity pricing.

Finally, trading of licences is already applied in some countries. In the UK, Ofcom intends to allow trading of the 800 MHz licences. Setting trading conditions can be complex[61] and can be closely related to other licence conditions. With trading licences, the spectrum manager tries to reduce its interference in the market. The question arises whether an oversight of this trading is necessary (i.e. the spectrum manager should check the trade). For example, are new licence holders capable or qualified to comply with the spectrum licence conditions? Hoarding could also be a risk. When a licence holder does not use the spectrum the licensee may be required to return the licence (or a part of the rights). To avoid competitors entering the market, incumbent licence holders could decide to sell to a 'related' party.

Clearly, this discussion shows that spectrum managers should carefully incorporate new spectrum management approaches in the design of digital dividend allocation and assignment procedures and should not underestimate the effort required to arrive at a solution appropriate for their market.

4.4.　Up for debate

Established regulatory areas exist where clear patterns for best practice have emerged, but many areas lack consensus and consistent practice across regions, regulators and market players.

Most issues at the heart of the regulatory debate are related to money or data, or both. The following section looks at four such issues and analyses latest trends surrounding them:

1. **Digital platforms** – the global data pipes which capture the monetary value of data and turn it into potent business models, including **net neutrality** – an issue with far-reaching implications.

2. **Data protection and privacy** – a central issue in the debate on digital platforms and beyond, looking into new rules as to how data can be used and cashed out – and if this should be an option at all.

3. **Taxation** – a major instrument for governments to balance their budgets. In developing countries where there may be a high proportion of cash transactions, taxation of the telecom/ICT sector is often an important part of the formal economy.

Towards the regulation of digital platforms?

Digital platforms have become a true melting pot of technologies, ideas and business models bound up with many new, big regulatory issues – from competition to consumer protection to universal access. It may even be necessary for stakeholders and policy-makers to 'unlearn' many lessons learned in pre-digital rulebooks to deal with digital platforms.

Greater scrutiny and pressure

Digital platforms have managed to remain under the regulatory radar for a long time (see Figure 51). Since their inception and despite generating extensive and contentious public debate globally, they have generally been exempt from or non-categorized for the purposes of regulation – and in effect have enjoyed a prolonged regulatory honeymoon. Often, existing regulations (from ICT regulators or others) may not apply, simply due to

the categorization problem, as digital platforms can straddle different industries.

Digital platforms and their handling of data security, privacy, zero-rated service offerings, are now coming under regulatory scrutiny. This follows on from multiple court cases (mainly in Europe), recent cases of data mishandling and failures in content moderation with adverse social impact. A group of like-minded regulators is also leading the way to greater, and more targeted, regulation over the practices of digital platforms, from fiscal compliance to user data management to content moderation. In future, more regulators from different sectors will look to harmonize their approach to digital platforms with the rest of ICT services, for improved regulatory consistency and enforcement.

Self regulation, targeted regulation and muted regulation

Digital platforms are one area where consumer-centered self-regulation is most needed, as imposed regulatory alternatives might be disproportionate or even counter-productive. Self-regulation, however, may be self-serving[63] and inadequate for large, global digital players. In effect, self-regulation in this case may be equivalent to a regulatory honeymoon. Large numbers of disputes indicate that regulatory frameworks are overwhelmed and cannot cope with problematic market behaviours (including, for example, anti-competitive practices, inappropriate data sharing and/or predatory pricing). Increasing the volume and scope of regulation may not be a plausible option, and may possibly generate positive and negative effects – a more balanced, neutral approach may be better than a heavier framework. Targeted, unified regulation in regard to specific market failures may be one way to address issues, while preserving incentives for innovation and investment.

An evolved version of targeted regulation is 'muted' or 'contextual' regulation: regulation is 'switched on' when limits of regulatory tolerance are exceeded. Regulation only targets certain market behaviours in certain situations. Muted regulation is an alternative to traditional always-on regulation, and could be less intrusive and more effective - as regulation is not needed to the same degree at all times and in all circumstances. Using this approach, issues from content moderation

Box 13: What digital platforms are and aren't

Regulators need to respond to difficult questions in addressing digital platforms.

For the purposes of this report, we use the definition of digital platforms of the ACCC 2018 inquiry, according to which digital platforms are a short name for "*digital search engines, social media platforms and other digital content aggregation platforms*".

So what exactly are digital platforms?

Digital platforms **are** often:

- **Global –** few services or applications of unique providers have gathered as many users previously. More people use social media, for instance, than have access to clean drinking water and sanitation.

- They may also be **'borderless'**, insofar as national frameworks and jurisdictions may struggle to control their operations, due to their global nature – let alone tax them.

- **Desirable –** these services can appeal to several billions of users. The demand for some platforms and apps is huge and growing.

- **Opinion-building** – for better or for worse, digital platforms can make or break local businesses, markets and possibly even political and social systems. Their power has grown exponentially and it is not clear if the organizations themselves are able to handle it.

- Funded by **advertising and monetizing user data** as part of their native business models. It is clear that many digital platforms collect, manipulate, process and analyse user data as a core part of their operations.

- In addition, many are **moving into traditional industries**, providing alternative services based on digitally native business models and are creating disruption across the economy. This makes them difficult to classify, following established categories – for example, in 2017, the European Court of Justice ruled that Uber is officially a taxi firm[62] when deciding between categories of taxi firm or online platform.

- They may **straddle often unrelated industries** – for example, Google straddles unconnected sectors of search, advertising, translation, maps and navigation, satellite imagery, e-mail (Gmail) and documents. In reality, all these areas deal with data – just one of Google's many competencies.

Digital platforms **are not:**

- **Solely 'Over-the-Top'** content providers. These have become major data carriers and infrastructure providers in their own right, building massive Content Distribution Networks (CDN) and submarine cables.

- **Public networks**, so they cannot be considered as utilities.

- **Open access** over their infrastructure. According to critics, this is ironic as digital platforms were initially able to access telecom networks. User data portability remains limited, where available, too.

- **Transparent**, especially with regard to data practices and user content management. Recent examples of data mismanagement have fueled heated public debate globally.

- **Regulated** in most fields of their operations. This can give digital platforms a sizable competitive advantage and effectively, a regulatory honeymoon.

Source: ITU

to user data management could be handled by internal mechanisms without direct supervision or guidance. Unlike self-regulation, however, if key parameters are exceeded, regulatory inquiry and enforcement are possible.

Arguably, regulatory models are bound to evolve towards more harmonized regulatory approaches to regulating digital markets irrespective of who provides services and with a strong focus on consumer protection. Ultimately, the status of market players in the regulatory process is likely to be elevated to a partner and ally, moving away from the traditional relationship between regulators versus regulated entities. Collaborative

regulation is the next frontier and digital platform regulation may serve as a launch pad towards it (see also section 4.5).

Status of digital platform regulation

A growing number of regulators have turned their attention to digital platforms with varying expectations. One in five had been given a mandate to regulate digital platforms in 2017 (see Figure 51), although in the majority of countries, that mandate may appear vague. According to ITU data, social media and CDNs are addressed frequently in most regulatory frameworks, together with related issues such

Figure 50: Maturing patterns for digital platform regulation

| Regulatory honeymoon | Indirect/selective regulation | Targeted regulation | Muted regulation | Regulatory harmonization | Collaborative regulation |

01 — 02 — 03 — 04 — 05 — 06

Source: ITU

as child grooming, sexual predation and hate speech. Countries with national digital platform regulations[64] in place stands at 7 per cent of countries worldwide, with 10 per cent of countries looking into issuing regulatory rules. Azerbaijan, Croatia, Guinea, the Islamic Republic of Iran, Latvia, Morocco, Pakistan, Serbia, Sierra Leone and Somalia are all planning or adopting possible regulation over digital platforms.[65]

Africa, Asia-Pacific and Europe have the highest number of regulators with a digital platform mandate (see Figure 51, right graph). Europe has the strongest regulatory focus on digital platforms, with the highest number of national regulations in place – in addition, EU-level regulatory decisions can be passed into national law. Europe is also the region with the most consistent regulatory treatment of digital platforms (see also Box 14).

Finding the right balance for digital platforms

Recent practices related to competition and the handling of user data have prompted some regulators to investigate further patterns of market behaviour and the implications for society and the economy.

Consultations are ongoing around the world. Remarkably, many government agencies are leading inquiries in different countries, underlining the high levels of interest in Internet platform regulation and its impact. Parliament and other government executive arms are also leading the way in finding the right regulatory balance for digital platform services – testimony to how 'digital platforms' are impacting sectors beyond ICT.

For example:

- **Australia:**

The Australian Competition and Consumer Commission (ACCC) has opened an inquiry to examine whether platforms are exercising adverse market power in commercial dealings to the detriment of consumers, media content creators and advertisers. ACCC will examine longer-term trends and the effect of technological change on

Figure 51: Status of digital platform regulation, worldwide and by region, 2017

worldwide, 2017

by region, 2017

Africa   Arab States   Asia & Pacific   CIS   Europe   The Americas
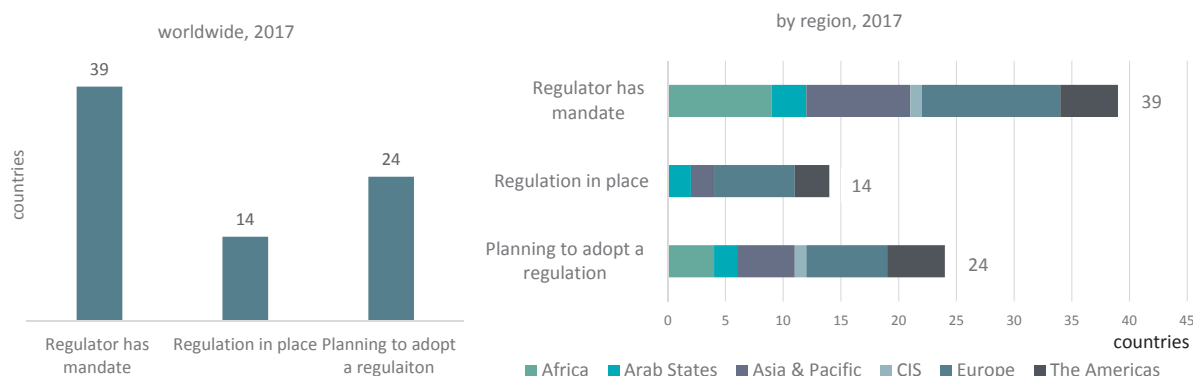
Source: ITU

Box 14: The EU harmonized approach to digital platforms

A high-level overview of the current state of digital platform regulation in EU includes:

- New proposed regulation on promoting fairness and transparency in online platforms, providing small businesses with a safety net in the digital economy.
- The 'data portability' right to take user data from one platform to another (for example on social networks), enshrined in the General Data Protection Regulation (GDPR), is expected to increase the multi-homing options for users and hence competition. The GDPR and the accompanying e-privacy regulation also make it illegal in many cases to combine consumer data from various platforms without an individual's consent.
- Adopted recommendation on the fight against illegal content online.
- Following a public consultation on fake news and online disinformation,[66] no EU regulation will be adopted for the time being on fake news.

Areas for future regulatory attention:

- Algorithms, including ethical aspects and decision-making
- Platform interoperability

Some examples of enforcement rules with regards to digital platforms:

- Video-sharing platforms such as YouTube will need to take concrete measures to filter out copyright infringing material, and to protect minors and citizens from illegal and harmful content; however, it is not clear whether this will apply at the EU or at the national level, as individual countries may have different national definition on what is illegal.
- Online platforms like Twitter and Facebook will be asked to track and remove fake news. Initiatives could also be stepped-up at the national level.
- Non-national video-streaming services such as Netflix will need to contribute to local film funds.

Source: ITU research, European Commission, Jacques Delors Institute, Cullen International, various others.

competition in media and advertising. The final report is due by June 2019.[67]

- **Hong Kong, China:**

The Hong Kong Competition Commission has said that it will not examine the major platforms such as Amazon and Google, citing agency inexperience.[68]

- **Europe:**

The EU has launched a public consultation on digital ethics[69] to examine complex philosophical questions relating to the existence and running of digital platforms. Are new technologies shaping our values? Can data protection rules and laws alone regulate new technological developments? The consultation aims to gather food-for-thought on existential issues that may indicate a future direction for regulation of digital services, among others.

- **India:**

The Telecom Regulatory Authority of India (TRAI) announced in September 2018 that the scope of

the ongoing consultation on OTT players would be narrowed down to look into potential regulatory imbalances and ways to remedy those.[70] This consultation follows the previous one in 2015, which culminated in a recommendation focusing on net neutrality, leaving OTT aspects aside.

- **UK:**

The UK Parliament has opened an inquiry exploring how the regulation of the Internet could and should be improved, including through better self-regulation and governance, and whether a new regulatory framework for the Internet is necessary or whether the general law of the UK is adequate. This inquiry will consider whether online platforms which mediate individuals' use of the Internet have sufficient accountability and transparency, adequate governance and provide effective behavioural standards for users.[71]

Legal and regulatory frameworks already integrate a number of aspects related to digital platforms. These frameworks vary – both in general perspective and focus. By way of illustration, a

few examples of recent or imminent regulatory decisions include:

- **A digital level playing field in Colombia**

Colombia has been in process of drafting a new law, which includes OTTs with other providers of audiovisual communication services, i.e. regulation would apply independently of the network or device used to provide or access audiovisual content.

- **India is formalizing rules on data ownership and security**

TRAI released in 2018 its much-anticipated Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector in India.[72] Although not directly reflected in the title, the recommendation considers digital platforms extensively.

- **Myanmar has banned zero-rate services, while other countries continue to allow them**

The decision of Myanmar came after reports emerged about outbreaks of violence and political strife that local activists blame partly on Facebook.[73] The Government of Papua New Guinea is considering a similar ban, following a one-month suspension period.[74] Other countries report similar events, such as Sri Lanka, Cambodia and the Philippines, but have not taken a regulatory stand against Free Basics.

- **Cloud providers come under the purview of regulators in Saudi Arabia**

Saudi Arabia's telecommunication regulator, CITC, has published a Cloud Computing Regulatory Framework aimed at clarifying the rights and obligations of cloud service providers and users of cloud services. It establishes a framework to manage the potential security risks connected with cloud services and encourage improved quality of service.[75]

- **Viet Nam**

A new cybersecurity law in Viet Nam requires foreign digital platforms to open a Vietnamese office and store their data there. They will also be required to provide user data to the public security ministry at the government's request, in cases where the government believes the law may have been violated.[76]

High-profile court cases

Partly in line with the growth in their pervasive use, there is controversy on topics related to digital platforms, and high-profile court cases are multiplying in all regions. The following is not an exhaustive list, but reflects the range and diversity of emerging issues:

- The Brazilian Supreme Court will rule on procedures applicable to US companies, such as Facebook, to give authorities access to electronic communications during criminal investigations.[82]

- Likewise, the US Supreme Court will decide whether a warrant is needed to access mobile phone location records.[83]

- EU courts have recently issued a number of decisions on cases related to competition in digital markets (see Box 14 above).

- A German court has filed an enquiry to the European Court of Justice for a preliminary ruling on whether Internet-based e-mail services constitute regulated telecommunication services in the high-profile Gmail Case.[84] The outcome of this case is seen by some as a seminal test case for the regulatory fate of OTT services in Europe.[85]

- An Italian administrative court has ruled that Google Ireland and Google Italy must provide the Italian regulatory authority (AGCOM) with information on the company's advertising revenues generated in Italy.[86] Google had brought the case to challenge AGCOM's original decision to require this reporting.

- Anti-trust suits have proliferated across Asia. The Ministry of SMEs and Startups in the Republic of Korea has recommended an investigation of eBay Korea,[87] and JD.com filed an anti-trust suit against Alibaba in January 2018 in a Beijing court according to some sources.[88] In addition, the digital business platform Airbnb has been probed for anti-trust violations in Japan.[89]

Box 15: Do OTT providers need to be regulated? The CTO view

The Commonwealth Telecommunications Organisation (CTO) carried out a survey-based study to better understand the challenges and opportunities of OTT services and the need for regulation. The key findings confirm the diverging views of stakeholders on the need to regulate OTTs or not. Questionnaires were sent to stakeholders in both Commonwealth and non-Commonwealth countries.[77] Four broad categories of stakeholders (sectors here) were targeted:

1) Government, Regulators & Policy-makers[78]

2) ISPs, Telecom, Broadcast & Other Network Operators[79]

3) OTT Service Providers, Vendors, and Content & Application Providers[80]

4) Consumers, Civil Society & Advocacy Group

The survey results and the analysis carried out show the diverging views of stakeholders.[81]

Key findings

Legal and regulatory frameworks: Governments, regulators and policy-makers as well as telecommunication and network operators are broadly of the opinion that such regulatory frameworks currently do not address OTT services and need to be adapted to address current issues related to OTTs; end users felt the same. OTT service providers were of the opposite view and overwhelmingly voted against the adoption of regulatory frameworks in the future.

Figure 52: Is there a need to develop a regulatory framework for OTT services?
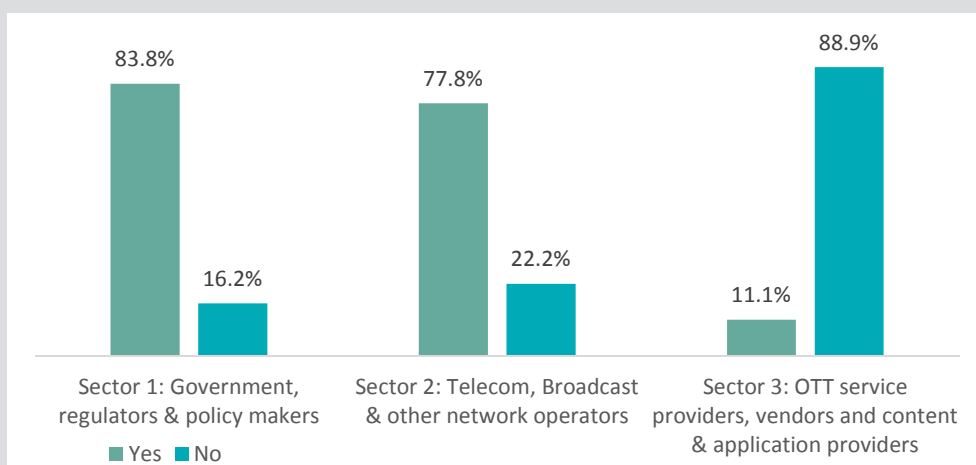
Source: CTO

Application of the regulatory framework to both local and international OTT service providers: The majority of governments, policy-makers and regulatory bodies, and telecommunication and network operators are in favour of a regulatory framework to be applied to both local and international OTT service providers offering communication services (such voice, messaging and video call services via Apps) to local consumers. Conversely, 89% of OTT service providers are opposed to the idea.

Upkeep of networks: While 100% of ISPs, telecom, broadcast and other network operators are of the opinion that OTT service providers should contribute to the upkeep of the network(s) they utilize, only 65% of governments and regulators and 11% of Sector 3 OTT service providers share this view.

Contributions to Universal Service Fund (USF): 100% of OTT service providers do not support the idea of having a requirement for OTT service providers to contribute to USF. In contrast, a majority of governments, policy-makers and regulatory bodies, and nearly 67% of telecommunication and network operators feel they should.

Quality of Service (QoS): Almost all government, regulators and policy-makers and ISPs, telecom, broadcast and other network operators agree that there are no QoS parameters currently in place in their jurisdictions for OTT service providers.

Net neutrality: An overwhelming majority of respondents from stakeholder listed under 1, 2 and 3 agree that net neutrality should be considered as one of the key issues to take into account when addressing the dynamics of OTTs.

Safety, Data Protection & Privacy: 100% of stakeholders from the different sectors all consider these as important issues in the provision of OTT services.

Interdependence of traditional network services and OTT services: A majority of respondents from all stakeholder groups believe that traditional network services and OTT services are interdependent given that consumer demand for OTT services drives demand for data services.

Impact of regulation on innovation: Nearly 89% of OTT service providers are of the opinion that the impact would be extreme while only 11% of Sector 2 believes the impact would be significant. On the other hand, nearly 49% of governments and regulators believe the impact would be moderate; nearly 19% believe the impact would be slight while another 14% believe there would be no impact at all.

These results confirm the diverging views and interests of operators and OTT players and their opposite views on regulatory interventions. As further stressed in the analysis, governments and consumers emerge to a certain extent as the adjudicators in the regulatory debate. The results of the survey provide a useful indication on the strength of sentiment for and against regulatory change going forward.

Source: Adapted from CTO, Over-The-Top Services Understanding Challenges and Opportunities, 2018

ITU's work to monitor digital platform regulation

Given the importance of digital platform regulation for ITU membership, ITU's work programmes explore:

• ITU-D Study Group 1 Question 3/1 on Emerging technologies, including cloud computing: m-services, and OTTs: Challenges and opportunities, economic and policy impact for developing countries[90]
• ITU-D work stream on policy and regulation[91]
• ITU-T Study Group 3 on Tariff and accounting principles and international telecommunication/ICT economic and policy issues[92]

There are as yet few firm conclusions, but ITU membership continues to monitor this evolving situation to support Member States as they review their regulatory approaches to telecommunication/ICT issues, including the telecommunication aspects relating to the operation of digital platforms.

Digital platform regulation effectively mirrors virtually every other regulatory issue related to ICT service providers, but with more complexity and controversy. A high-level mapping of issues is illustrated in Figure 53. Discussion on some of

these issues is provided in the respective thematic sections (see sections in chapter 4).

In a nutshell, regulatory practices and mandates related to digital platforms diverge and there is no clear pattern of digital platform regulation to date. However, there are growing calls for and agreement that digital platform regulation should provide oversight and shelter from bullying, racial hatred and online abuse.

Internet content

Some of the first regulation has targeted online content, an umbrella term used to cover issues as broad as child online protection and fake news. Such regulation provides general guidance on dealing with content over the Internet and has a scope broader than just digital platforms. Internet content regulation has not yet become mainstream – just over a third of countries worldwide count Internet content in their digital regulatory toolbox (see Figure 54). In comparison, broadcasting content is unregulated in only 6 per cent of countries, versus the majority of countries (58 per cent) for Internet content. ICT regulators in a fifth of all countries have been dealing with Internet content, while ICT regulators in a quarter of all countries have been in charge of broadcasting content. Self-regulation for both are at odds with the other trends in content regulation, and stand at a mere 6 per cent. It is worth noting that government ministries are four times less involved in regulating Internet content than broadcasting content.

Figure 53: Digital platforms: mapping of issues of regulatory interest

Universal access & service

Competition

Taxation

Infrastructure sharing

Privacy & data protection

Consumer protection

Inter-connection

Data portability
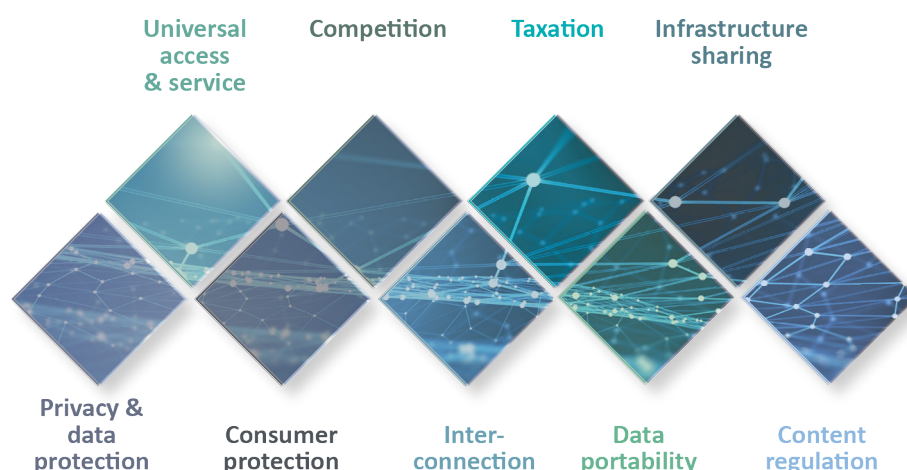
Content regulation

Source: ITU

There a clearly a lack of agreement on who should regulate Internet content, and no uniform pattern as to what Internet content regulation should cover, tolerate or forbid. Ultimately, Internet content regulation can develop towards a more open, safer Internet, or towards a more controlled online environment.

It is worth noting that the regulation of Internet content is less collaborative than regulation of broadcasting content. Eight countries see more than one entity involved in Internet content regulation, while 43 countries have multiple regulators involved in broadcasting content – a counter-intuitive trend, given the transversal nature of Internet content and the size of the population reached.

Net neutrality

The mere term is divisive. For some, it is the incarnation of the 'young and free' Internet. For others, it is about money and choosing to pay more for better or 'guaranteed' services – or to pay less for services delivered on a best-effort basis. Many see it as a technical issue of traffic management, indispensable for carrying rapidly growing volumes of Internet traffic over congested networks. There are also those who wonder whether, after more than a decade of global debate, national net neutrality regulations make any real difference.

Although net neutrality has been one of the most hotly debated regulatory topics in relation to the Internet over the past few years, views and regulations diverge widely, although the majority

Figure 54: Who regulates content?, worldwide, 2017

	Sector Ministry	Other Ministry or gov. body	Regulator	Self-regulation	Not regulated
Internet content	8%	8%	21%	6%	58%
Broadcasting content	20%	43%	25%	6%	6%
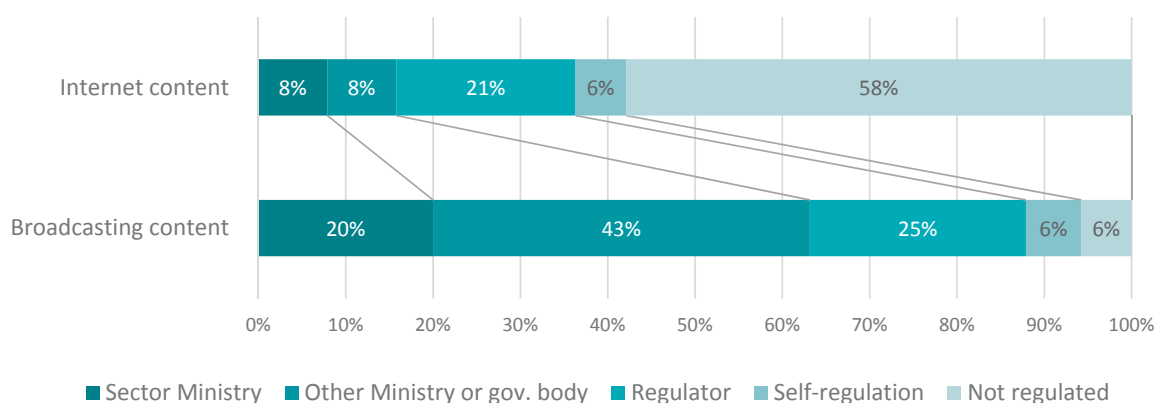
Source: ITU

Box 16: Pros and cons in the net neutrality debate

At one level, net neutrality refers to debates about the way that Internet Service Providers (ISPs) manage the data traffic carried on their networks when data is requested by broadband subscribers or end-users from digital platforms, as well as when traffic is exchanged between end-users. Choices in the network management layer can then go on to shape the way in which content can be accessed and viewed over the web as a whole.

A central concept in net neutrality is the *best-effort Internet*, which is about the equal treatment of data traffic being transmitted over the Internet, i.e. that the 'best efforts' are made to carry data, no matter what it contains, which application or platform transmits the data, where it comes from or where it goes. The benefits of the best effort Internet notably include the separation between application and network layers of the Internet. This separation enables innovation of applications independent of the ISP, thereby enhancing end-user choice.

The pros and cons of the debate over net neutrality include:

- Supporters of net neutrality cite two major concerns. The first is that breaking the Internet down into packages renders pricing confusing and difficult to compare, providing cover for mobile operators and ISPs to increase overall costs and pocket the difference. The second is that an exclusive list of apps and services that receive preferential treatment divides the Internet into a 'two-speed Internet', which runs the risk of entrenching incumbents at the top of the field, while making it very hard for start-ups to grow to the same scale.

- Some carriers have argued that net neutrality is an unnecessary regulation that will stifle competition and slow the deployment of broadband technologies.

- In contrast, others perceive net neutrality as encouraging greater competition in online content and services. By keeping broadband providers from raising artificial price barriers to competition, net neutrality preserves the egalitarian, 'bit-blind' principles that may have made the Internet historically one of the most level playing fields in history.

- If companies such as Netflix and Amazon are forced to pay additional fees in the United States to have their streaming services included in offers, consumers are likely to pay the price, not just in the US, but also in other countries where these companies offer international services.

- Such companies will ultimately also have to develop the necessary skills and tool-sets to navigate an Internet that doesn't guarantee a level playing field, since they will have to negotiate with Internet providers to remain competitive. In this way, an unregulated Internet in one jurisdiction could potentially feed into a push to instill the same legal environment elsewhere.

Source: ITU

of countries worldwide still have not yet developed any legal basis for net neutrality enforcement. Just over a quarter of all countries have a policy about net neutrality (see Figure 55, left graph). From the 55 countries with enforceable rules in place, the two main instruments used to define net neutrality are laws and regulations. In five countries, there is a broad overarching policy in favour of net neutrality, without specific regulatory mechanisms to enforce it.

Europe is the region with highest number of countries with national net neutrality rules using various legal instruments (see Figure 55,

Figure 55: Net neutrality rules, worldwide and by region, 2017

worldwide, 2017

Have policy 28%

No policy 72%

by region, 2017

■ Broad overarching policy ■ Law/legislation ■ Regulation ■ Other
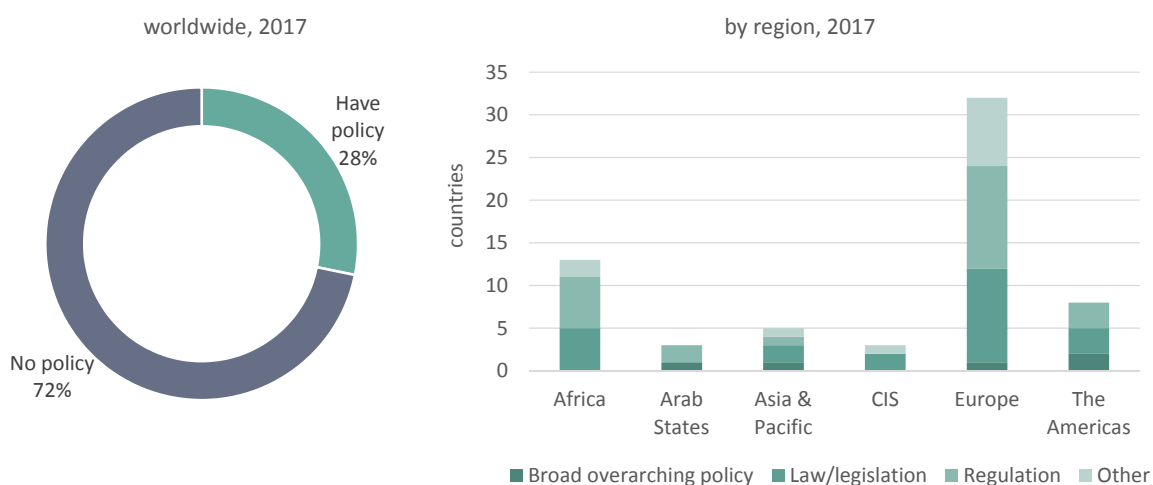
Source: ITU

right graph) and these are related to Directive 2002/22/EC on the open Internet (amended in 2015). In Africa, the region with the second highest number of countries with such rules, provisions for net neutrality are mainly included in the operator's licence. In the Americas, net neutrality is most commonly viewed as a high-level principle and related rules and definitions are set in broad overarching policies. In CIS, the rules are predominantly entrenched in law. Across Asia, fewer countries consider net neutrality a regulatory issue in its own right, with the notable exception of India (see also Table 17).

Net neutrality has now become a political issue. The US Federal Communications Commission (FCC) recently repealed world-pioneering regulatory rules generating global debate,[93] *de facto* de-regulating net neutrality and declaring that it is no longer an issue in the digital world. Conversely, in France, the President of the National Assembly recently proposed to include net neutrality in the French Constitution, suggesting it be given the status of a fundamental right. As a result, a working group of MPs and senators has been created to work on a constitutional charter of rights and freedoms in the digital age.[94]

Between these two extremes, many countries are considering enshrining net neutrality in national legal frameworks while the majority of countries continue to ponder regulatory action.

At this stage, public debate and collective thinking about the immediate and far-reaching

consequences of regulation are key to guarantee the smooth running of networks and the inclusive, non-discriminatory access to digital content and services. With or without codified ex ante net neutrality rules, it is important to create a solid, positive relationship between digital platforms and regulatory agencies.

Zero-rated services

From a regulatory perspective, zero-rated services can be attributed to either a market-driven approach or a regulatory loophole. Either way, these services have not only generated a lot of public debate, but have also become extensively-argued cases in many national or supra-national courts.

The regulatory landscape for zero-rate services is nascent and very few countries have taken a clear legal stand. According to 2018 data, a handful of countries have banned zero-rated offerings (Korea (Rep.), Myanmar, Norway, Togo) although Norway has nevertheless allowed Telia's zero-rated music streaming offer.[98] A few countries have explicitly allowed zero-rated services, such as Germany and the Netherlands[99]. In some countries, the provision of zero-rated services is part of mobile operators' licences. The large majority of countries do not have clear ex ante rules on zero-rated service delivery.

In many countries, such services are deployed without a legal framework specifically designed for them. In 30 countries worldwide, offers fall

Table 18: Selected national regulatory approaches to net neutrality, 2018

Rationale	Observations
EU rules on net neutrality (open Internet), 2016 Regulation (EU) 2015/2120	
The approach directly applicable in 27 EU Member States is meant to avoid fragmentation and a patchwork of national rules, which is seen as better for business – especially in the case of 5G and broadband investments, which require legal certainty. (Source: Andrus Ansip, Vice-President of the European Commission, in charge of the Digital Single Market at Mobile World Congress 2018)	- This regulation has been criticized as being too heavy-handed to operators, while being too loose for digital platforms; seen as and has been argued to potentially hamperinghamper network investment. - After the first year of application of the Net Neutrality regulation, a BEREC report acknowledged that most NRAs are still at an early stage of the implementation of net neutrality rules. - Loopholes exist – for example, when Netflix entered the European market in 2012, some national telecom companies forced it to pay 'tolls' to deliver content to customers. Netflix did not name the companies but told a regional regulator in a letter that the dispute showed "the importance of strong net neutrality rules." (Source: Contribution by Netflix to the public consultation on BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules)
US Net neutrality rules	
In 2018, FCC repealed net neutrality rules adopted in 2015. The old rules: - banned blocking, throttling and paid prioritization; - required ISPs to offer equal access to all web content without charging consumers for higher-quality delivery or giving preferential treatment to certain websites. Under the new rules - in practice, US has returned to the framework which governed the Internet from 1996-2015; - broadband service isn't considered as a utility any more (Title II of the Communications Act); - the Federal Trade Commission, the top body for consumer protection may take overall responsibility for the Internet again. The new rules: - increase the transparency requirements of ISPs so they must publicly disclose information regarding their network management practices, performance, and commercial terms of service; - create an agreement in which the FCC and FTC work together to coordinate on consumer protection. (Source: FCC)	The new rules allow broadband providers to block websites on content grounds, decide which apps consumers can use, charge online services to reach subscribers, create fast lanes that favour wealthier companies, and may make it more expensive for local and niche sites to reach readers.
FRANCE	
Now that net neutrality has been laid down in EU law, ARCEP is considering applying net neutrality to devices. (Source: ARCEP, France) Smartphones are just the tip of the iceberg – voice assistants and connected speakers may prove even less neutral than smartphones. Game consoles, smartwatches and connected cars all share the same issues. ARCEP has been scrutinizing the limitations imposed by device manufacturers so users do not end up being locked into a closed ecosystem. For instance, you should be able to uninstall all pre-installed apps on your phone or be able to use an alternative to the App Store or Play Store. According to ARCEP's President, the findings of the report can be passed as a law in France. (Source: TechCrunch)	Some observers consider it may be too late to regulate smartphones and too early to regulate voice assistants. The debate has also raised questions as of which government agency would have jurisdiction to regulate devices. Others have questioned the effectiveness of national regulations in this case. (Source: The Medium)

Table 18: Selected national regulatory approaches to net neutrality, 2018 (continued)

Rationale	Observations
INDIA : TRAI's recommendations on net neutrality 2018	
The regulations are considered by some as the world's strongest and most progressive policy on equal Internet access for all and affirm the Indian Government's commitment to a free and fair Internet. TRAI has stated that "Internet access services should be governed by a principle that restricts any form of discrimination or interference in the treatment of content, including practices like blocking, degrading, slowing down or granting preferential speeds or treatment to any content." (Source: TRAI, India; BBC; Economic Times of India)	The rules do not apply to 'critical IoT services' or 'specialized services', including autonomous vehicles and remote surgery operations (which have been compared to ambulances that can legally disobey traffic rules, or in this case, get prioritized status to maintain service quality). The rules also do not allow the provision of zero-rated services. ISPs will need to agree to the deal when they sign licence agreements with the Department of Telecommunications. ISPs that violate the rules could have their licences cancelled. (Source: The Verge)
JAPAN - Unregulated	
The Ministry of Internal Affairs and Communications takes a largely hands-off approach to regulating Internet service. Much of the regulation in the country is voluntary self-regulation by the industry itself, which grew out of the privatization and break-up of the state-owned Nippon Telegraph and Telephone Corporation in the late 1990s. Today, the Japanese Government considers broadband Internet service to be a portion of a 'universal telecommunications service' that is to be provided fairly and stably.	
AUSTRALIA - Unregulated	
Australia has no net neutrality laws, with Internet service regulated by the Australian Communications and Media Authority. Across the country, ISPs regularly offer zero-rated content through partnerships with content providers. The system works because of the large number of ISPs (63 according to the Australian Bureau of Statistics), strong consumer protection laws to prevent ISPs from throttling or blocking competitors' content, and rules mandating that ISPs have to be transparent in their policies.	
RUSSIAN FEDERATION - Net neutrality laws, 2016	
The legislation focuses on non-discriminatory access to content.	The regulations demonstrate than in most situations, net neutrality may not be the only issue. A neutral approach to data does not mean any data is permissible, and an ISP can still choose to block access to some Internet sites if it has the ability to do so.
BRAZIL - Civil Rights Framework for the Internet, enacted in 2014 and further refined in 2016	
The legislation only allows Internet service companies to prioritize certain types of traffic for technical reasons – such as overloaded networking capacity – or to allow network use by emergency services. Also, proposals have been put forward to grant publicly owned telecom infrastructure to private companies for free. The country's telecom companies are also suggesting that regulators align with the new US rules.	Despite these rules, enforcement has proved challenging. Some of the largest telecommunications companies have been providing their mobile Internet customers with preferential access to content on sites and services owned by business partners, and in particular large foreign corporations, including Facebook, Waze, Spotify, WhatsApp, Twitter and the music-streaming service, Deezer.

under the scope of general telecom/ICT laws and regulations. In the EU, the umbrella regulation for such services includes the Telecom Single Market (TSM) and EU rules on net neutrality. In other countries, it is unclear that the provision of zero-rated services complies with the general regulatory framework for electronic services, and yet their provision is tolerated. There are countries where zero-rating is permitted but no operator has provided consumer offerings, such as in Estonia and Finland.

Zero-rating offerings face increasing regulatory scrutiny. In 2018, regulators in Portugal and Sweden stipulated that operators must comply with roaming rules, with the rationale that they

Table 18: Selected national regulatory approaches to net neutrality, 2018 (continued)

Rationale	Observations
SWITZERLAND - Code of conduct on net neutrality, 2014	
The code was created by Swisscom, Sunrise, UPC Cablecom, Orange and the cable network companies' association Swisscable. They also established an ombudsman's office which engages independent experts in specific cases. The code states that network management for the purposes of ensuring quality and provision of services tailored to end-users may continue – for example, when official rulings have to be put into effect, harmful activity blocked or capacity bottlenecks bypassed. In addition, time-critical services may be prioritized, if customers so wish. This includes, for example, IP telephony, television, emergency calls, video conferencing and future telemedicine applications, in which data have to reach customers as quickly as possible. (Source: Swisscom)	The model has drawn little criticism; the Swiss model is seen as a workable and light-weight regulatory arrangement.
Where it is suspected that a service provider is in breach of the code of conduct, users will in future be able to call on the ombudsman's office, which will draw on the expertise of independent consultants in examining the case.	
DENMARK - Voluntary net neutrality principles, 2011	
The principles were drafted by a group of Danish industry representatives and government regulators forming a private body called the Net Neutrality Forum. The group meets on an ad hoc basis to adjudicate any conflicts with their principles that do arise. To date, there has been only one issue concerning a surcharge for WhatsApp access; the body advised against the practice, and the industry participants voluntarily obliged. As a result, Denmark's voluntary net neutrality system sparked a revolution in mobile-app development in the country. (Source: Reason.com; Publicnow)	The model has drawn little criticism; the Danish model is widely viewed as a workable and light-weight regulatory arrangement.
NORWAY - Net neutrality provisions in the Norwegian electronic communications adopted by the national parliament, 2017	
Norwegian Communications Authority (Nkom) launched national guidelines for net neutrality in February 2009, based on a common understanding among stakeholders in the industry. A major difference is that the voluntary agreement is replaced by a binding law.	The 2018 annual report on net neutrality from the Norwegian Communications Authority (Nkom) concludes that, in general, the state of net neutrality in the Norwegian market seems to be relatively good. Nkom also has critical comments regarding a few conditions.
The bill Proposition states that "Safeguarding net neutrality is essential in order to ensure good, future-oriented electronic communications services for users throughout Norway and foster industrial development and innovation, and is a prerequisite for further economic, social, cultural and democratic development in modern society. The goal of the work on net neutrality is to ensure that the Internet remains a well-functioning, open and non-discriminatory platform for all types of communication and distribution of content." (Source: Nkom, Norway)	Nkom's data collection from ISPs shows no significant changes in traffic management practices compared to last year. It was noted, however, that the information by providers vary by its clarity and level of detail. Under a de facto self-regulatory scheme, it is up to service providers to self-report on their practices, without routine checks.
CHILE - Net neutrality is covered in the General Law of Telecommunications, since 2010	
The National Congress of Chile amended the country's telecommunication law in order to preserve network neutrality, becoming the first country in the world to do so. Three articles were added: forbidding ISPs from arbitrarily blocking, interfering with, discriminating, hindering or restricting an Internet user's right to use, send, receive or offer any legal content, application, service or any other type of legal activity or use through the Internet. To that effect, ISPs must offer Internet access where content is not arbitrarily treated differently based on its source or ownership. (Source:)[95]	

Source: Various, as detailed in footnotes

must allow their customers to continue to benefit from zero-rated services while traveling in Europe. The roam-like-at-home principle applies to all zero-rated content. Operators can set fair use limits, as they can for open data bundles.[100] Similar requirements may also follow for quality of service, the choice of free applications and,

> **Box 17: What are zero-rated services?**
>
> Broadly speaking, in **zero-rated offerings** mobile network operators do not charge for data used on certain applications or services. In the majority of cases, ahead of educational apps and national news outlets, digital platforms form the core of the deal and the top three global sites are Facebook, Google and YouTube. In some countries, such offers have been commercialized under the misleading branding of 'Internet basics'.
>
> Zero-rated services **are**:
>
> • As the name suggests, they are advertised as 'free of charge' although mobile Internet users typically have a mobile subscription with a data cap, for which they pay monthly or on a pay-as-you-go basis. Users of zero-rated offers are not charged for surfing over a selection of digital platforms pre-defined by the operator.
>
> Zero-rated services **aren't**:
>
> • Free, as users are making an implicit agreement to provide personal information in exchange for use of the sites.[96] This valuable personal data[97] is generating revenues for the site's owners through targeted digital advertising.
>
> Source: ITU

importantly in EU countries, the use of personal data for commercial by-products.

In developing and low-income countries in particular, regulators are increasingly evaluating the social impact of zero-rated services. Recent studies have found that zero-rating is one of many cost saving strategies. However, it is not actually helping to bring people online – so the benefits seem low, while the risk of creating an anti-competitive environment is high.[101] A holistic view of policy and regulation and a social focus is likely to lead to a new approach to zero-rated services in the coming years.

There are other services and content that can be leveraged through zero-rated schemes. In Argentina, the government is studying the introduction of zero-rated e-government services.[102] In Oman, Omantel has started offering free and unlimited Internet access to educational websites,[103] effectively a zero-rated scheme for educational content. Such pioneering experiences open a new perspective and can lead to models which help connect people at the bottom of the pyramid to key government services.

Zero-rated service offers and their regulatory treatment are an extension of the issue of end-

user sharing and user-generated content. Their impact on the market and society have generated significant debate in some countries (India, Myanmar and Togo) while seeing swift acceptance in other countries and regions (Guatemala, Eastern Europe).

Adapting regulation to safeguard privacy and consumer protection

As the world goes digital, our identities, opinions and behaviours spill over into the online world. Aspects of our lives are transformed into terabytes of data and flow over digital highways. Some aspects are meant to be public while others should remain confidential; others fall in between because of a misconception or a breach of privacy. Protecting consumers while navigating the rough seas of digital privacy is about protecting personal data, safeguarding users' right to remain anonymous and having the ability to erase their digital blueprint.

The observation that 'privacy is a complex issue' is an understatement. At the individual level, privacy is complex: it is often defined by upbringing and cultural context, and individuals vary in their personal preferences. Privacy for social media

is complex because many individuals volunteer personal information and time (implying consent), and post information in exchange for services which benefits them. Many social media services offer different 'privacy settings', implying users have a degree of choice, consent and control – which may or may not exist. Some services are now large digital players, with massive market capitalizations built on their ability to harvest and reuse data.

At the social level, privacy represents a trade-off between the individual's right to control his/her personal data with the public's or employer's right to access and distribute information. This is relevant for example, when a worker's integrity is called into question, or when an individual runs for public office – when voters may be asked to assess the suitability of candidates. Add in the technological dimension – (i) rapid innovation; (ii) instantaneous dissemination; (iii) new and combined sources of data; (iv) multiple and/or back-up storage (making it unclear or impossible that data can be definitively deleted or erased); and (v) the global accessibility of these services over the Internet – and it is easy to see how complicated the picture has become.

From a regulatory perspective, privacy is even more complex. It has become urgent and essential to forge a framework able to deal with this complexity and providing protection of consumers' personal digital data while facilitating cross-border data flows, new forms of trade and new digital services right across the economic canvas.

Alarmingly, personal data for millions of people have been shared, breached and leaked – accessed legally, accidentally, or illegally — including some cases where the individuals' data owners have been unaware of any breach for some time. Even where individuals have given agreement, data can be subverted or used for purposes other than those stated – including psychological and personality profiling surveys, for example, used for targeted commercial or political advertising campaigns.

Putting consumer choice first complicates the job further – regulators have to find a balance between protecting consumers and fostering

---

Box 18: Privacy has been called a 'fundamental right, deserving of protection'

See, for example:

(a) Universal Declaration of Human Rights, Article 12 (United Nations, 1948)

(b) Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (European Court of Human Rights, 1950)104

(c) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108 (Council of Europe, 1981)105

(d) International Covenant on Civil and Political Rights (UN, 1966)106

(e) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), effective May 25, 2018.

(f) European Court of Justice Judgment 13 May 2014[107] found that certain users have the right to ask search engines like Google to remove results for queries that include the person's name. To qualify, the results shown would need to be inadequate, irrelevant, no longer relevant, or excessive.

Source: World Bank, Data-Driven Development, 2018

Figure 56: Who sees what online?

	Personal Information	Devices	Browsing	Location	Purchases
Google	✓	✓	✓	✓	✓
Facebook	✓	✓	✓	✓	
Amazon	✓	✓	✓		✓
Verizon	✓	✓	✓	✓	
Yahoo	✓	✓	✓		
AOL	✓	✓	✓		
Comcast	✓	✓	✓		
AT&T	✓	✓	✓	✓	
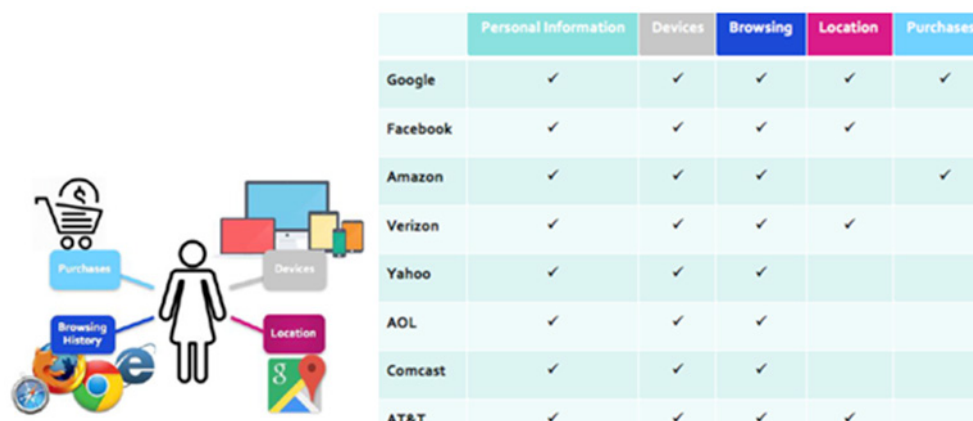
Source: Enders Analysis

innovation and competition. The impossibility of final, definitive deletion of data, coupled with changes in culture, arguably new attitudes to privacy on the part of the 'Millennials' have culminated in claims like Mark Zuckerberg's when he referred to the 'death of privacy'. The regulation of personal data flows, aimed at preserving privacy, may take place at the:

1) National level – e.g. with the introduction or change of national law over a certain country.

2) Regional level – such as the European General Data Protection Regulation (GDPR).

3) International level – governed by bilateral or multilateral trade agreements. It is a generally held principle of regulating cross-border data flows that countries should only transfer data to countries with similar level of protections to avoid the 'weak link in the chain' scenario.

These initiatives are expressed either as *positive* (e.g. trade agreements) to promote or regulate data flows, or as *negative* (e.g. data localization requirements) to restrict or limit data flows.

Protecting personal data: changing regulatory paradigm

The Internet, comprising thousands of smaller networks connected together, is global – users in countries from Argentina to Zimbabwe can access different content, applications and services. In some respects, the main barriers to accessing content may be linguistic,[108] rather than national borders. Companies and small- and medium-sized enterprises (SMEs) in developing countries can benefit from free online tools and global platforms to access information, sell services and increase their visibility.[109] The availability, sheer size and diversity of content accessible over the Internet is its incredible attraction and opportunity, but also creates risks when talking about privacy and personal data protection.

It is becoming increasingly hard to protect consumer data, due to:

- Many **consumers volunteer data** freely and willingly, even without incentives to do so.

- **New services and providers** – online platforms are proving ever-innovative and inventive in finding new uses for old data. The breadth and depth of data collected and obtained by online platforms vary (see Figure 56).

- **Questions surrounding data ownership and lack of erasure**. Early on, the data policies and Privacy Agreements of early social media services often spelt out explicitly that data ownership belonged to service providers.[110] Now, it can be difficult to find the term 'data ownership' in a Privacy Agreement. Instead, some of these user agreements skip the ownership issue altogether and instead mostly describe data use.

- **The new range of data sources**. The mobile phone is now one of the most powerful tracking devices invented in history. Mobile phones now generate substantial data trails about location (via triangulation), activity,

speed of displacement, call history, network of contacts, browsing history and can be equipped to provide biometric data and mood data (e.g. through social media posts as well). Mobile phones open the door to location and information portals – a powerful combination.

- **Difficulties in erasing data trails** – including the 'right to forget'.

Collecting data can be a very expensive activity, depending on the type of data. The argument of 'public good' is often used to justify access to and use of large datasets. When an NHS hospital in the UK provided the electronic health records of 1.6 million Britons over five years to Google's DeepMind, it did so with a view to helping analyse and improve treatment of kidney disease. This action was subsequently determined to be 'legally inappropriate',[111] but the intention at least appeared morally defensible. AI companies argue that, in order to realize the benefits of these technologies for diagnosis and treatment, the larger and better the datasets they can have access to, the sooner and better the AI technologies will become.

All of these questions have multiple and potentially conflicting answers depending on the context, legal system and perspective. For regulators, forging legal privacy norms might feel like building the Tower of Babel. For consumers, navigating through privacy settings of digital platforms and making sense of the options at hand might seem a complex labyrinth with no exit. Indeed, for a large majority of digital platform services, agreeing to the providers' terms and conditions is the *sine qua non* condition for accessing their services. Fine-tuning privacy settings does provide a level of flexibility; fundamentally, however, it is the provider of digital services who defines the rules, creating a *de facto* imbalance between the guaranteed rights and the aspirations of consumers. The protection of the rights of consumers in this setting can only have relative effectiveness and leaves regulators with fewer options.

Currently, the best practice for privacy should be consent-based and implies that an 'opt-in' should be the initial default setting, and consumers should actively choose to opt out. Data portability is another important right that needs to be guaranteed by a greater number of digital service providers. However, it is unclear whether this is in fact the setting for many online services.

There are, nevertheless, dissenting few voices who believe that the current consent-based framework might be flawed. On one hand, the developments of AI and big data render the requirements of informed consent and purpose limitation debatable and a consent-based approach is not scalable in the digital age where each user maintains numerous accounts online. On the other hand, the consent-based framework fails to address fundamental risks to the privacy rights of users. The main argument here is that privacy should not be considered as having a transactional nature, in the sense that we can trade some aspects of our privacy – for example, free e-mail or free webhosting.

Instead, any threat to privacy can be perceived as a collective problem, where individual choices worsen the condition of the group as a whole. Through this lens, the notion of consent may even become irrelevant when discussing how privacy can be protected. Along these lines, it can be argued that privacy, like environmental regulation, should not be a matter of bilateral bargaining.[112] Such an approach, however, could undermine many of the currently envisioned approaches and applied uses of big data, unless the technical solution adopted guarantees elements of privacy.

Personal data or personally identifiable information (PII) or data relates to an individual and is generally concerned with private information. Personal data can form large, complex datasets in relation to several areas – health, government, Internet activities and interests, data generated by mobile phones, financial information or other. In the eyes of consumers, there are different levels of confidentiality for many of these areas – for example, many people might regard health and financial information as especially sensitive and worthy of greater protection. However, many consumers are freely volunteering information about their lifestyles, consumption patterns, religious and political beliefs or sexual preferences via social media.

Irreversibly and effectively anonymized data is not 'personal data' and data protection principles do not have to be complied with in respect of such data. However, pseudonymized data remains personal data,[113] and is subject to data protection

Box 19 : Short lexicon of data protection

Anonymized data – Data anonymization is a type of information sanitization, usually when the intent is privacy protection. It describes the process of either encrypting or removing personally identifiable information from datasets, so the data subjects whom the data describe cannot be identified.

Anonymous data – data that cannot be traced or tracked back to any single individual.

Computer security – if the system always stays in states that are allowed, and users can only perform actions that are allowed, the system is secure.

Consent – consumer permission and approval are granted; the consumer agrees to the terms and conditions of service.

Data/information privacy – the ability an organization or individual has to determine what data in a computer system can be shared with (specified/authorized) third parties.

Direct identifiers – these include the data subject's name, face or image.

Identifiable – when, although the person has not been identified yet, it is possible to do it.

Identified – a natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group.

Identifiers – pieces of information which are closely connected with a particular individual, which could be used to single them out. This does not have to be a name – police use fingerprints, and a retinal scan can also uniquely identify an individual, given its unique nature.

Indirect identifiers – can include phone numbers, e-mail addresses or unique identifiers assigned to data subjects by the data controller (removing direct identifiers does not make datasets anonymous).

Non-secure – describes whether (and when) a computer system can enter a disallowed state, or if a user can successfully execute a disallowed action.

Privacy – the ability to control and restrict information about you, in terms of who can access which data, and when, to certain authorized parties (e.g. via privacy settings).

Personal data (sometimes called personally identifiable data): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (EU GDPR)

Privacy-by-design – setting out to build privacy and data security into the system, hardware and software by default, usually from the beginning, instead of only being tacked on or implemented later.

Privacy settings – users may have some control over whether to use an application or not as well adjusting privacy settings within applications, but sometimes these configurations can be complicated or unwittingly bypassed (Greenfield, 2012).

Pseudonymized data – pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Security – the protection of computer systems and information from harm, theft, and unauthorized use (Britannica), as well as disruption or misdirection. *In contrast to privacy (controlling or limiting access to authorized access), security is often used to describe the prevention of access by clearly unauthorized parties.*

Sensitive personal data – relates to specific categories of data, such as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. Individuals may have additional rights in relation to the processing of any such data.

Safety – free from danger.

Source: Various

legislation in Europe. This is an important point as it highlights that methods exist to reverse anonymization and what is anonymized data today (and therefore not personal data) may be pseudonymized and become personal data tomorrow.

Personal data may be **willingly exchanged**, in return for convenience (e.g. a phone number or e-mail address) but it can also be **given away unwittingly** (e.g. date of birth provided to enter an online competition) or **unwillingly** (e.g. data hacked from a personal e-mail account). They may

also be exchanged over time – e.g. you may have given away data years ago, that may suddenly resurface.

The consequences of a loss of personal data can include:

- A **loss of privacy**: people may have access to your data without your consent.

- A **loss of control** over future use(s) of personal data.

- **Loss of agency** – for instance, being exposed to a more limited range of news sources or opinions as a result of previous expressed preferences.

The loss of personal data of any form requires a regulatory response. At the individual level, consumer protection and redress still remain limited. Government-led court filings account for the majority of regulatory enforcement action in this area to date, with class actions and individual complaints failing to become mainstream. Different mechanisms may be needed to address individual consumer cases where the hardship and cost of the proceedings do not work as a barrier for accessing the protection of personal data.

Persistence, repurposing and spillovers from big data increase the risk and uncertainty about how private data can be used in the future.[114] Indeed, users may effectively be unable to control consent over the future uses of personal data. For example, in 2015, the fine detail of a 'Privacy Agreement' of a well-known European family tree website authorized the transfer and storage of biological samples in the United States, where samples would continue to be stored for an unspecified length of time.

What regulatory framework for data privacy?

A sizeable minority of countries worldwide have no specific, modern legal instrument in place for data protection. While some countries have no legislation at all, others only have sector-specific legislation, but no economy-wide data protection regulations such as the EU GDPR, which applies both horizontally and vertically.

A number of countries have nevertheless clearly defined personal data protection laws (Figure

57). According to ITU data, 109 countries have legislation that secures either the protection of data or privacy, or both. This is up from 83 countries in 2015, indicative of a clear trend worldwide. Various national efforts are underway and draft legislation is under discussion in around 10 per cent of countries according to UNCTAD,[115] including India, Pakistan and Thailand.

The US National Telecommunications and Information Administration (NTIA) has launched a consultation on how to achieve proposed consumer-privacy outcomes and high-level goals for federal action on consumer privacy, as part of an inter-agency effort led by the US National Economic Council.[116] Similarly, TRAI has released Recommendations on privacy, security and ownership of the data in the telecom sector.[117] Brazil enacted a law for the protection of personal data in August 2018; it will however be applicable starting from 2020.[118] What's more, 56 countries including Argentina, Korea (Rep.), Russian Federation, Switzerland and Timor-Leste, are the sponsors of a revised draft of the resolution of the United Nations' General Assembly entitled "The Right to Privacy in the Digital Age"[119].

The approaches chosen by regulators vary in scope and perspective. Some countries, such as Morocco, see data protection as an extension of consumer protection and take a consumer-centred approach. On the other hand, recognizing that personal data is not only an issue of privacy, security and trust, Australia regulates the use of personal data based on the basis of anti-trust and competition. This legislation aims to give consumers control over their own data, ensuring security and privacy while promoting competition and new opportunities for businesses to grow.[120]

Who is in charge of data protection?

Historically, **national data protection authorities** have monitored issues relating to privacy and regulated the use of data through privacy, data protection laws, cybercrime legislation, rules pertaining to privacy and sharing of specific types of data (e.g. health or financial data), and now rules about electronic transactions.[121] Currently, over 70 countries have established a separate data protection regulator (see Figure 58). In some countries, mainly federal states, there are multiple data protection bodies, often with a limited geographic jurisdiction. Globally, there is

Figure 57: Data protection and online privacy legislation, by region, 2017
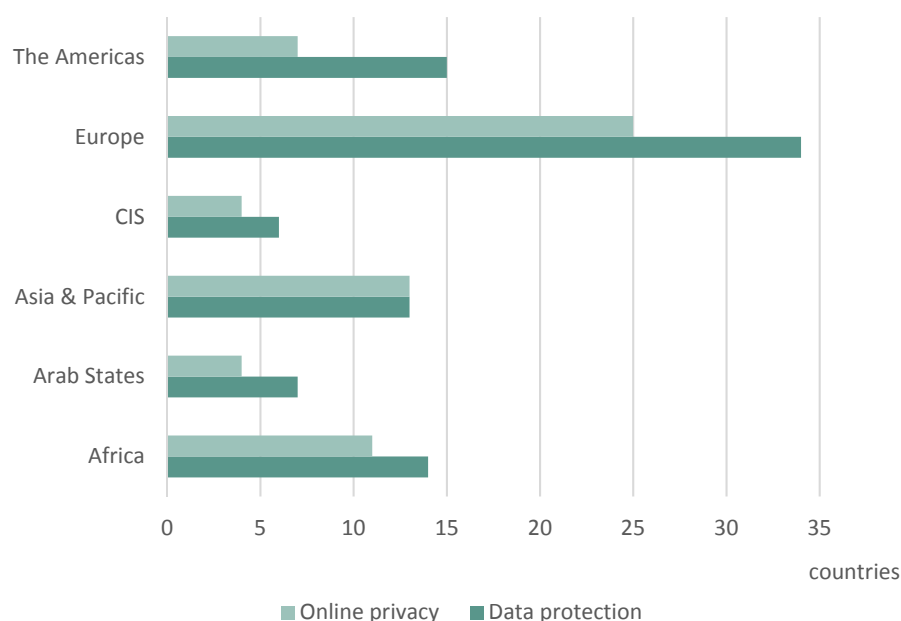
Source: ITU

a strong global trend towards the establishment of special data protection authorities with strong enforcement powers.[122]

Data regulators have sought to protect consumers by defining and enforcing rules around the use of their data. The role of data protection agencies has included some/all of the following functions:

- Regulating data protection across different industries and sectors;

- Cooperating across regulatory areas such as data protection authorities, consumer protection agencies, competition authorities, antitrust bodies and telecom/ICT regulators;

- Raising consumer awareness on data protection, privacy and security rules and regulations in place. Inform consumers of their rights;

- Aiding the private sector in regulatory efforts e.g. through co-regulation or self-regulation;

- Conducting privacy impact assessments (PIAs) when developing rules and regulations;

- Facilitating the creation and adoption of industry and sector-specific standards for data protection;

- Enforcing and upholding individual data protection rights.

In over 60 countries where no separate data protection authority exists but an ICT regulator does, the latter has been given a broad mandate to deal with online data protection (see Figure 58). Among them, Kuwait, Rwanda and Saint Kitts and Nevis. Overall however, it is not clear if many or all of these regulators have been actively involved in data protection enforcement activities.

In either institutional set-up, lead regulators increasingly need a strong, multi-sector team to support them in monitoring and enforcing data protection rules. Interestingly, in a tenth of countries worldwide both the data protection regulator and the ICT regulator have a mandate in those fields. Section 5.4 looks more closely at the collaboration among regulators in the field of data protection.

In addition, new players are now key stakeholders in debates over privacy:

- **Companies** may offer products that provide data security, stronger data protection or information about personal data that is collected.[123]

1. **Obtain and process information fairly** – most notably, including the consent of the data subject (person to whom the data relates) and the right to rectify their data if inaccurate or processed unfairly.

2. **Keep it only for one or more specified, explicit and lawful purposes** – most notably, informing data subjects of the uses to which it is intended to put the data not repurposing existing data or using it for purposes other than those specified.

3. **Use and disclose it only in ways compatible with these purposes** – Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. Also, any processing of personal data by a data processor on your behalf must also be undertaken in compliance with this.

4. **Keep data safe and secure** – appropriate security measures must be taken against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

5. **Keep data accurate, complete and up-to-date** – there is a risk that decisions or actions may be taken, based on inaccurate data. Consequently, data controllers and processors may have a duty of care to ensure that data are accurate, complete and up-to-date through e.g. appropriate cross-checking.

6. **Ensure that data is adequate, relevant and not excessive** – in general data controllers should seek and retain only the minimum amount of personal data needed to achieve their purpose(s). Asking about people's political views in a health survey is clearly not appropriate.

7. **Retain it for no longer than is necessary for the purpose or purposes** – personal data should be held for the minimum period necessary and if collected for one purpose, cannot be retained once that initial purpose has ceased (*to note that this is somewhat at odds with the inability of the digital environment to forget*!)

8. **Give a copy of his/her personal data to an individual, on request** – data subjects should have the freedom to request a copy.

Source: Irish Commission for Data Protection

- **Other organizations** can offer guidance and advice about protecting personal data – data protection agencies usually offer guidance, as well as Citizens Advice, Freedom House or online websites.

- However, **individuals** make the decision to provide personal data in exchange for use of many services. It emerges that many consumers may be choosing to sacrifice privacy in the name of 'consumer choice' or for real or perceived benefits (e.g. more targeted advertising).

New rights – a call for a harmonization of national regulatory response

New concepts are emerging, such as the 'right to be forgotten' (which is explicitly included in the EU's new GDPR[124]), the 'right to be anonymous' online or the 'right to disconnect'.[125] With such concepts, important new questions are emerging:

- Do people know what data they are providing when, under which conditions, and at what cost?

Figure 58: Who is in charge of data protection?, worldwide, 2017
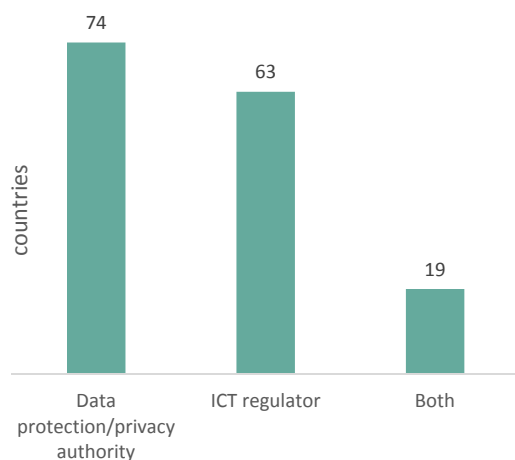
Source: ITU

- Do people understand the value of benefits they may receive in exchange?

- Are people able to value the data they provide in a manner that reflects an accurate evaluation of the benefits that they receive?

- And how can we ensure that maximum benefit is derived and delivered?

From a regulatory perspective, defending the right to privacy of people who have consciously chosen a 'public' privacy pattern becomes problematic. This is the case of virtually over a billion people active on social media digital platforms. Normalizing the rights and obligations of users and providers of digital services becomes challenging as does enforcement: there are no clear boundaries between what is good and what is not in the area of privacy when multiple factors are mixed into the context – time, stakeholder group and national context.

From a regulatory perspective, those questions remain unanswered because jurisdictions may diverge on legal instruments for enforcement of data protection and privacy rules. The global debate is certainly helpful in clarifying common values and building loose consensus around them; a full-fledged cross-border legal and regulatory framework to address them, however, does not yet exist. Some people suggest that GDPR will be the global launch pad for such a framework (see next section). Without nearly-global reach, however, enforcing such a framework might be difficult.

But while countries adopt different types of legislation, most data protection regimes build on a set of core principles, which date back to the OECD guidelines from 1980. UNCTAD has identified eight core principles, which can be found in some form or other in local and regional agreements and guidelines (see Table 19).[126]

As suggested by the UN Special Rapporteur on the right to privacy in his recent report to the UN General Assembly "[...] commitment to one right should not detract from the importance and protection of another right. Taking rights in conjunction wherever possible is healthier than taking rights in opposition to each other."[127]

In terms of regional efforts, the Council of Europe's Convention 108 was one of the first data protection initiatives, providing a treaty which opened for ratifications in 1981 (COE, 1981). More recent widely cited frameworks to define the rules around the privacy of personal data include:

- OECD's Privacy Guidelines (OECD, 2013)

Table 19: Core data protection principles

1. Openness: Organizations must be open about their personal data practices.	**5. Security:** Personal data must be subject to appropriate security safeguards.
2. Collection limitation: Collection of personal data must be limited, lawful and fair, usually with knowledge and/ or consent.	**6. Data quality:** Personal data must be relevant, accurate and up-to-date.
3. Purpose specification: The purpose of collection and disclosure must be specified at the time of collection.	**7. Access and correction:** Data subjects must have appropriate rights to access and correct their personal data.
4. Use limitation: Use or disclosure must be limited to specific purposes or closely related purposes.	**8. Accountability:** Data controllers must take responsibility for ensuring compliance with the data protection principles.

Source: UNCTAD

- APEC Privacy Framework (APEC, 2015)

- European General Data Protection Regulation (GDPR –EU, 2018)

Spotlight on GDPR

The European Union's General Data Protection Regulation (GDPR), under negotiation since 2012, was published on 27 April 2016 and came into force on 25 May 2018. GDPR offers explicit criteria, rules and enforcement action for those organizations that have transgressed.

Significantly, the GDPR places restrictions on cross-border data transfers, guaranteeing that data is not exported from the EU without the adoption of safeguards.[128] The reach of the GDPR extends to companies controlling or processing personal data of EU citizens in any country, giving it broad applicability to providers outside the EU.

The GDPR built on previous instruments, including Directive 95/46/EC (General Data Protection Regulation) and EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data". The new regulation and old directive share much of their content and principles. Indeed, the GDPR recognizes in paragraph 9 that "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity."

However, the EU GDPR is stricter, fining companies up to 4 per cent of global revenue or EUR20 million (whichever is greater), and increasing the legal requirements and accountability for data controllers and data processors. The EU GDPR also regulates the data controller across several aspects – compliance with individual rights, guaranteeing adequate data security based on a risk assessment, obligation to conduct Data Protection Impact Assessments (DPIAs), keeping of records on processing, notification of authorities and data subjects in the event of a data breach, and appointment of a data protection officer if necessary. The GDPR contains an accountability

requirement, where a controller and processor must also be able to demonstrate compliance with GDPR requirements by providing adequate documentation upon request by supervising authorities.

African Union Convention on Cybersecurity and Personal Data Protection

The African Union Convention on Cybersecurity and Personal Data Protection (2014) stresses that data can only be processed for legitimate purposes, but fails to define the term 'legitimate'. The AU Convention identifies many of the principles around which GDPR was built. The Convention has not yet come into force and awaits ratification by 15 countries.[129] To facilitate the implementation of the Convention, the African Union Commission and the Internet Society developed Guidelines on Privacy and Personal Data Protection for Africa in May 2018 containing some 18 recommendations.[130]

Regulation of cross-border data flows

Data is now recognized as a valuable resource or asset. However, it is unclear that the logic of the benefits to free trade applies to data flows. Many trade agreements dictate special treatment for data relating to individuals. Further, recent data leaks highlight an obvious risk – once individual data owners or producers part with data, they no longer exert any control over those data.

Governments are increasingly intervening in language relating to data flows in multilateral, bilateral or preferential trade agreements (PTAs). It is important to note here that those flows can carry personal and non-personal data. The Trans-Pacific Partnership (TPP), signed in 2016, but never submitted for a Congressional vote was an early trade agreement to include rules on digital issues – privacy, consumer protection, cross-border data transfers, net neutrality, competition policy and intellectual property (IP).

In September 2018, a new US-MCA trade deal was agreed, replacing the North America Free Trade Agreement (NAFTA). The text inherited some of the language from the TPP, but included new

Box 21: The growing use of digital trade in Preferential Trade Agreements (PTAs)

In terms of the history of e-commerce and digital trade, the first e-commerce provision was made in the Jordan-US Free Trade Agreement (FTA), valid on 24 October 2000. The first chapter was present in the Singapore-Australia Agreement (SAFTA) in February 2003, with the first general provisions on data flows found in the Korean-US Trade Agreement (2007). By September 2018, there are currently:

- 98 PTAs with e-commerce/digital trade provisions;
- 73 with e-commerce/digital trade chapters;
- 13 with data flow provisions;
- 64 PTAs with specifics on financial services;
- 61 PTAs with telecoms;
- 9 PTAs with provisions on data localization.

Of treaties negotiated so far in 2018, all except one include a chapter on digital trade. The number of provisions is increasing every year, and the number of provisions made with data chapters is increasing, especially in bilateral trade agreements. With regard to privacy and data protection – not every agreement mentions privacy; 77 PTAs have provisions on privacy. On consumer issues, the wording used is generally consumer protection or consumer confidence – not every agreement that deals with electronic commerce and trade: 70 PTAs contain consumer protection (71% of all PTAs with provisions on e-commerce, digital trade and e-commerce).

Source: Dr. Rodrigo Polanco, University of Luzern (forthcoming), presentation made at the WTO, Geneva, 4 October 2018

additions. Chapter 19 covers Digital Trade and includes:

- **Online consumer protection (Art 19.17):** "The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities when they engage in digital trade".

- **Personal information protection (Art 19.8)**: Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.

- Principles on access to and use of the Internet for **digital trade** (Art 19.10).

- **Cooperation** (Art 19.14).

- **Cybersecurity** (Art 19.15).

- **Source code** (Art 19.16) – significantly, including mention of algorithms which are defined as source code (defined in the preamble).

The agreement is clearly an indication of the US's new approach to digital trade in data and is likely to have global implications and an impact on the regulatory treatment of trade in data.

Data localization measures

Many governments have plans to transform traditional economy to a digital economy, including data, but there is little clarity today about data localization measures, which promote national storage or retention of data – preventing the flow or transfer of data from within a jurisdiction.

In 2015, Russian Federation passed a data localization law, which requires data to be stored in the country, when it originates from Russian territory. The transfer of data is legal under this legislation, though only in copy form, and the 'main database' must be located in Russian Federation.[131] In June 2018, Viet Nam passed a cybersecurity

law requiring that data of all Vietnamese users be stored in Viet Nam.[132] Information stored locally must include the user's personal information, online relationships, and all other data generated by users. Further details on storing user's data and restrictions on the cross-border transfer of data are yet to be provided through decrees and circulars.

Those in favour of data localization measures see them as the exercise of national sovereignty, keeping a valuable asset within geographic borders and controlling the use of that asset, protecting consumers and data, once it has left a jurisdiction. For critics, such measures are a costly form of regulation which adds considerably to compliance and data transaction costs.[133]

Ethics

A world of ubiquitous data and smart algorithms requires ethics to protect fundamental human rights and help make decisions where law does not have clear-cut answers. When combined with digital identity systems, privacy is interacting in new ways with rights to freedom of expression, civic participation, entitlement and the exercise of rights. Ethics comes to the fore as a key consideration.

Consideration to 'data ethics' must help setting privacy norms – the UN Special Rapporteur on the right to privacy recommends that formal mechanisms be instituted "including ethics committees, with professional, community and other organizations and citizens to protect against the erosion of rights and identify sound practices."[134] Another UN document is the "Guidance Note on Big Data for the achievement of the 2030 Agenda" adopted by the UN Development Group[135] where ethics and moral obligations of handling data were addressed. The Note stresses the importance of ensuring that data ethics is included as standard procedure for data governance. For example, the World Food Programme (WFP)'s "Guide to Personal Data Protection and Privacy" considers ethics in the application of humanitarian principles and risk assessments.[136]

Ethical considerations may come to the fore when digital identity systems combine with information from personal or financial life. Gerd Gigerenzer, director of the Harding Center for Risk Literacy at the Max Planck Institute for Human Development in Berlin, has asked[137]:

• Should we score people in areas like finance, health, criminality, rental housing, mail-order businesses and so on?

• How are these scores calculated across different areas? Can they be published, revised or altered?

• Who can access such scores, and for what purposes should they be used?

• And should we allow all of the data gathered to be brought together, so we can come up with a total score for every citizen?

The COMPAS algorithm has been used in some US states to predict the likelihood of re-offense by criminal offenders. The tool helps judges with sentencing by looking at defendants' criminal histories and predicting the likelihood of reoffending. Further research however found that the algorithm committed errors in over a third of the cases and was racially-biased. Another algorithm used in a Medicaid assessment instrument was challenged in court on charges of bias for patients with diabetes.[138]

A major ethical consideration relates to whether we put the computer system in charge. For example, using artificial intelligence and algorithms as an additional tool to identify, for example, children at risk of abuse or criminals likely to reoffend may be helpful, but 'putting the algorithm in charge' and giving it responsibility for a decision is subject to debate.

Computers, machines and algorithms teach us a lot about observable behaviour (e.g. laughter, tears or shouting fits). They may also teach us about human behaviour (e.g. qualities of humour, sadness, patience or rage, and our individual propensity to each). But can they teach us about human experience – what it is like to be human, to have a cultural perspective and feelings? If it is far from clear that people are rational economic agents, what place is there for emotion, passion, loyalty or love in a society ordered by algorithms, as well as laws?

At the international level, technology must remain a tool, and not a decider, in guiding our shared

Box 22: AI and ethics admonition

AI is developing with enormous speed and is affecting many elements of human society. It is impossible to predict how AI will impact systems, infrastructures, ethical and social areas of concern to ICT policy-makers and regulators. To respond quickly and effectively to ethical and social issues that arise, and to be proactive and prudent, ICT policy-makers must remain up-to-date on AI social and ethical issues, engage in real-time and continuous multi-stakeholder and cross-institutional consultations on these issues, and maintain nimble policy mechanisms.

While there are ways that AI feels new – it is broad in scale and scope and is advancing with unprecedented speed – it nonetheless shares features encountered in the growth of mobile telephony or the Internet. As we reflect on these connections between AI's social and ethical importance and related values encountered with other ICT infrastructures, there are several ways in which AI impacts on areas already mandated to ICT policy-makers:

- The ICT sector as a target or beneficiary of AI. For example, customer data retained by mobile and Internet Service Providers can be subject to powerful de-anonymizing AI analysis increasing the import of data security and privacy among operators.

- The ICT sector as a tool for supporting the best forms of AI and responding to the worst. For example, operators may be best able to assist other stakeholders in identifying and responding to potentially harmful AIs released onto their networks.

- The ICT sector as a set of businesses directly employing AI, potentially in ways that have policy and regulatory relevance. For example, consider how much of operator customer support may move away from human agents (including offshored call offices) to AI chatbots.

While these are examples of ways AI is related to existing core ICT regulatory and policy areas, it is likely that ICT policy stakeholders will be asked to take on even more direct consideration of emerging AI issues. To respond to existing mandated areas, and be ready for increasing and new considerations, ICT policy-makers must remain informed, agile, and conversant around the various social and ethical aspects of artificial intelligence. To do so, they must engage in real-time learning and consultation among multi-stakeholder, cross-institutional coalitions.

This is already happening across some jurisdictions, among multilateral and professional societies, and within various companies.

Source: ITU, AI for Development Series, Module on AI, Ethics and Society: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2018/documents/AISeries_EthicsModule_GSR18.pdf

future. We must be guided by the universal values and norms that we have established over centuries. Ensuring human security and dignity must be our guiding principle in the space where fast-evolving technologies intersect with our peace and security.

Digital identity systems

Individuals may have multiple identities, from simple ID, login password-protected access and formal ID. Different transactions require different levels of identity. In most countries, physical birth certificates are issued to citizens as legal proof of identity.

There is a growing trend however to digital identity for e-government, financial health, commercial and business services. Governments increasingly recognize that a system of trusted digital identity is needed, and may contribute to the growth of the digital economy. Therefore, the concept of 'digital identity' comprises the set of mechanisms which assert and verify personal data in the

context of digital services, based on identification, authentication, and authorization processes. Digital identity can be classified as[139]:

- **Foundational**: A core digital identity, part of a national identity scheme, may be based on official documents such as birth records, marriage certificates, and social security documents. This may be used, for example, in accessing government services;

- **Functional**: A digital identity created to address the specific needs of an individual sector, such as health care;

- **Transactional**: A digital identity designed to ease the conduct of financial or other transactions (either face-to-face or across the Internet) across multiple sectors used for example in making purchases/transactions online but not granting legal identity.[140]

Trust remains at the core of all digital identification systems: secured connectivity and access, verification and authentication of digital identity all must underpin online transactions.

Identity can be defined by items such as names, address, age, gender, etc., or by biometric measures such as fingerprints, texture or voice, etc. A minimum set of attributes can be established for information systems. Different types of digital identity exist, for registering, enrolling, and authorizing transactions. Citizens can enroll, be authenticated and have identity validated, enabling them to carry out e-transactions remotely. Financial 'know your customer' identity is used in a growing number of countries in which mobile operators identify their customers, thus enabling digital identity systems where national registration systems are missing.

SDG Target 16.9 provides for legal identity for all people by 2030. Today, around one billion people lack legal identity, most of whom are located in Sub-Saharan Africa and South Asia.[141]

However, progress is being made, and significant advances have been achieved in data protection, security, privacy, trust. Security and trust are fundamental, as without this, citizens may be reluctant to enroll. A coordinated approach can reduce the risk of duplication, conflict rules, lack of

interoperability and security between technologies and systems.

In Denmark and Estonia, governments issue digital identities which can be used to access public services such as welfare, tax, health care, and commercial registration, while also facilitating certain private services such as online banking, pension and much more. While using different technologies to facilitate these services, the range of uses is fairly similar. India's Aadhaar system is one of the largest national identity systems, at over one billion individuals identified, and giving access to goods, services and governmental programmes for a large part of the population.[142] This makes it the world's largest biometric ID database covering welfare, tax payments and access to social services.

Ghana is working to develop a single unique national ID, the Ghanacard, as an identity card combining different applications[143] including that of a driving licence. In Oman, the government went live with a national identity system in 2013.[144] The card combines national PKI, digital identity, e-signature and registration systems. There are a range of stakeholders integrated into the system, from the mobile operators Omantel and Ooredoo, the police, TRA and the CPO.

The focus of regulation should be the person, not the data

Privacy is a complex and evolving issue – it represents many trade-offs, between the public's 'right to know' and individual's 'right to be forgotten', between an opportunity to commercialize data, and the need to protect data from inappropriate exploitation by other parties. The rise of global online data players with massive market capitalization based, in significant part, on their ability to harvest, farm and use data in multiple ways has complicated this picture.

A huge, invisible trade in data is developing, based on the collection, aggregation, transfer, storage and analysis of data relating to billions of individuals. The quantity, amount, type and variety of data is multiplying rapidly, enabling enhanced analysis and prediction of patterns in correlated or seemingly uncorrelated datasets.

The regulation of data flows can take place at the national level, regional or international level,

mainly through bilateral or multilateral trade agreements. When combined with digital identity systems and identification techniques, ethical considerations are increasingly coming to the fore. Can we rate people across different areas of their lives? Can these rating scores be published, revised or altered? Who can access them, and for what purposes should they be used? In our future hyperconnected world, the openness, transparency and accountability of extensive digital identity systems must be examined.

Taxation in the digital ecosystem

The issue of taxation of digital services and content remains 'work in progress'. While digital transformation is improving productivity, employment and competition worldwide, taxation could damage or enhance these benefits. Much depends on the way governments address these policies and strategies. Adding further complexity, the number of taxation options is growing – but it remains unclear as to how these taxation approaches can work with respect to digital services and digital platforms, including OTTs.[145]

According to an ITU GSR-16 Discussion Paper, the taxation of digital services raises essential questions: Should governments, for example, tax mobile services and broadband services? Will a higher tax burden mean lower mobile adoption and hamper economic growth? Two opposing trends can be detected in terms of digital taxation policy:

• Those in favour of taxation – with the aim of maximizing tax collection;

• Those who oppose taxation – with the view that lower taxation benefits consumers, businesses and economic growth.

From a pro-taxation perspective, governments recognize that digitalization is critical in their generation of revenues and are putting mechanisms in place to maximize tax collection. From an anti-taxation perspective, some countries regard lower taxes as generating spillovers that are larger than the foregone taxes. Figure 59 presents the case of reduced taxes on broadband and the virtuous circle that is created.

Reduced taxes on telecommunication/ICT services and devices can positively impact adoption and usage, which in turn means an increase in ICT penetration as a result of demand elasticities. This penetration increase can enhance the return on

Figure 59: Virtuous circle of tax reduction on broadband equipment and services
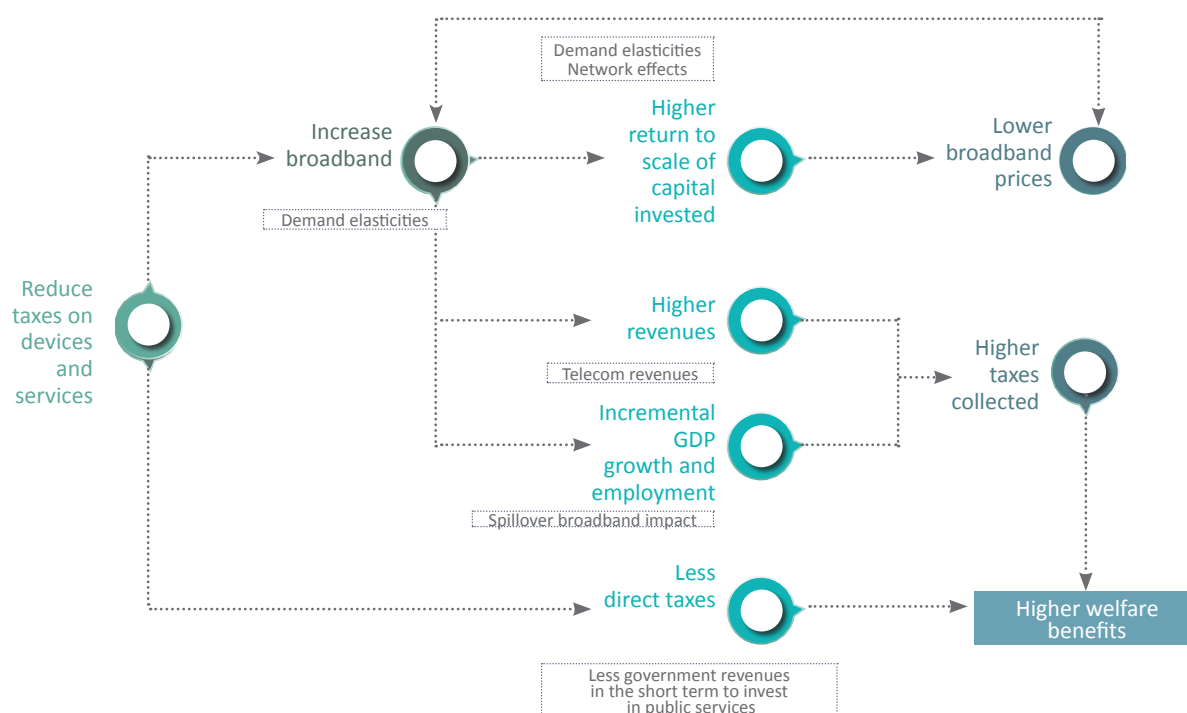
Source: ITU GSR-16 Discussion Paper, *The impact of taxation on the digital economy*

the network capital invested. A higher return on capital allows operators and service providers to reduce prices, which in turn has a positive impact on penetration. This will also enable operators to invest in infrastructure development. As noted in Chapter 1, an increase in broadband penetration has direct and indirect effects:

- **Direct**: it means an improvement in operators' revenues.

- **Indirect**: it enhances the contribution of broadband services to economic growth and employment.

Both effects increase the taxable base, which in turn grows the collected taxes beyond the amount foregone by reducing taxes on telecommunication/ICT services and devices. This effect could yield more affordable broadband services for all, which translates into higher welfare benefits.[147]

Regional differences

Countries clearly do not follow a uniform approach for taxation of digital services. The type of taxes applied and their amount vary significantly – as a result, service costs vary, as do prices paid by consumers.

The value-added taxes (VAT) category in which telecommunication/ICT services are taxed varies across the regions (see Figure 60).

The good news is that telecommunication/ICT services are no longer considered as 'luxury goods'. However, some countries still impose a high rate of tax – five countries for fixed services and four countries for mobile services.

Table 20 compiles the type of taxes that countries are applying to telecommunication/ICT services grouped by region and describing the rank of taxes. In all regions, many countries are applying sector-specific taxes, at high rates. For example, Sri Lanka applies 49.77 per cent for international mobile roaming, national voice services and pre-paid mobile cards. VAT remains constant for different services, only varying the percentage applied in each region. Sales taxes are however very elevated, especially in the Americas, where some countries are not taxing VAT but applying sales taxes ranging from 3.65 to 25 per cent.

Countries can place a variety of taxes on telecommunication/ICT, including:

- Value added taxes (VAT) on ICT goods

- Sales taxes

- Corporate taxes on profits

- Property taxes – based on physical assets

- Specific spectrum or licence fee taxes

- Customs taxes on the import of devices or telecommunication equipment - import duties (on equipment and/or handsets)

- Content taxes

- Sector-specific taxes

Some of these taxes (e.g. property taxes) are also levied on digital service providers on the physical assets they own in a specific country, as well as digital service and content taxes. Figure

Figure 60: Category of value-added tax (VAT) where telecommunication/ICT services are classified
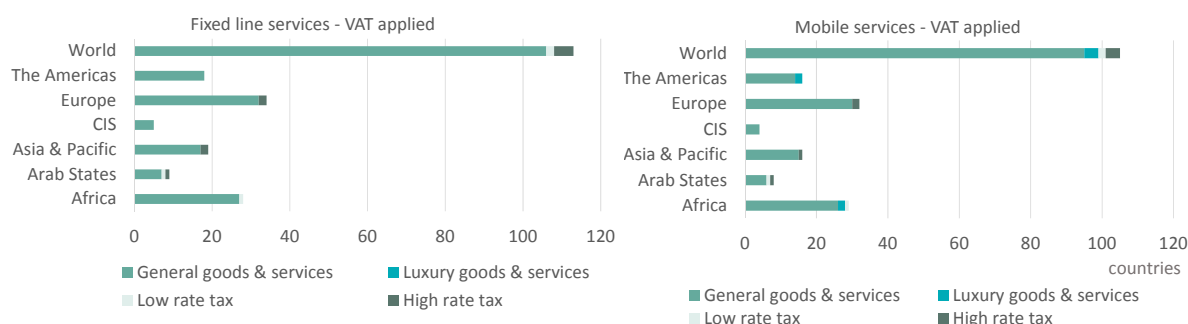
Source: ITU Tariff Policies Survey, 2017[146]

Figure 61: Type of taxes applied to the telecommunication/ICT sector, world percentage

Value-added taxes

No 15%
Yes 85%

119 countries

Sales taxes

No 45%
Yes 55%

106 countries

Corporate taxes

No 19%
Yes 81%

116 countries

Property taxes

No 39%
Yes 61%

100 countries

Content tax

No 50%
Yes 50%

89 countries

Sector-specific taxes

No 41%
Yes 59%

104 countries

Spectrum/license fee subject to VAT

No 58%
Yes 42%

106 countries

Import duties on equipment

No 22%
Yes 78%

108 countries

Import duties on handsets

No 24%
Yes 76%

104 countries

Source: ITU Tariff Policies Survey, 2017

61 shows the percentage of taxes applied to the telecommunication/ICT sector at world level.

The level of application of telecommunication/ICT taxes varies significantly across the world. The most widely applied taxes worldwide are VAT, corporate taxes and import duties. However, 59 per cent of countries apply sector-specific taxes (see Figure 62).

Only countries from the CIS region are not applying sector-specific taxes. A study from GSMA[148] finds that nearly 40 per cent of the tax revenues raised from the mobile sector came in the form of mobile-specific taxation. Sector-specific taxes distort the provision and consumption of services by affecting prices for consumers. This in turn can reduce the operators' investment. Furthermore, sector-specific taxation can generate competitive distortions by applying differently to providers of equivalent services. This can apply at international level, where taxes vary from one country to another, specifically for international services such

as international mobile roaming and international voice calls.

An overview of current practices and experiences in the field of taxation of telecommunication and ICT services is provided in Table 21.

Taxation of digital services

Taxation of digital services is complex: digital services and content flow across borders, with countries encountering difficulties in determining where business profits should be taxed. Data show that only 11 per cent of countries worldwide apply digital services and content taxes, including in Africa, Asia-Pacific, Europe and the Americas (see Figure 63).

Table 20: Types of taxes and range of rates applied to each service (in per cent), by region, 2017

Region	Africa	Arab States	Asia and Pacific	CIS	Europe	The Americas
National Voice Services	VAT: 26C (12% to 20%) Sector specific: 8C (2% to 17%) Sales: 2C (5% to 10%)	VAT: 2C (17%) Sector specific: 3C (1% to 10%) Sales: 1C (3.5%)	VAT: 8C (6% to 15%) Sector specific: 4C (0.5% to 49.77%) Sales: 3C (5% to 27%)	VAT: 6C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 31C (8% to 27%) Sector specific: 3C (0.1% to 15%) Import Duty: 1C (8%)	VAT: 17C (5% to 19%) Sector specific: 5C (1% to 5%) Sales: 7C (3.65% to 25%) Import Duty: 1C (15%)
National Data Services	VAT: 21C (12% to 20%) Sector specific: 7C (2% to 17%) Sales: 2C (5% to 10%)	VAT: 2C (17%) Sector specific: 3C (1% to 1.5%) Sales: 1C (3.5%)	VAT: 8C (6% to 15%) Sector specific: 4C (0.5% to 32%) Sales: 3C (5% to 27%)	VAT: 6C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 29C (8% to 27%) Sector specific: 3C (0.10% to 18%) Sales: 1C Import Duty: 1C (8%)	VAT: 15C (5% to 19%) Sector specific: 3C (1% to 5%) Sales: 6C (8% to 25%) Import Duty: 1C (15%)
International Data Services	VAT: 16C (12% to 20%) Sector specific: 6C (2% to 13%) Sales: 1C (10%) Import Duties: 1C (40.55%)	VAT: 2C (17%) Sector specific: 3C (1% to 8%) Sales: 1C (3.5%)	VAT: 6C (6% to 15%) Sector specific: 3C (0.5% to 5%) Sales: 1C (27%)	VAT: 6C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 28C (8% to 27%) Sector specific: 2C (0.10% to 4%) Sales: 1C Import Duty: 1C (8%)	VAT: 11C (5% to 19%) Sector specific: 2C (1% to 2%) Sales: 4C (4% to 25%) Import Duty: 1C (15%)
Incoming International voice services	VAT: 17C (12% to 20%) Sector specific: 8C (2% to 30%) Import Duties: 1C (40.55%)	VAT: 1C (17%) Sector specific: 3C (1.5%) Sales: 1C (3.5%)	VAT: 6C (6% to 15%) Sector specific: 4C (0.5% to 12%) Sales: 1C (27%)	VAT: 5C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 26C (8% to 27%) Sector specific: 1C (0.10%) Sales: 1C Import Duty: 1C (8%)	VAT: 12C (5% to 19%) Sector specific: 4C (1% to 2%) Sales: 5C (10% to 25%) Import Duty: 1C (15%)
Outgoing International voice services (IDD)	VAT: 21C (12% to 20%) Sector specific: 8C (2% to 17%) Sales: 2C (5% to 10%)	VAT: 2C (17%) Sector specific: 3C (1% to 10%) Sales: 1C (3.5%)	VAT: 7C (6% to 15%) Sector specific: 3C (3% to 5%) Sales: 1C (27%)	VAT: 5C (18% to 20%) Sector specific: 1C (1%) Sales: 1C (20%)	VAT: 28C (8% to 27%) Sector specific: 1C (0.10%) Sales: 1C Import Duty: 1C (8%)	VAT: 13C (5% to 19%) Sector specific: 4C (1% to 13%) Sales: 5C (10% to 25%) Import Duty: 1C (15%)
Pre-paid mobile top-up cards	VAT: 23C (12% to 20%) Sector specific: 6C (2% to 13%) Sales: 2C (5% to 10%) Import Duties: 1C (25%)	VAT: 2C (17%) Sector specific: 3C (1.5 % to 15%) Sales: 1C (3.5%)	VAT: 8C (6% to 15%) Sector specific: 4C (0.5% to 49.77%) Sales: 4C (5% to 27%)	VAT: 5C (18% to 20%) Sales: 1C (20%)	VAT: 30C (8% to 27%) Sector specific: 3C (0.10% to 12%) Sales: 1C Import Duty: 1C (8%)	VAT: 16C (5% to 19%) Sector specific: 4C (1% to 13%) Sales: 8C (3.65% to 25%) Import Duty: 1C (15%)
National Mobile Roaming	VAT: 21C (12% to 20%) Sector specific: 7C (2% to 17%)	VAT: 2C (17%) Sector specific: 3C (1% to 15%) Sales: 1C (3.5%)	VAT: 7C (6% to 15%) Sector specific: 2C (0.5% to 3%) Sales: 3C (5% to 27%)	VAT: 5C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 29C (8% to 27%) Sector specific: 3C (0.10% to 4%) Sales: 1C Import Duty: 1C (8%)	VAT: 13C (5% to 19%) Sector specific: 3C (1% to 2%) Sales: 6C (3.65% to 25%) Import Duty: 1C (15%)
International Mobile Roaming	VAT: 17C (12% to 20%) Sector specific: 6C (2% to 13%) Sales: 1C (10%)	VAT: 1C (17%) Sector specific: 4C (1% to 15%) Sales: 1C (3.5%)	VAT: 6C (6% to 15%) Sector specific: 4C (0.5% to 49.77%) Sales: 1C (27%)	VAT: 4C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 27C (8% to 27%) Sector specific: 3C (0.10% to 4%) Sales: 1C Import Duty: 1C (8%)	VAT: 12C (5% to 19%) Sector specific: 2C (1% to 2%) Sales: 5C (4% to 25%) Import Duty: 1C (15%)

Table 20: Types of taxes and range of rates applied to each service (in per cent), by region, 2017 (continued)

Region	Africa	Arab States	Asia and Pacific	CIS	Europe	The Americas
Internet Services	VAT: 20C (12% to 20%) Import Duties: 1C (40.55%) Sector specific: 6C (2% to 13%) Sales: 1C (10%)	VAT: 3C (12% to 17%) Sector specific: 2C (1% to 1.5%) Sales: 1C (3.5%)	VAT: 8C (6% to 15%) Sector specific: 2C (0.5% to 3%) Sales: 3C (5% to 27%)	VAT: 6C (18% to 20%) Sector specific: 1C (1.2%) Sales: 1C (20%)	VAT: 31C (8% to 27%) Sector specific: 3C (0.10% to 18%) Sales: 1C Import Duty: 1C (8%)	VAT: 16C (5% to 19%) Sector specific: 3C (1% to 5%) Sales: 7C (3.65% to 25%) Import Duty: 1C (15%)
Content Services	VAT: 16C (12% to 20%) Import Duties: 1C (40.55%) Sector specific: 5C (2% to 17%)	VAT: 2C (17% to 18%) Sector specific: 1C (5%) Sales: 1C (3.5%)	VAT: 9C (6% to 15%) Sector specific: 2C (0.5% to 3%)	VAT: 4C (18% to 20%)	VAT: 26C (4.5% to 27%) Sector specific: 1C (0.10%) Sales: 1C Import Duty: 1C (8%)	VAT: 10C (5% to 19%) Sector specific: 1C (1.5%) Sales: 5C (3.65% to 25%) Import Duty: 1C (15%)
OTT Content Services	VAT: 6C (12% to 18%) Sector specific: 8C (2% to 13%)	Sector specific: 1C (1.5%)	VAT: 5C (6% to 15%) Sector specific: 4C (0.5% to 3%) Sales: 1C (8%)	VAT: 4C (18% to 20%)	VAT: 21C (8% to 27%) Sales: 1C Import Duty: 1C (8%)	VAT: 5C (5% to 19%) Sales: 4C (10% to 25%) Import Duty: 1C (15%)
Data available	based on 23/44 countries' responses	based on 10/21 countries' responses	based on 11/40 countries' responses	based on 4/12 countries' responses	based on 29/41 countries' responses	based on 17/35 countries' responses

Note: 26C = 26 countries
Source: ITU Tariff Policies Survey, 2017.

Figure 62: Taxation of telecommunication/ICT services by region: Sector-specific taxes, 2017
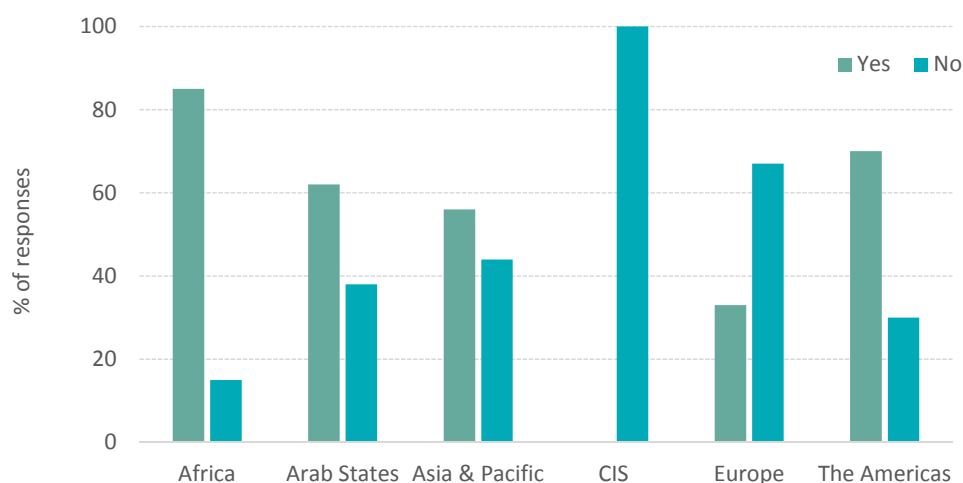
Source: ITU

While the volume of international transactions in the digital economy has grown rapidly, multinational digital businesses have sought to minimize their global tax contributions and national tax administrations have sought seeking to collect taxes – and the application of international tax rules is still not clear. The central question remains – how to establish national taxation duties in a country where a business has a digital presence only and no physical presence. Regional and international associations are working to develop new rules. In March 2018,

Table 21: Taxation of telecommunication/ICT - recent practices and initiatives

Argentina	In September 2018, Argentina's new Law 27,430 introduces a VAT applicable to the importation of 'digital services' rendered by a non-resident to a resident individual or entity when the effective use or exploitation of the service is carried out inside Argentina. The VAT of 21% must be paid at the time of the total or partial payment of the service charge. (Source: DLA Piper)
Australia	The Australian Federal Government amended its Goods and Services Tax (GST) law to ensure digital products and services receive an equivalent tax of 10%, whether they are provided by Australian or foreign entities over a threshold of AUD75,000. Australia has responded to international tax challenges in the digital economy by tackling BEPS and more recently introducing a Multinational Anti-Avoidance Law (MAAL). (Source: ITU Training on Competition analysis in the digital environment for Asia-Pacific 2018)
Belize	The Belizean Government formally applied a 12.5% general sales tax on Internet and data services as of 1 April 2018. It was outlined in the government's budget presentation for fiscal year 2018/2019. (Source: Quaderno.io)
Benin	On 20 September 2018 the Government of Benin launched a tax on social networks and Internet packages. Calling, SMS and Internet services were taxed at 5% of their pre-tax price, while a contribution of 5 CFA francs (0.8 eurocent) per megabyte is levied for access to the Internet using a bypass service or a social network platform. On 24 September 2018, the government decided to cancel these taxes. (Source: Benin local press)
Chile	If the Tax Law is approved, the tax on the digital economy will be 10% and will be charged directly through the credit cards of the users of these platforms. (Source: Quaderno.io)
Colombia	In June 2018, the Colombian Tax Authority (DIAN) published a resolution proposing a VAT collection mechanism on electronic digital services executed by foreign service providers to Colombian residents. Such services are related to: (i) audiovisual services, (ii) services through mobile app distribution platforms, (iii) online publicity services, and (iv) online training services. (Source: El Pais.com)
EU	In March 2018, the European Union proposed a digital sales tax that would require tech companies with global annual revenues of at least EUR750 million (USD868 million) and EUR50 million (USD58 million) in annual EU revenues to pay a 3% tax on revenue generated via ads, online sales, or sales of user data. The taxes would be based on revenues, and are separate from the corporate taxes tech companies already pay – which are based on net income. France and Germany are the biggest proponents of this tax. Ireland, Finland, Sweden, and the Czech Republic and other countries are opposed, arguing that the tax reform would deviate from internationally agreed upon principles. (Source: Business Insider)
France (EU)	On 21 September 2017, the decree of application to tax advertising revenues of Internet video sites/platforms was published. This taxation, which targets free or paid video platforms, will contribute to the financing of audiovisual creation. The 'YouTube tax' of 2% was passed in Parliament in December 2016, against the advice of the government. The 'Netflix tax' of 2%, which concerns video-on-demand services based abroad but operating in France, was adopted in 2014. The VAT applicable to the telecom sector is 20%. The taxation of digital services and OTTs is in discussion at European level. Lastly, telecom operators are subject to the IFER tax (flat-rate charge for network companies – Imposition forfaitaire pour les entreprises de réseaux) on relay antennas and telephone exchanges. In 2018, this tax has been extended to fibre and coaxial cable. (Source: ITU Tariff Policies Survey, 2018)
Japan	On 15 October 2018, it was announced that Japanese consumption tax of 8 percent which previously applied to digital business owners since 1 October 2015, will rise to 10 percent from October 2019. It applies to foreign businesses supplying digital services to Japanese consumers. (Source: A statement from the Japanese Prime Minister)
Jordan	On 11 September 2018, the government announced that it intends to increase the special tax on telecom services from 24% to 26%, at the same time introducing a new 1% levy on net profits dubbed the 'solidarity tax' that will be used to fund scientific research and support for the poor. This will be collected from all companies – not just telcos. Mobile services in Jordan are currently subject to a fixed 24% tax, as well as the standard 16% general sales tax, in addition to which operators also pay the equivalent of 10% of their operating revenues to the government. (Source: TeleGeography)
Kenya	On 18 October 2018, Safaricom announced it is raising the cost of its wireless and broadband services, after changes to taxes were passed through the Finance Act 2018. In particular, the Excise Duty tax applicable on voice, SMS and data services was hiked from 10% to 15%, in addition to the existing VAT of 16% applicable to mobile services. Safaricom has increased the headline price for voice calls and data by KES0.30 (USD 0.003) and SMS by KES0.10 (USD 0.009), while the firm says it has also reviewed the cost of its fibre-based broadband plans. (Source: TeleGeography). The removal of VAT on telecom devices and equipment has led to a 200% increase in device purchases and an important increase in the mobile penetration rate. (Source: ITU Regional Economic Dialogue for Africa, RED-AFR2018)

Table 21: Taxation of telecommunication/ICT - recent practices and initiatives (continued)

Republic of Korea	On 24 October 2018, the Republic of Korea's Ministry of Strategy and Finance (MOSF) released a document summarizing recent statements by senior government officials about the need to introduce a digital tax. Currently, many non-resident multinationals (e.g., Google) pay no corporate income tax due to lack of a physical presence (e.g., servers) in the country. It is understood that no formal decision has yet been taken but the imposition of the tax is supported by a number of lawmakers. (Source: Thomson Reuters)
Lesotho	Starting from April 2018, the Ministry of Finance (MoF) decided to equate communication services' VAT to that of general goods and services which is now 15%. However, this increase was staggered and not applied all at once. As such, from April 2018 communication services' VAT was increased from 5% to 9%. Other increases will be implemented in the subsequent years. (Source: ITU Tariff Policies Survey, 2018)
Malaysia	The Malaysian Government is looking into the possibility of introducing a digital tax in its 2019 budget in November. Malaysia has not yet confirmed the final rules for taxation of digital services supplied by foreign companies to domestic residents. (Source: Quaderno.io)
Mexico	In addition to value-added taxes (VAT), the Special Tax on Production and Services (Impuesto Especial sobre Producción y Servicios – IEPS) is charged in Mexico. The IEPS is a special tax applied to the production of specific goods and services. Telecommunications services are subject to this tax of 3.0% of the total value of the service. However, this tax is not applied for fixed and mobile Internet services, public telephony, rural and interconnection. (Source: ITU Tariff Policies Survey, 2018)
Saudi Arabia	Saudi Arabia is a member of the Gulf Cooperation Council (GCC) and has implemented the group's policy on digital VAT from foreign sellers. The VAT rate for digital products is 5%. Once a foreign business passes the country's sales registration threshold, it must register for VAT in Saudi Arabia. The initial sales registration threshold of SAR 1 000 000 will be reduced to SAR 375 000 on 20 December 2018. (Source: Quaderno.io)
Senegal	For the use of digital services, consumers pay 23% of taxes: 5% of RUTEL (Redevance d'Utilisation des Services de Télécommunications – Charge for Use of Telecommunications Services) and 18% of VAT. (Source: ITU Regional Economic Dialogue for Africa, RED-AFR2018)
Singapore	From 1 January 2020, foreign-supplied digital services will be subject to Singapore Good and Services Tax (GST). The Singaporean Government has already confirmed that it will likely levy 7% VAT on goods and electronic services provided to consumers by non-resident companies. (Source: Quaderno.io)
Thailand	The National Broadcasting and Telecommunications Commission (the NBTC) has announced that it will propose a tax regime to the ASEAN Telecommunications Regulators Council by the end of 2018, to set a regulatory framework governing OTT companies in ASEAN, with appropriate state benefits. The current stated intention is that owners and operators of onshore and offshore OTT services will be subject to the same or similar regulations as traditional broadcasters and telecommunications companies, including requirements to obtain and pay for operators' licences, pay a value-added tax and be subject to stringent checks on illegal content. (Source: ITU Training on Competition analysis in the digital environment for Asia-Pacific 2018)
Uganda	The Government of Uganda introduced an OTT tax effective 1 July 2018. The tax is an excise duty on over-the-top (OTT) services and it is charged at rate of UGX200 per user per day of access. Users of any communications apps, not provided by their mobile operator, will have to pay a tax of UGX200 (USD0.05) per day. (Source: ITU Training on Competition Analysis in the digital environment for Asia-Pacific 2018)
UK	On 29 October 2018, in the UK Budget Speech it was announced that UK would impose a digital services tax of 2 percent of revenues of GBP500 million in global revenues from April 2020. The first GBP25 million of UK revenues is not taxable. It is estimated it will raise GBP1.5 billion in four years. It was also announced that UK is currently working with the G20 and the OECD also to consider how best to tax digital companies, and if those talks reach an agreement, the UK might consider those mechanisms instead of these announced plans. (Source: UK Government)
US	The tax authorities are developing a standard definition of digital products for sales taxed as there has been wide interpretation thus far. (Source: ITU Training on Competition analysis in the digital environment for Asia-Pacific 2018)

Source: ITU, based on various sources

the Organisation for Economic Co-operation and Development (OECD) released its report "Tax Challenges arising from Digitalization - Interim 2018".[149] The report divides different taxation perspectives amongst Member States into three categories – while noting today's international corporate tax rules are no longer fit for purpose in regard to multinational digital businesses:

- **The first group of countries' view:** the reliance on data and user participation may lead to misalignments between where profits are taxed and where value is created.
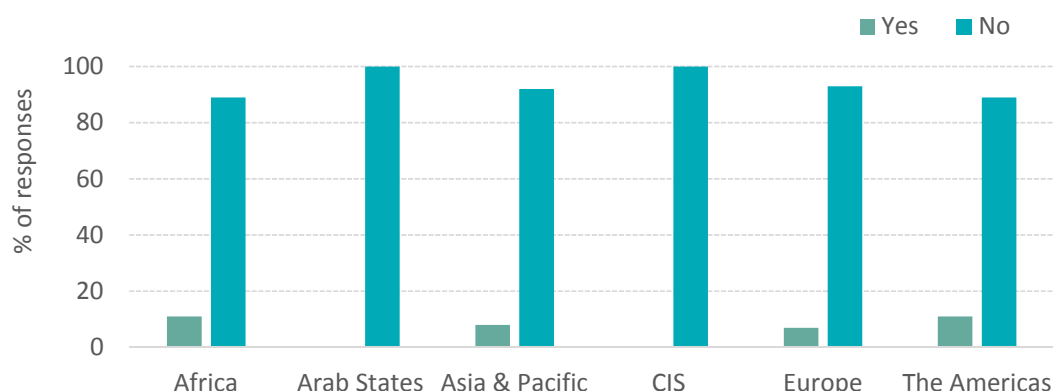
Source: ITU Tariff Policies Survey, 2017

- **The second group of countries' view**: the ongoing digital transformation of the economy and globalization, present challenges to the effectiveness of the international tax frameworks.

- **The third group of countries' view:** the Base Erosion and Profit Shifting (BEPS) package has addressed double non-taxation, although it is still too early to fully assess the impact of all the BEPS measures.

The OECD has identified three categories of policy challenge in this area:

- **Nexus -** The link between economic activity and a national jurisdiction may not be evident given that physical presence is not essential to conduct business in the digital economy.

- **Data -** Given prolific cross-border use of digital information in digital services, it is difficult to attribute where value is created – i.e. where collected or where used.

- **Characterization -** Digital technology delivers new services in ways t not readily aligned with tax rules based on traditional business and tax concepts.

Developing agreement and implementing a global, consensus-based solution will take time, and, in some countries, there are pressing calls for governments to take more immediate action to address the taxation issues. The OECD recommends that countries considering

implementing interim measures should take into account the following aspects:

- Be compliant with international tax obligations

- Be temporary

- Be targeted

- Minimize over-taxation

- Minimize impact on start-ups, business creation and small businesses

- Minimize cost and complexity

The OECD report further outlines a number of areas where there are clear differences of views held by countries, including over the need for future reform of the international tax system.

On 21 March 2018, the European Commission[150] proposed new rules to ensure that digital business activities are taxed in a fair, growth-friendly way in the EU, and makes two legislative proposals:

1. **Common reform of the EU's corporate tax rules for digital activities**
   Even if a company does not have a physical presence in the EU, Member States can tax profits generated in their territory. With these new rules, online businesses contribute to public finances at the same level as traditional companies. A digital platform will be deemed to have a taxable 'digital presence' or a virtual

Box 23: Taxation of the digital economy: steps to build on

- Taxation of the digital economy is a challenge faced globally and various approaches are being established. Governments should collaborate more closely on digital services taxation matters at regional and international level.

- It is important to establish effective mechanisms for collaborative regulation, given that taxation decisions fall to finance ministries and tax authorities rather than telecommunication/ICT authorities – for example, working together with all parties before making decisions. This could help in evaluating the possible distorting effects of each tax on the quality and quantity of services, as well as possible loss of welfare of the population.

- Governments should not compromise long-term, national economic benefits by targeting short-term revenue.

- As highlighted by the ITU-D Study Group 1 Question 4/1,[151] it is better to promote fiscal, para-fiscal and other incentives to encourage operators and service providers to reduce tariffs; this could include, for instance, the elimination of customs duties on telecommunication/ICT equipment and terminals – rather than apply excessive taxes.

- Governments should promote policies that: i) encourage balanced and harmonized taxes; ii) avoid excessive burden to all stakeholders; iii) promote both innovation and effective competition among all sector players in the digital ecosystem; iv) consider affordability as a priority.

Source ITU

permanent establishment in a Member State if it fulfils one of the following:

- It exceeds a threshold of EUR7 million in annual revenues in a Member State;

- It has more than 100 000 users in a Member State in a taxable year;

- Over 3 000 business contracts for digital services are created between the company and business users in a taxable year.

The new rules will also change how profits are allocated to Member States in a way that better reflects how companies can create value online, for example, depending on where the user is based at the time of consumption.

2. **Proposal 2: An interim tax on certain revenue from digital activities**
This interim tax ensures that those activities which are not effectively taxed would begin to generate immediate revenues for EU Member States.

The tax applies to revenues created from activities where users play a major role in value creation and which are the hardest to capture with current tax rules, such as revenues created from:

- Selling online advertising space;

- Digital intermediary activities which allow user interaction and which can facilitate the sale of goods and services between them;

- The sale of data generated from user-provided information.

Tax revenues would be collected by the Member States where the users are located, and will only apply to companies with total annual worldwide revenues of EUR750 million and EU revenues of EUR50 million. This limit will help ensure that smaller start-ups and scale-up businesses remain unburdened.

The private sector is also active in the field of taxation. GSMA has researched taxation of

ICT services,[152] and these studies suggest that jurisdictions with simple and transparent tax regimes on ICT goods and services have higher adoption rates. Sector-specific taxes on digital services distort and negatively impact take up of digital services (taxes on digital services are usually higher than other service sectors such as tourism). Higher taxes on digital services disproportionately affect groups sensitive to pricing and affordability of ICT services (i.e. low-income groups). Transparent, simple tax regimes are least distortive and disruptive. Each government will have to strike a balance between generating revenue and guarding against the negative impact on the take-up of digital services. Some of the steps to build on towards more balanced tax regimes for digital services and platforms are highlighted in Box 19.

4.5. New frontiers

We are already seeing technology paradigms that challenge existing regulatory patterns and frameworks. From the imminent entry in markets of 5G and the Internet of Things, to the profusion of cloud services and artificial intelligence, finding the regulatory sweet spot requires a new perspective and not mere incremental improvement. New technological phenomena will drive and define a new paradigm for regulation – for many regulatory issues, what is coming down the road will cause fundamental upheaval rather than seamless evolution. Many existing core regulatory questions and fixtures will take on a new meaning and will need to be re-tooled (see Figure 64).

> The lightbulb did not come from the continuous improvement of candles.
> *Oren Harari*

Regulatory upheaval from new technologies will give rise to the fifth generation (G5) of regulation. Countries need to leap forward to the next level of regulation, with a new attitude and a new toolbox – and regulators will need to reflect on their roles and revisit their responsibilities.

Collaborative regulation: reaching the next frontier together

At the core of collaborative regulation are principles of strengthening institutional capacity and the legal mandate of the regulator, sound regulatory regimes and enhanced competition frameworks. G5 does not mean more regulation, but rather more hands-on, inclusive and evidence-based regulation and decision-making. G5 also uses new tools and processes while building on the acquis of previous generations of regulation.

There is a growing consensus that collaborative regulation is the way forward. To attain moving regulatory targets today, the immediate questions are *how* to collaborate and *with whom*. Typically, the stakeholders involved in the consultative process in a collaborative regulatory setup can be grouped into three main knots (see figure 65):

- At the core is a tightly-knit group of separate sector regulatory institutions, such as the competition authority, the ICT regulator or the spectrum management agency. This is the area where collaboration is the most well-established compared with other groups as the agencies involved have a decades-long record of dealing with complex, converging issues.

- The middle knot, the verticals, creates a ring of formerly sector- or thematic-specific

Figure 64: Regulatory upheaval for new and emerging technologies

WHO REGULATES?
ICT regulator ——→ Multiple regulators

WHO'S REGULATED?
One/few ——→ many

REGULATORY PROCESS
Linear ——→ network, in cycles

REGULATORY OUTCOME
Legal text only ——→ plus connections, exchange of ideas and expertise, living outcome

REGULATORY INSTRUMENTS
Obligations ——→ incentives & collaboration

REGULATORY TOOLS
Legal ——→ also empirical, analytical, evidence-building
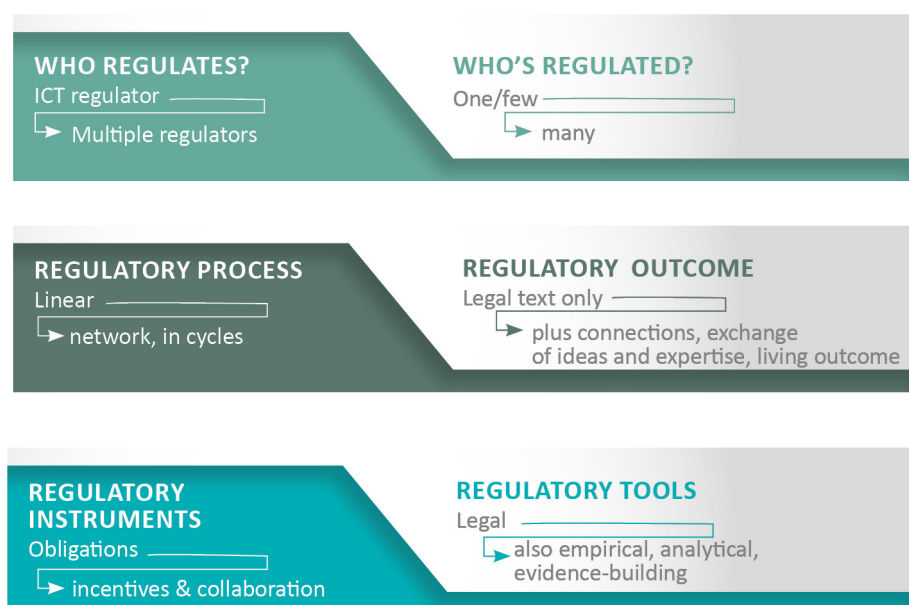
Source: ITU

Figure 65: The three knots of collaborative regulation

Core			
• Competition authority • Consumer protection authority	• Data protection/ Cybersecurity authority	• Media & broadcasting authority • Internet authority	• Radio spectrum agency • ICT regulator • ICT Ministry

Verticals

• Energy regulator • Financial authority	• Health authority • Education ministry	• Trade bodies • Government Ministries	• Technical agencies

Mesh

• Operators & service providers • Digital platforms	• Industries • Consumers associations	• Consumers at large, incl. unconnected/ unserved	• Academia • The judiciary • Municipalities

Source: ITU

regulators, such as the financial and energy authorities. Collaboration across this group remains rare and mostly partial and further efforts are needed to build institutional bridges and walk the talk of effective collaboration. This collaboration among the ICT regulator and eight of the agencies from the core and middle knot are examined in chapter 5.

- The third, widest and most heterogeneous knot brings together operators and service providers and digital platforms, together with consumer associations, municipalities, the judiciary and academia. Their respective roles differ; however, they all share the ultimate goal of building resilient, agile regulatory frameworks for the digital transformation.

Figure 66: Collaborative regulation – benefits and challenges

Benefits

- Strengthened institutional capacity, legal mandate of the regulator, sound regulatory regimes and enhanced competition
- Hands-on, inclusive regulation and decision-making featuring tools and processes
- Teaming with other sector regulators to address multi-sector issues – shared sector-specific expertise and responsibility for decision-making
- Focus on how to collaborate and with whom
- Not a silver bullet

Challenges

- Slow pace or difficulties to carry out a policy review/ development
- Develop new strategic thinking about regulatory priorities and challenges
- Comply with government procedures & rules, jurisdiction issues
- Capacity of the ICT regulator to handle new issues (expertise & staff development, motivation)
- Get the evidence to support decision-making
- The more important the matter, the more complex the collaboration
- Institutions working in silos, turf wars

Source: ITU

But collaboration – and collaborative regulation – is not a silver bullet. There are going to be challenges along the way (see Figure 66). From redefining policy cycles to grounding them in concrete evidence to bridging the gaps in mandates and operational power through collaboration – the challenges tip the massive digital transformation and might trap collaboration within stiff, closed institutional and regulatory framework and malfunctioning rule-making mechanisms.

New technological paradigms will create significant challenges – and addressing them effectively will take time. Regulation will not necessarily lag behind markets since inventions are still looking for the 'killer app', or are struggling to find the right business model. Market and regulatory paths will evolve simultaneously – not in parallel, but in symbiosis. Concepts will therefore need to be defined, understood and reflected on before a regulatory response can be given.

We cannot yet talk about 5G or AI regulation since these technologies encapsulate a wide range of issues, some requiring regulatory oversight, others not. They are technically complex and their current definitions are too broad to be helpful from a regulatory perspective.

We do suggest that it is important to define a regulatory paradigm for 5G, IoT, AI or any new technological phenomenon that might come up in the ever-accelerating digital economy is outlined in Figure 67. Such a framework can host and guide the co-creation of new regulatory rules, capitalizing on the strengths of the actors involved and allowing space for teaming up around a market failure to turn it into a digital market opportunity.

G5 regulatory response – design principles

Design principles are at hand for regulators to help develop an understanding of new technology paradigms and guide them towards appropriate regulation (see Figure 68). Led by these principles, regulators can fine-tune their regulatory response, ensuring optimal impact on the market.

Design principles to help respond to new technology paradigms stemming from G5 include:

• **Collaborative and trust-based**

Gone are the days when regulation was regulators' business. The regulatory process counts as much as its outcome, and may in fact determine the regulatory outcomes to a great extent. Regulation

Figure 67: Framework for blending the technology and regulatory paradigms

Technology paradigms

New
- 5G
- IoT
- Cloud
- Big data
- AI
- Blockchain
- Data portability
- Digital currencies
- Digital identity

Related to core
- Competition
- Spectrum management
- Infrastructure sharing
- Interconnection
- Privacy & data protection
- Consumer protection
- Universal access & service

Key factors

Technology:
- Is it a native new technology, an upgrade of an existing one or a combination of technologies?

Economic:
- What is the social and economic impact?

Financial:
- What is the cost of services?

Innovation:
- Can it be compared to anything pre-existing?

Inclusion:
- Who is likely to use it? Who will benefit?

Regulatory tools
- Evidence-based tools & approaches: RIA, quantitative & qualitative mapping/GIS
- Regulatory lab: from sandboxes to regtech
- Data-driven regulation
- Adaptive, blended regulation
- Reg packages/ formulas
- Blockchain for regulation
- Design sprints
- Grass-root outreach

Source: ITU

Figure 68: Collaborative regulation design principles
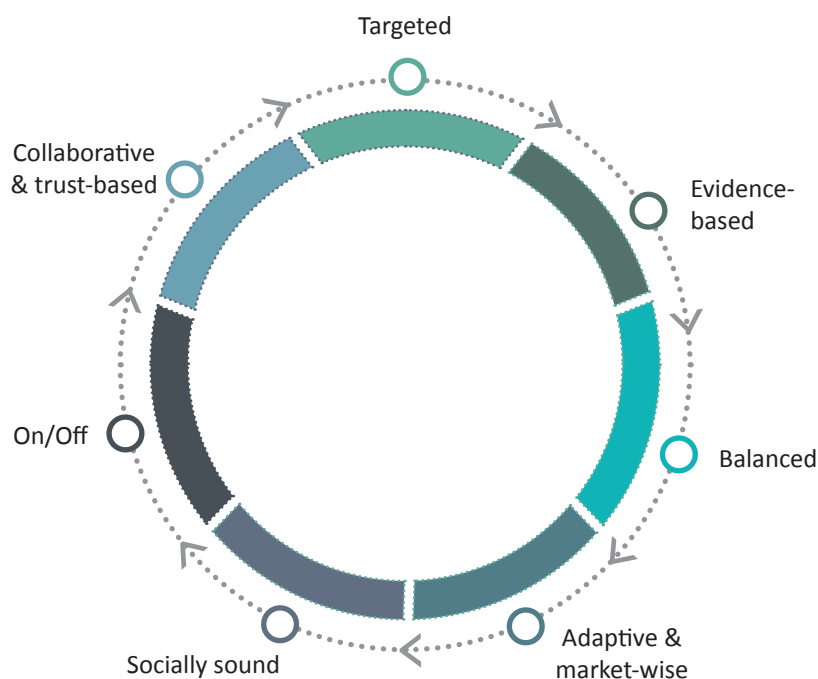
Source: ITU

of new, complex technological paradigms needs to be open and inclusive. The regulatory thinking cycle should include the expectations, ideas and expertise of all market stakeholders, including government agencies from different sectors, private sector players and data scientists.

- **Targeted**

Regulators need to look at the most pressing issues and create a domino effect on market barriers and enable synergies. Adopting new regulations 'just in case' or because other countries have done so should not be the rationale for regulatory response to new technologies. Regulators – the ICT regulator or any similar agency – should not aim to cover each and every topic. They should remain committed however to covering only those topics that they consider key for their markets and not regulating those with little impact in their jurisdiction – as committing to everything might equal committing to nothing.

- **Evidence-based**

We cannot overemphasize the importance of grounding regulatory decisions in robust, multi-faceted evidence. Evidence matters for creating a sound understanding of the issues at stake and

identifying the options going forward, as well as their impact.

- **Balanced**

The balance in regulatory treatment of new services is more delicate than ever. Imposing too tight a regulation can stifle innovation and investment, alienating market players. Too loose and light a regulation, on the other hand, can be insufficient, leading to market dominance or unfair market practice. The delicately judged requirement for future regulations might also be one of the most complex to handle.

- **Adaptive and market-savvy**

Regulation-making is about flexibility – continually improving, refining, and adjusting regulatory practices, an increasingly iterative process. A close, continuous link to markets and market players and a listening ear to consumer feedback are important to get markets on the right glide path to achieving social and economic goals – and social comes first.

- **Socially-sound**

Regulation is increasingly becoming 'value-based'. Going forward, it can accommodate social needs

blending it with the expected social impact of technologies and their use. Regulation might address questions such as: 'Do we, as a society, need those new services?', 'Are they aligned with our values?', 'Should we allow them just because they've come of age?', and 'Wouldn't it be better for consumers as a whole to not allow those services to markets?'. This is a complex new role for regulators, and it should be recognized by market players and consumers alike.

- **On/off**

Going forward, regulation is likely to evolve with a dual focus: enabling positive market dynamics and problem solving. Regulators should thus be ready to operate with a carrot and a stick. Regulation should no longer be seen as a permanent fixture, but rather as a temporary enabler or remedy, to be switched off once markets reach equilibrium – if they do so.

In applying such design principles for regulatory response to new technology paradigms, regulators have available a range of tools across the continuum of regulation action or response (see Figure 69). Incentives and monitoring are likely to be preferred, thus creating the drivers of the digital economy. Obligations and regulatory remedies will not disappear; however, they remain the last resort in monopoly or market dominance situations. Many aspects of the digital economy may not require any regulation at all. On the other hand, when markets have matured and have established healthy competition or self-regulatory mechanisms, deregulation will prevail.

Regulatory thinking cycle 2.0

A broad framework for exploring new technologies and design principles should form the basis for a revisited regulatory thinking cycle, one that supports collective thinking on new technological paradigms led by regulators.

The cycle we propose covers ten steps (see Figure 70):

Step 1: Observe & gather evidence

The first phase of the cycle is fundamental for building up a sound regulatory response to new technologies, services and more complex phenomena. It is also one of the most important as it grounds the process and links it to market realities.

Step 2: Model & analyse

Based on the evidence and using various analytical and economic modelling techniques as well as regulatory impact assessment, this phase structures available elements/features and creates an evidence-based framework for decision-making.

Step 3: Consult

In order to open dialogue with all stakeholders affected by the new paradigm, it is essential to engage in consultations and constructive dialogue around the new technology paradigm, supported with the evidence produced during the previous phase.

Step 4: Define

Based on the dual input received – hard evidence and stakeholder views – regulators need to develop a definition or, at least, a delimitation of the paradigm, which is crisp and clear, as well as useful from a regulatory perspective. The definition should identify areas for regulatory codification, incentives or enforcement.

Step 5: Ideate

In order to go beyond established regulatory practices and pinpoint new tools, it is important to generate a wide range of ideas, among all stakeholder groups. These will feed into the top scenarios to be explored and prototyped.

Figure 69: Continuum of regulatory action

No regulation → Incentives → Monitoring → Obligations → Remedies → Deregulation

Source: ITU

Figure 70: Regulatory thinking cycle 2.0
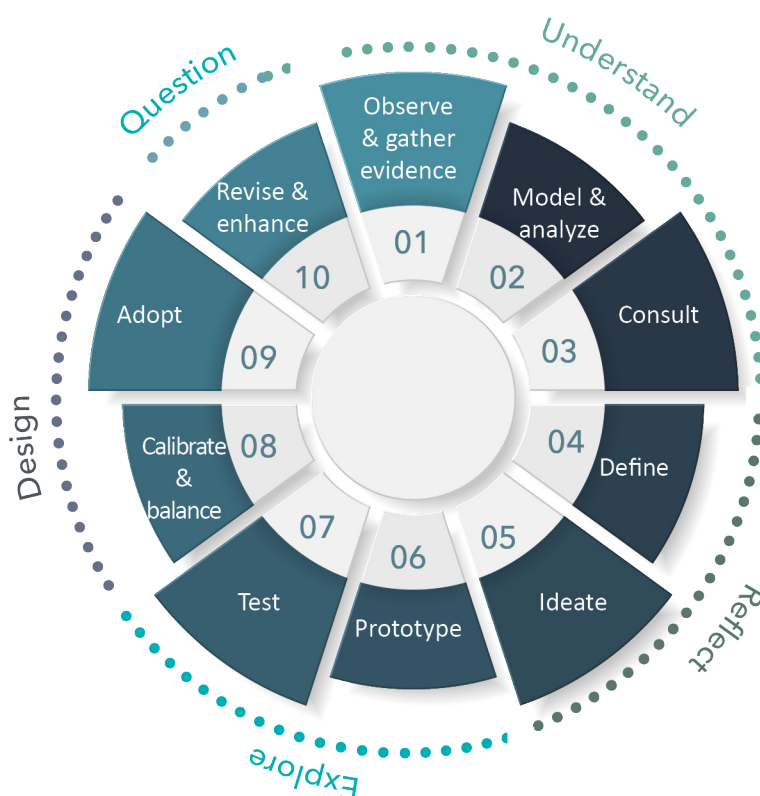
Source: ITU

Step 6: Prototype

Once all resources are available, the regulatory multi-stakeholder team can develop prototypes for the top ranked solutions based on the ideas identified and the buy-in of stakeholders.

Step 7: Test

Testing is a new, core pillar of the regulatory thinking cycle. It provides space for trial and error, along with the opportunity to fine-tune, revise or scrap ideas before they flow into formal policy and regulatory frameworks. Regulatory sandboxes, accelerators and unregulated pilot projects are central pieces of this phase.

Step 8: Calibrate & balance

Fine-tuning is an important step that allows for calibration of regulatory targets and the regulatory solutions towards them. The process leaves room for rebalancing regulatory intervention, evaluating tools at hand, while increasing chances for successful future regulatory frameworks.

Step 9: Adopt

The culmination of the process is the adoption of the (hopefully) true-and-tested solution and its implantation into the body of national regulation.

Step 10: Revise & enhance

Even when a regulatory decision is adopted, the process is not over – and probably will never be. Regulators need to monitor and continuously analyse implementation and enforcement patterns while studying the short-to-mid-to-long-term effects of regulations and ways to revise and enhance them.

Design principles and new tools for collaborative regulation will be elaborated in the next edition of the Global ICT Regulatory Outlook, to be published in 2019.

Finding the shortest path to collaboration

On the regulatory horizon, G5 is the next frontier. A few countries have already started the journey and their experiences can light the way to others coming after them. Various countries (including Croatia, France, Kenya, Pakistan, Russian Federation and Uganda) have shared their insights with ITU on the smooth or rough transition towards enhanced regulatory collaboration. Several important points have recurred repeatedly, emphasizing their importance in the process:

- **Stakeholders** have a key role to play at all stages of the regulatory process, from consultation to prototyping to picking the top regulatory options.

- **Regulatory oversight vs stakeholder input**: the regulatory process is becoming an ongoing conversation and channel the expertise, views and expectations of all market stakeholders.

- **Striking a balance** between effective listening to the feedback from the private sector and peer regulators, on one hand, and regulatory mandates and imperatives, on the other, will be central to forging failure-proof regulatory rules.

- **A bottom-up** approach to rule making is a stark characteristic of collaborative regulation. Participative leadership and shared thinking are likely to provide better outcomes than power structures. Regulators of any breed also need sufficient capacity to have impact. Synergies across institutions can help augment regulatory capacity and provide a shortcut to common regulatory goals.

- **Collaborative regulation is a philosophy** evolving around active listening, joint exploration and weighing of options, evidence-based decision-making and active monitoring of trends, markets and regulatory impacts. Organic collaboration is only possible when a set of important criteria are met. They are outlined in Figure 71.

Figure 71: Collaborative regulation: an actionable philosophy

People are the key to successful collaboration: creating a culture

Know your market

Important to speak the same language

Be mindful of the impact of regulation on the economy

Listen, Act, Observe

Maintain transparency & disclosure in corporate governance

Sharing of data and common principles is important

Think holistic – boundaries are blurring and changing

Source: ITU

Figure 72: The most important steps towards collaborative regulation

UCC Uganda
- Review of regulatory frameworks
- Market review
- Clear identification of roles & responsibilities and areas of collaboration

HACOM Croatia
- Get operators on the table to discuss investment and price reduction
- Serve as an interface in the negotiations between government and industry
- Develop a regulatory thinking about new businessconcepts

CA Kenya
- Gap analysis to identify areas lacking collaboration
- Map agencies and entities to collaborate with
- Have a strategic outlook or plan what needs to be achieved through collaboration

PTA Pakistan
- Work with Government to shape new progressive policy guidelines
- Work out concrete mechanisms for collaboration with entities whose mandates overlap
- Skill up regulatory professionals, especially at the executive level

MICT Russian Federation
- Define mechanisms for effective collaboration
- Hold an inclusive dialogue across verticals
- Share guiding principles and best practices on how regulation can be leveraged for ICT development

ARCEP France
- Gather evidence on market performance and reg impact
- Promote innovation: adopt an open approach to ensuringaccess to scarce resources
- Data-driven regulation as a new toolbox

CRC Colombia
- Full-fledged regulatory impact assessment
- Roadmap for regulatory simplification
- Defining a new regulatory agenda based on market evidence and broad consultation

Source: ITU, based on feedback from national regulatory authorities

Among those regulators who have been ahead of the curve and have already introduced collaborative regulation as a high-level principle in their work, ITU has sought to find out what were the top three most important actions a regulator can undertake to move towards collaborative regulation. A concise exhibit of their views and priorities based on direct reports by regulators is given in Figure 72.

We find many commonalities among the feedback from regulators, however – not surprisingly – there is no single pattern emerging out of it.

Models for collaborative regulation – as any other good regulation – cannot simply be copied and pasted onto existing regulatory and institutional frameworks. Every regulator needs to develop

their own thinking and put it in the perspective of their own goals and priorities in order to shape the most appropriate, sound and effective framework for decision-making and enforcement.

Open call: We need your views, experiences, perspectives, insights and comments on the topics of:

- Generations of regulation
- Collaborative regulation
- The transition towards more mature and collaborative regulatory frameworks.

Please express your interest at: treg@itu.int

Box 24: GSR-18 Best practice guidelines on new regulatory frontiers to achieve digital transformation

We, the regulators participating in the 2018 Global Symposium for Regulators, recognize that, flexible and innovative policy and regulatory approaches can support and incentivize digital transformation. The best practices in this regard would allow us to respond to the changing landscape and address the continuing need for secure and reliable ICT infrastructure, affordable access to and delivery of digital services, as well as protect consumers and maintain trust in ICTs.

We believe that clear consideration is needed to ensure that the policy and regulatory approaches adopted are not a barrier to future innovation and progress while protecting consumers and extending connectivity to those who remain unconnected.

To this end, we the regulators participating in the 2018 Global Symposium for Regulators, believe that we need to:

- consider putting in place innovative, out-of-the-box measures such as:
  ° regulatory sandboxes for enterprises wishing to test an emerging technology or innovative service without being bound by all the regulations that would normally apply;
  ° "start-up and experiment" interfaces to support start-ups, enterprises and communities in their experimental initiatives;
  ° 5G pilot projects to obtain initial feedback and facilitate reflection and design of future spectrum allocations while stimulating the take-up of services, building specific use cases and assessing future challenges related to emerging technologies under real-life conditions;

- promote further public participation and consultation in the regulatory process through regulation by data, that is based on information and observations of digital stakeholders and users, providing citizens and stakeholders with the most detailed and transparent information, and allowing consultation and participation in the regulatory decision-making process to complement the regulator's traditional tools;

- establish effective mechanisms for cooperation across the sectors to promote the development of cross-cutting services such as e-commerce, e-banking, and e-health, including with consumer protection authorities, service providers and other relevant bodies at the national, regional and international levels;

- consider, as appropriate and within our mandate, the necessary frameworks to ensure privacy and security of government, business and consumer data so that stakeholders are adequately informed about potential security and privacy challenges they may face with online services, and have access to timely and accurate information regarding the services and applications they use (including reliability, speed, quality of service and data traffic management).

Source: ITU

Endnotes

1   http://nca.gov.so/about-us/

2   http://www.paclii.org/nr/legis/num_act/caba2018293/

3   Telegeography (24 October 2018) : https://www.telegeography.com/products/commsupdate/articles/2018/10/
     24/niger-adopts-three-new-telecoms-sector-decrees/?utm_source=CommsUpdate&utm_campaign=da49c7ce29
     -CommsUpdate+24+October+2018&utm_medium=email&utm_term=0_0688983330-da49c7ce29-11619241

4   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/
     RegulatorySurvey.aspx

5   Postal & Telecoms Regulatory Authority Zimbabwe (POTRAZ): http://www.potraz.gov.zw/

6   Telegeography and The Economic Times, https://telecom.economictimes.indiatimes.com/news/trai-to-be-renamed-as
     -digital-communications-regulatory-authority-of-india-manoj-sinha/65971515

7   Cullen International, https://www.cullen-international.com/ (account necessary)

8   Cullen International, https://www.cullen-international.com/ (account necessary)

9   ITU research and G20 New Industrial Revolution Action Plan: http://www.g20chn.com/xwzxEnglish/sum_ann/201609/
     P020160912341429630547.pdf

10   Analysys Manson (April 2018): https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G
     _2018.pdf

11   ARCEP: https://www.arcep.fr/index.php?id=8571&no_cache=1&no_cache=1&tx_gsactualite_pi1%5Buid%5D=2160
     &tx_gsactualite_pi1%5Bannee%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx
     _gsactualite_pi1%5BbackID%5D=26&cHash=1c6543c915ed03e42982c7b134d62b52&L=1

12   ITU, Regulatory challenges and opportunities in the new ICT ecosystem, 2017, https://www.itu.int/dms_pub/itu-d/opb/
     pref/D-PREF-BB.REG_OUT03-2018-PDF-E.pdf

13   http://www.amcham-egypt.org/Trac/reports/Competition_Law_Dec_2006.pdf

14   http://www.drewnapier.com/DrewASPX/media/assets/Publications/Guide-to-Merger-Control-in-Sg_Drew-Napier.pdf

15   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/
     RegulatorySurvey.aspx

16   https://telsoc.org/sites/default/files/tja/pdf/70-773-4-pb.pdf

17   http://www.cuts-ccier.org/7up4/pdf/7up4-Synthesis_Report-En.pdf

18   https://www.acm.nl/en/about-acm/our-organization/the-netherlands-authority-for-consumers-and-markets

19   https://www.state.gov/e/eb/rls/othr/ics/2013/204687.htm

20   https://www.wto.org/english/tratop_e/tpr_e/s349_sum_e.pdf

21   ITU, Regulatory challenges and opportunities in the new ICT ecosystem, 2018: https://www.itu.int/pub/D-PREF-BB.REG
     _OUT03-2018/en

22   Cullen International, https://www.cullen-international.com/ (account necessary)

23   Luc Hindryckx, ECTA Executive Director (28 February 2018): https://www.ectaportal.com/news/ecta-press-releases/800
     -competition-must-prevail-in-the-quest-for-telecoms-investment

24   Broadband TV News (2 July 2018): https://www.broadbandtvnews.com/2018/07/02/belgian-regulator-keeps-cable-open
     -adds-fibre/

25   ECTA (14 February 2018): https://ectaportal.us1.list-manage.com/track/click?u=429f3f6ee74e8713f2d06b2c7&id=
     7079a2a9c9&e=cebaee0e23

26   COMCOM (31 August 2018): https://comcom.govt.nz/__data/assets/pdf_file/0025/94255/Study-of-mobile
     -telecommunications-markets-in-New-Zealand-Issues-paper-31-August-2018.pdf

27   SAMENA Daily News (5 August 2018): "TRA Oman to review market, identify constraints to competition": http://www
     .samenacouncil.org/samena_daily_news?news=69266

28   UCC (13 December 2017): https://www.ucc.co.ug/files/downloads/USSD_and_SMS_Market_Review_Short_Final_Report
     _171213.pdf

29   TeleGeography (22 June 2018): https://www.telegeography.com/products/commsupdate/articles/2018/06/22/ofcom
     -publishes-draft-statements-on-wholesale-market-reviews/?utm_source=CommsUpdate&utm_campaign=777c77dae3
     -CommsUpdate+22+June+2018&utm_medium=email&utm_term=0_0688983330-777c77dae3-8871709
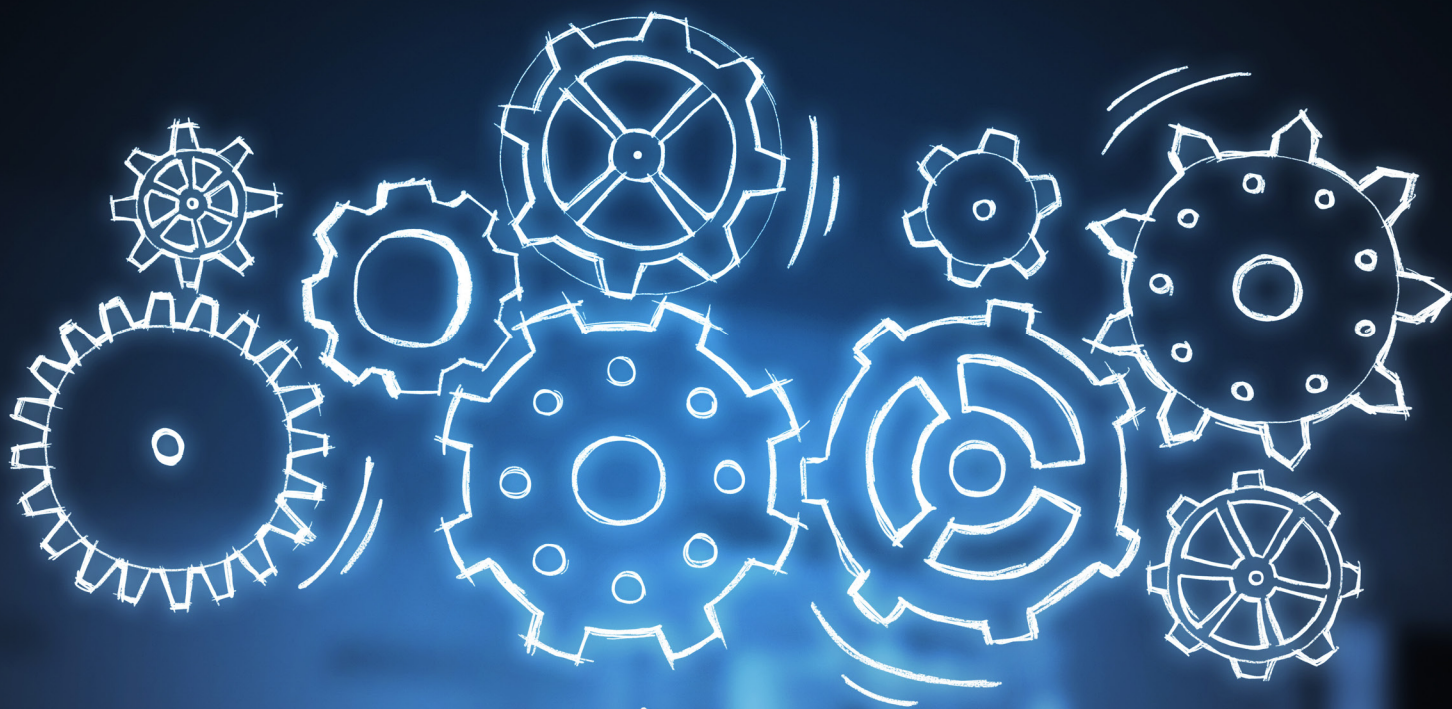
30   ITU, *Global ICT Regulatory Outlook 2017*: itu.int/go/outlook

31   TeleGeography (27 June 2018): https://www.telegeography.com/products/commsupdate/articles/2018/06/
27/supreme-court-orders-trio-to-return-spectrum/?utm_source=CommsUpdate&utm_campaign=117c20de4f
-CommsUpdate+27+June+2018&utm_medium=email&utm_term=0_0688983330-117c20de4f-8871709

32   Reuters (15 November 2017): https://www.reuters.com/article/telecomitalia-network/italy-regulator-to-decide-fate-of
-telecom-italia-network-by-mid-2018-idUSL8N1NL48M

33   InfoCuria (21 February 2018): http://curia.europa.eu/juris/document/document.jsf?text=&docid=199512&pageIndex=0
&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=614478

34   TeleGeography (22 June 2018): https://www.telegeography.com/products/commsupdate/articles/2018/06/22/telenor
-norge-fined-nok788mn-for-abuse-of-dominant-position/?utm_source=CommsUpdate&utm_campaign=777c77dae3
-CommsUpdate+22+June+2018&utm_medium=email&utm_term=0_0688983330-777c77dae3-8871709

35   ComCom (22 June 2018) "Lack of legal basis hampering competition in the area of telecommunication connection":
https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-71242.html

36   Quartz (27 June 2018) "A Nobel-winning economist's guide to taming tech monopolies": https://qz.com/1310266/nobel
-winning-economist-jean-tirole-on-how-to-regulate-tech-monopolies/

37   ACM (25 July 2018): https://www.acm.nl/en/publications/acm-launches-market-study-mobile-app-stores

38   European Commission (18 July 2018): http://europa.eu/rapid/press-release_IP-18-4581_en.htm

40   Mobile World Live (14 March 2018) "France to sue Google, Apple over app store concerns": https://www
.mobileworldlive.com/featured-content/apps-home-banner/france-to-sue-google-apple-over-app-store-concerns/?ID=
00320000011qCpUAAU&BU=

41   UNCTAD (8 June 2018) "Unity needed to shield people and markets from digital giants": http://unctad.org/en/pages/
newsdetails.aspx?OriginalVersionID=1778

42   ARCEP (France) contribution to the 2018 Consultation on the GSR Best Practice Guidelines, http://www.itu.int/
bestpractices

43   https://www.itu.int/net4/ITU-D/CDS/GSR/2018/documents/contributions/ARCEP_English.pdf

44   The CCF strives for a balanced membership of consumer representatives, industry organisations and regulators, and/or
policy-makers.

45   https://www.acma.gov.au/theACMA/About/The-ACMA-story/Communicating/acma-consumer-consultative-forum

46   Ofcom (@Ofcom), https://twitter.com/ofcom?lang=en

47   Communications Authority of Kenya, https://ca.go.ke/about-us/who-we-are/code-of-conduct/

48   ARCEP contribution to the GSR2018 Consultation, https://www.itu.int/net4/ITU-D/CDS/GSR/2018/documents/
contributions/ARCEP_English.pdf

49   ITU, Susan Schorr, GSR08 Discussion Paper: *What do we mean by 6 degrees of sharing?*, https://www.itu.int/ITU-D/treg/
Events/Seminars/GSR/GSR08/discussion_papers/Overview_Final_web.pdf

50   The title was inspired by the theory 'six degrees of separation', which argues that all people in the world can be
connected through no more than five intermediaries. This name was, in turn, used by Professor Martin Cave as the title
for his seminal article on functional separation.

51   A reference to the 2008 GSR Discussion Paper on functional separation: https://www.itu.int/ITU-D/treg/Events/Seminars/
GSR/GSR08/discussion_papers/Malcolm_Webb_session3.pdf

52   In 2012, the ITU's Radiocommunications Sector (ITU-R) embarked on a programme to develop international mobile
telecommunication (IMT) standards for 5G by 2020.

53   "The 5G era: Age of boundless connectivity and intelligence automation", GSMA Intelligence, 2017: https://www
.gsmaintelligence.com/research/2017/02/the-5g-era-age-of-boundless-connectivity-and-intelligent-automation/614/

54   https://www.techradar.com/news/eu-backed-groups-warns-about-5g–claims

55   ITU, Investment strategies for broadband deployment and access to the digital economy, 2016: https://www.itu.int/en/
ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR15_session1_Bedi.pdf

56   2017 ITU Telecommunication/ICT Regulatory Survey

57   For more information, see the PTS website: www.pts.se/en-gb/Industry/Radio/Auctions/Licences-in-800-MHz-band

58   For more information, see the EU website on the digital dividend, EU workshops on cable interference: http://ec.europa .eu/information_society/policy/ecomm/radio_spectrum/topics/reorg/dividend/index_en.htm

59   See the debate between Ofcom and two incumbent licence holders Vodafone and O2 about revoking a part of their spectrum rights in the 900 MHz band.

60   Oliver and Ohlbaum, "The Effects of a Market-Based Approach to Spectrum Management of UHF and the Impact on Digital Terrestrial Broadcasting", 27 February 2008: https://www.ebu.ch/CMSimages/en/Executive_summary_ENG_FINAL _tcm6-57752.pdf

61   Many variants are possible, like total, partial and concurrent transfer of (parts of) the licence.

62   BBC (20 December 2017) "Uber is officially a cab firm, says European court": https://www.bbc.com/news/business -42423627

63   Quartz (27 June 2018): https://qz.com/1310266/nobel-winning-economist-jean-tirole-on-how-to-regulate-tech -monopolies/

64   According to national definitions and self-reported to ITU.

65   ITU, data collected through the World Telecommunication/ICT Regulatory Survey 2017: https://www.itu.int/en/ITU-D/ Regulatory-Market/Pages/RegulatorySurvey.aspx

66   EU: https://www.antitrustlawblog.com/2018/01/articles/european-union/competition-regulatory-trends/

67   ACCC: https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry

68   Globalcompetitionreview.com: https://globalcompetitionreview.com/insight/the-asia-pacific-antitrust-review-2018/ 1166698/overview-competition-economics#endnote-037

69   AGE Platform Europe: https://www.age-platform.eu/policy-work/news/public-consultation-digital-ethics

70   liveMint: https://www.livemint.com/Industry/A17OkHBizuSRRJqwj2qinO/Trai-decides-to-reduce-scope-of-regulation-for -WhatsApp-Sky.html

71   UK Parliament: https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications -committee/inquiries/parliament-2017/the-internet-to-regulate-or-not-to-regulate/

72   TRAI, India: https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

73   Marzuki Darusman, chairman of the UN Independent International Fact-Finding Mission on Myanmar in The Guardian: https://www.theguardian.com/technology/2018/mar/13/myanmar-un-blames-facebook-for-spreading-hatred-of -rohingya

74   BBC: http://www.bbc.co.uk/news/technology-44290012

75   Baker McKenzie: https://www.bakermckenzie.com/en/insight/publications/2018/03/saudi-arabia-regulates-cloud -computing

76   Financial Times: https://www.ft.com/content/28edfa20-6e26-11e8-92d3-6c13e5c92914

77   Initially the survey targeted 61 Commonwealth and non-Commonwealth countries (including relevant ministry and regulator); 71 ISP, telecommunication and other network providers; and 15 leading OTT service providers. Out of the targeted respondents, 37 countries (approximately 46%) responded to the survey. 11 telecommunication and other network providers (approximately 14%) responded to the survey; in addition, 9 OTT service providers (11%) and 23 consumers (29%) responded to the survey.

78   This category included representatives of governments, policy-makers, regulators, competition authorities, and data protection authorities and related entities.

79   — Includes representatives of mobile and fixed network operators, Internet Service Providers (ISPs), broadcasting networks and other network operators.

80   — Includes representatives of OTT service providers, vendors, and content and application providers.

81   — Includes consumers of OTT services and representatives of civil society and consumer advocacy groups.

82   Cullen International, https://www.cullen-international.com/ (account necessary)

83   Cullen International, https://www.cullen-international.com/ (account necessary)

84   ReedSmith: https://www.technologylawdispatch.com/2018/03/in-the-courts/are-ott-services-telecommunications -services-german-court-asks-european-court-of-justice-for-preliminary-ruling-gmail-case/

85   Lexology: https://www.lexology.com/library/detail.aspx?g=62df0a70-3b37-4a27-a7e7-dcf41ba2e469

86   EUR-Lex (2016): http://curia.europa.eu/juris/celex.jsf?celex=62015CO0322&lang1=de&lang2=FR&type=TXT&ancre=

87   The Hankyoreh (29 November 2017): http://english.hani.co.kr/arti/english_edition/e_business/821285.html

88   Globalcompetitionreview.com: https://globalcompetitionreview.com/insight/the-asia-pacific-antitrust-review-2018/1166698/overview-competition-economics#endnote-037

89   CNBC (23 April2018): https://www.cnbc.com/2018/04/23/at-war-with-alibaba-top-brands-fight-china-e-commerce-giant.html

90   ITU-D Study Group 1: https://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2018&rgq=D18-SG01-RGQ03.1&stg=1

91   ITU Digital Ecosystem Portal: https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Collaborative_Regulation/App_Economy.aspx

92   ITU-T Study Group 3: https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Pages/default.aspx

93   FCC (11 June 2018): https://www.fcc.gov/restoring-internet-freedom

94   Nouveau magazine littéraire: https://www-nouveau--magazine--litteraire-com.cdn.ampproject.org/c/s/www.nouveau-magazine-litteraire-com/idees/le-numérique-a-toute-sa-place-dans-la-constitution?hs_amp=true

95   Law 20,453: http://www.leychile.cl/Navegar?idLey=20453

96   Users also provide free labour for the global sites by creating content. See: John Thornhill. 2018. "Social media users of the world unite! Might our data be better viewed as labour rather than capital?" *Financial Times*, 5 February: https://medium.com/financial-times/social-media-users-of-the-world-unite-75ff9c225b2b

97   "Data is giving rise to a new economy" *The Economist*, 6 May 2017: https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

98   Cullen International, https://www.cullen-international.com/ (account necessary)

99   ITU World Telecommunication/ICT Regulatory Survey 2018

100   Cullen International, https://www.cullen-international.com/ (account necessary)

101   Research ICT Africa, LIRNEasia and IEP: https://blog.mozilla.org/blog/2017/07/31/mozilla-releases-research-results-zero-rating-not-serving-ramp-internet/

102   Presentation of Maria Florencia Forciniti, Secretariat for Digital Government and Technological Innovation, Ministry of Modernization of Argentina at the Internet for All Advisory Board Meeting, WEF, September 2018

103   SAMENA Daily News (16 September 2018): https://www.samenacouncil.org/samena_daily_news?news=69728

104   https://www.echr.coe.int/Documents/Convention_ENG.pdf

105   https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

106   www.hrweb.org/legal/cpr.html

107   InfoCuria: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&amppageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=276332

108   See "The State of Broadband 2015" report for a discussion of multilingualism in online services:

108   https://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf

109   See "New Pathways to E-Commerce: A Global MSME Competitiveness Survey", ITC, Geneva, 2017: http://www.intracen.org/publication/New-Pathways-to-E-commerce/

110   ITU, The Rise of Social Media, 2010, https://www.itu.int/net/itunews/issues/2010/06/35.aspx

111   https://www.theguardian.com/technology/2017/may/16/google-deepmind-16m-patient-record-deal-inappropriate-data-guardian-royal-free

112   For an extensive commentary of this view point, see The Guardian (27 May 2014): https://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy

113   https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm

114   Catherine Tucker, Privacy, Algorithms and Artificial Intelligence, 2017: https://www.nber.org/chapters/c14011.pdf

115   UNCTAD

116   Cullen International October 2018 newsletter. See also: https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy

117   TRAI (16 July 2018): https://www.trai.gov.in/notifications/press-release/trai-releases-recommendations-privacy-security-and-ownership-data

118 Library of Congress (28 August 2018): https://www.loc.gov/law/foreign-news/article/brazil-personal-data-protection-law -enacted/

119 United Nations Digital Library (9 April 2018): https://digitallibrary.un.org/record/761158/?ln=en

120 ACMA (2018): https://www.accc.gov.au/media-release/new-competition-laws-a-protection-against-big-data-e-collusion and https://www.accc.gov.au/system/files/DPI%20-%20Issues%20Paper%20-%20Vers%20for%20Release%20-%2025 %20F.._%20%28006%29.pdf

121 http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

122 See the interactive map of the French data protection authority *Commission Nationale de l'Informatique et des Libertés* (CNIL) for a full list of countries: https://www.cnil.fr/en/data-protection-around-the-world

123 BBC (6 July): https://www.bbc.com/news/business-44702483

124 Importantly, the right to be forgotten is explicitly included and recognized in the EU's GDPR, in paragraph 65, which states that "'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation". See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

125 https://en.wikipedia.org/wiki/Right_to_disconnect

126 http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf. See pages 56-57, including table contents and figure

127 UNHCR, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, 2017: https://www.google.com/ url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi7udCbkeTeAhVKM-wKHcorCAoQFjAAegQICRAC&url =https%3A%2F%2Fwww.ohchr.org%2FDocuments%2FIssues%2FPrivacy%2FA-HRC-31-64.doc&usg=AOvVaw15z8aA3 -sEfUTbO3NH73LM

128 See also from the EU Commission: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet -sme-obligations_en.pdf

129 The Convention includes a section on the institutional framework for the protection of personal data that foresees the establishment, in each Member State, of national personal data protection agency. The duties, powers and enforcement measures of the Agency are detailed in the Convention that sets the basic principles governing the processing of personal data and the obligations of the data controller: https://au.int/sites/default/files/treaties/29560-treaty-0048_ -_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

130 https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

131 https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data -localization-clarifications/

132 http://www.vietnam-briefing.com/news/vietnam-approves-new-law-cybersecurity.html/

133 See for example, the report of the Broadband Commission Working Group on Digital Entrepreneurship: https://www .broadbandcommission.org/Documents/publications/DigitalEntrepreneurshipReport2018.pdf

134 UNHCR, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, 2017: https://www.google.com/ url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi7udCbkeTeAhVKM-wKHcorCAoQFjAAegQICRAC&url =https%3A%2F%2Fwww.ohchr.org%2FDocuments%2FIssues%2FPrivacy%2FA-HRC-31-64.doc&usg=AOvVaw15z8aA3 -sEfUTbO3NH73LM

135 UNDG, Guidance Note on Big Data for the achievement of the 2030 Agenda, 2017: https://undg.org/document/data -privacy-ethics-and-protection-guidance-note-on-big-data-for-achievement-of-the-2030-agenda/

137 Extract from "Germany Edges Towards Chinese-Style of Rating Citizens", February 2018: https://global.handelsblatt.com/ politics/germany-mass-surveillance-social-credit-china-big-data-886786

138 Statement by Mr. Ansgar Koene to the WTO Public Forum, 4 October 2018.

139 ITU GSR Discussion Paper, Digital Identity in the ICT Ecosystem: An Overview, 2018: www.itu.int/pub/D-PREF-BB/en

140 ITU-T Focus Group Digital Financial Services: Identity and Authentication: https://www.itu.int/en/ITU-T/focusgroups/dfs/ Pages/default.aspx

141 ITU GSR Discussion Paper, Digital Identity in the ICT Ecosystem: An Overview, 2018: www.itu.int/pub/D-PREF-BB/en

142 https://www.uidai.gov.in/

143 Statement by Mr Joe Anokye, Director General, National Communications Authority (NCA), Ghana, to the Global Symposium for Regulators (GSR) at ITU, July 2018

144 Statement by Mr Yahya Salim Alazri, Director, National Digital Certification Center (Oman National PKI), Information Technology Authority, Oman, to the Global Symposium for Regulators (GSR) at ITU, July 2018

145 The ITU paper on "Taxing telecommunication/ICT services: an overview" (2013) presents a clear taxonomy of telecommunication/ICT taxes as well as the principles concerning the effects of taxes, including direct and direct effects: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.TAX-2013-PDF-E.pdf

146 The results from the ITU Tariff Policies survey are available at ITU ICT Eye: http://www.itu.int/net4/itu-d/icteye/

147 Based on GSR-16 Discussion Paper, *The impact of taxation on the digital economy*: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR16_Discussion-Paper_Taxation_Latest_web.pdf

148 GSMA (2014): https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/Mobile-taxes-and-fees-Key-findings-and-recommendations_summaryreport-FINAL1.pdf

149 OECD: http://www.oecd.org/ctp/tax-challenges-arising-from-digitalisation-interim-report-9789264293083-en.htm

150 EU Fair Taxation of the Digital Economy: https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en

151 ITU-D Question 4/1: Economic policies and methods of determining the costs of services related to national telecommunication/ICT networks including next-generation networks, https://www.itu.int/pub/D-STG-SG01.04.1-2017

152 https://www.gsma.com/newsroom/press-release/gsma-report-highlights-impact-taxation-mobile-connectivity-latin-america/

5.   Regulatory collaboration: 'power coupling'

In the midst of a changing balance between economy and society, regulators must rely more than ever on market mindfulness and resourcefulness – even more than on legally established rules. Collaboration among institutions is not merely 'nice to have' or an amenity but an essential ingredient for regulatory relevance, coherence and impact.

Collaboration requires leadership. Collaborative leadership builds on a shared purpose and vision. It opens the way to diverse perspectives and possibilities. It provides a positive drive for problem solving and compromise. It capitalizes on the best of the organizations involved, as mutual interest is obvious.

5.1.   Is collaboration in ICT regulation really taking off?

We have carried out in-depth research on current collaborative practices among regulators involved in digital markets. We have gathered fresh, first-hand evidence on the existence and depth of collaboration between the ICT regulator and their peers dealing with competition, consumer protection, finance, energy, broadcasting, spectrum management and Internet issues. The key findings of this research are featured in the sections below.

Looking through this 'magnifying glass' at the state of collaboration in 2018, we provide a succinct overview of global and regional trends in each area and for each 'power coupling'. We refer to them in this way because their united action has a multiplier positive effect on digital markets – and their meaningful partnership is more than the sum of their parts.

Box 25: What is the difference between collaborative regulation and regulatory collaboration?

Collaborative regulation or 5th generation regulation (G5) is a broad notion that ITU has defined based on the concept of generations of ICT regulation (see Figure 9). It marks a fundamental shift in the way regulation is executed and the stakeholders that it brings together – from policy-makers, single-sector and multi-sector regulators to market players of any size. Collaborative regulation puts consumer benefits and protection in its focus and leverages the resources of government institutions and industry to deliver them, through organic consultation, collaboration and conciliation. Collaborative regulation is driven by leadership, incentive and reward rather than by command and control schemes. The concept also refers to the set of new tools used by regulators to tackle the issues related to digital transformation and the data economy.

Regulatory collaboration refers to the ICT regulator working closely with peer regulators in other sectors. It is defined by:

1.   The breadth of collaboration – whether the ICT regulator collaborates with authorities in charge of competition, consumer protection, finance, energy, broadcasting, spectrum management and Internet issues;

2.   The depth of collaboration – whether regulators have engaged in informal, formal collaboration, or have put in place other hybrid mechanisms.

Both concepts are linked and reflect the interplay of institutions and regulatory frameworks in regulating digital markets.

Source: ITU

5.2.   Power coupling: the ICT regulator and the competition authority

Ironically, competition is one of the most collaborative areas in digital services regulation. With convergence, regulatory cooperation has become a privileged instrument for assessing market dominance and handling disputes. From mergers to zero-rate offerings, ICT and competition regulators have been rolling up their sleeves together to balance digital markets, ensure fair dealings and protect consumer interests. On the other side of the coin, 15 per cent of countries still do not have an ICT or a competition regulator, or both, and this is likely to impact their regulatory effectiveness.

Where regulators exist, they cooperate in 60 per cent of countries globally. Informal collaboration is most prevalent, practiced by a third of regulators (see Figure 73). One-seventh operate in the framework of formal agreements, including Namibia, Nepal, Serbia and UK. In seven countries, a joint programme or committee is entrusted with liaison between ICT and competition regulators, notably in Ireland, Romania and Saudi Arabia. In a handful of countries globally, regulators have put in place customized mechanisms to facilitate collaboration. The Government of Singapore, for example, has introduced a data sharing API for all government bodies, called APEX and described as a network of data "pipes and gates", facilitating seamless access to agency databases and opening the way to smoother and faster collaboration.[1]

Figure 73: The state of regulatory collaboration between ICT regulators and competition authorities, worldwide, 2018
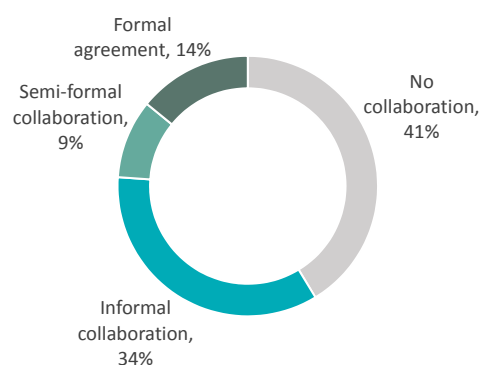
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 92 countries where an ICT regulator and a competition authority exist.
2) In 63, competition is part of the mandate of the ICT regulator.
3) In 29 countries, there is currently no scope for collaboration.
4) The research covered 195 countries; no data is currently available for 11 countries.
Source: ITU

Four in ten existing ICT and competition regulators have not yet engaged in collaboration, despite obvious gains. With collaboration gaining momentum, this is likely to change rapidly – increased regulatory collaboration will provide a welcome nudge to digital markets and trigger regulatory transformation.

Breaking down the global pattern into regional trends allows us to capture the degree of collaboration in the regions – and the differences

Figure 74: The canvas for collaboration between the ICT and the competition regulators, by region, 2018

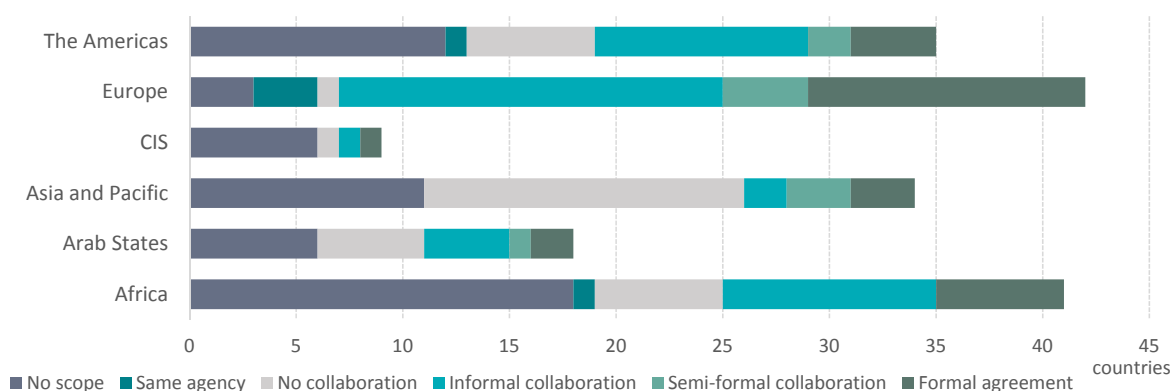Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 184 countries.
2) The research covered 195 countries; no data is currently available for 11 countries.
Source: ITU

are tangible (see Figure 74). Europe and Asia-Pacific, two regions of a comparable size, diverge widely in practice and degree of regulatory collaboration. In Asia-Pacific, seventy per cent of regulators are still uninvolved in collaboration compared to Europe, where over 97 per cent of regulators collaborate. In Africa, the Americas and Europe, regulators have a greater tendency to collaborate informally, unlike the other three regions. Europe is also the leading region in regard

Box 26: Degrees of collaboration explained

Collaboration comes in different shapes and forms. For the purposes of our research, we have defined the following four degrees of collaboration:

- **Informal collaboration**: refers to informal collaboration on enforcement action; it goes against established institutional frameworks and is driven by mutual interest and practicality. It is likely to become formalized over time.

- **Semi-formal collaboration:** refers to a one-off or *ad hoc* joint institutional fixture that works outside a formal framework for collaboration. It usually takes the form of a joint programme or committee and can be seen as an evolved model of informal agreement, where collaboration has an institutional status reflecting the importance of regulatory collaboration. This category also includes other hybrid regulatory collaboration fixtures.

- **Formal agreement**: reflects political awareness that collaboration benefits both organizations and a desire to capture these benefits; it involves systematic efforts to collaborate and define terms of engagement. Typically, regulators may sign a 'Memorandum of Understanding' to seal their partnership.

- **Same agency**: converged and multi-sector regulators in many countries have mandate over several areas, such as ICTs and broadcasting or spectrum, de facto providing a one-stop-shop for regulatory dealing. A consolidated regulatory structure may or may not guarantee close collaboration across the focus areas, so we have chosen to group such regulators in a separate category. This category also account for cases where the ICT regulator has a mandate in a focus area, in the absence of a separate specialized agency.

- **No scope for collaboration**: for the purposes of our research, when there is no ICT regulator or a specialized agency in the focus areas, or either, we may assume that there is no scope for collaboration. This proportion also shows the institutional gap that needs to be bridged to make collaboration possible.

- **No collaboration:** reflects the situation where there is no track for regulatory collaboration in place between the ICT regulator and sector-specific or multi-sector regulators.

And a word of caution: collaboration mechanisms do not on their own guarantee efficient collaboration. Multiple factors come into play, from human to resources to institutional. Our analysis does <u>not</u> imply that the benefits of collaboration are reaped by countries engaged in some form of collaboration. We do argue, nonetheless, that such mechanisms are an important indication and a prerequisite for consistent and mindful regulatory decisions.

The research is based on self-reported information gathered through the ITU World Telecommunication/ICT Regulatory Survey 2017 and 2018, additional desktop research and various contacts with officials from ITU Administrations.

Source: ITU

to formalized collaboration with the competition authority – over a third. Most joint programmes and committees have also been established in Europe. Overall, collaboration in the area of competition is the norm, although a large minority of regulators still need to join the trend.

Despite these encouraging trends, many countries still do not have a competition authority – a key stakeholder in boosting national economies and trouble-shooting competition dynamics. Around 40 per cent of countries in Africa and a third of the Americas do not have a competition regulator. This is also the case for a quarter of Arab States and Asia-Pacific countries, and only three countries in Europe. With growing government awareness of the expanding impact of the digital market on economies and society, new institutions are likely to come of age over the next few years to fill this gap.

5.3. Power coupling: the ICT regulator and the consumer protection authority

Consumers are at the centre of the digital market place; they pro-actively communicate and transact over two-sided digital platforms. Although they can make or break digital market leaders there are indications that consumers may become more vulnerable rather than less.

Consumer protection has shifted focus in the past decade, away from simply providing tariff information and channeling complaints and more towards data privacy and net neutrality. Regulators now face the challenge of better equipping consumers to deal with complex digital markets and make informed decisions. Consumer protection frameworks have evolved and are gaining ground in new areas, such as digital entrepreneur protection and digital financial transactions. Institutional frameworks have been converging – and regulatory collaboration is required and more valued.

Across all regions, two-thirds of existing ICT and consumer protection regulators have shared a table to tackle the toughest issues facing digital consumers (see Figure 75). More than half of these act under an informal collaboration framework,

Figure 75: The state of regulatory collaboration between ICT regulators and consumer protection authorities, worldwide, 2018
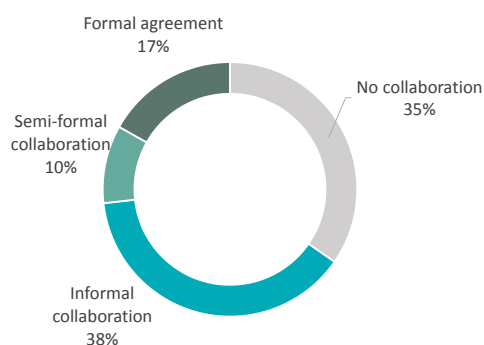
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
• The graph is based on data for 101 countries where an ICT regulator and a consumer protection authority exist.
• In 3 countries, consumer protection and ICTs fall under the mandate of a multi-sector regulator.
• In 78 countries, there is currently no scope for collaboration.
• The research covered 195 countries; no data is currently available for 13 countries.
Source: ITU

likely to lead to faster, dually-validated regulatory decisions. This is the established practice in Croatia, the Dominican Republic, Egypt, Iran and Moldova. In most cases, the consumer protection authority has the mandate to solicit and coordinate with various sector-specific regulators and ensure consistent, sound protection of consumers across the board.

One in six regulators have upgraded their collaboration through formal agreement, the outcomes of which, in turn, are likely to have more weight and legitimacy. This is the case of Armenia, Jamaica, Norway and Thailand where the shared jurisdiction of the two agencies has been recognized by a Memorandum of Understanding, also setting the practical arrangements for collaboration. In five countries, a core team has been tasked with collaboration under a joint programme or committee, jointly endorsing high-impact decisions and regulatory acts. A handful of countries have put in place other mechanisms reflecting their institutional set-up and specific market issues. The same authority is in charge of competition and consumer protection in Finland, Poland and Tanzania.

On the other hand, a third of regulators globally have yet to live up to the expectations of digital consumers, with consumer protection rules and their enforcement arriving via parallel channels with varied consistency and speed. For these digital consumers, the best protection might well be self-protection – though what hasn't been done by institutions might be difficult to achieve by consumers.

Regulatory collaboration practices for consumer protection differ by region (see Figure 76). Half of regulators in the Americas do not collaborate, compared to one-quarter of European and Asia-Pacific regulators, and 10 per cent in Arab States. In all regions, informal collaboration is more prevalent than formal, with Europe and Africa having respectively four and five of every 10 regulators engaged in informal collaboration. The region with the highest proportion – a quarter – of formally collaborating regulators is Africa. Ireland and Saudi Arabia have an operational joint programme or committee to deal with cross-cutting issues requiring multi-sectoral expertise.

Such figures need to be taken in the context of the institutional set-up in the regions. In Africa, Arab

Figure 76: Canvas for collaboration between the ICT regulator and the consumer protection authority, by region, 2018
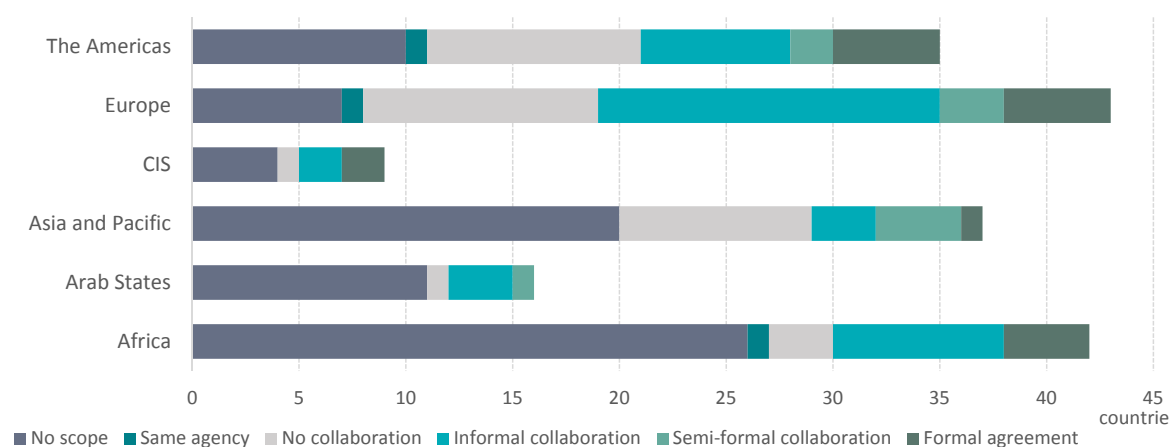
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
• The graph is based on data for 182 countries.
• The research covered 195 countries; no data is currently available for 13 countries.
Source: ITU

States and Asia-Pacific, over a half of the countries or more have neither a competition authority (for most) nor an ICT regulator. In contrast, three-quarters of countries in the Americas and more than 80 per cent of those in Europe have established separate regulators for ICT and consumer protection, and their increasingly closer collaboration is setting the tone for holistic, high-impact regulatory decisions.

5.4. Power coupling: the ICT regulator and the data protection authority

Data flowing over digital networks has been compared to oil, gold and blood. Not surprisingly, data protection has been a topic of heated discussion in recent years and has gained a lot of traction with regulators overseeing digital markets. For many consumers however, this has not been an issue because they have not been aware of the value of their data or how it is being commercialized by digital service providers. The issue needs to be addressed urgently.
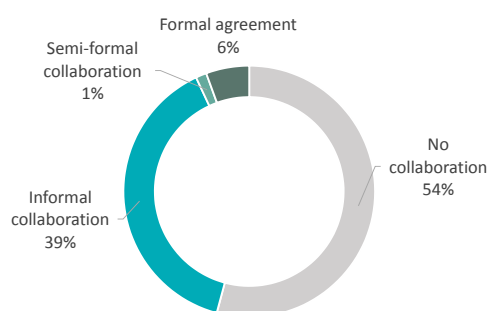
Compared to other key regulatory areas such as competition and consumer protection, data protection lags behind in institutions coming together – and this despite urgency of the task. At least half of regulatory agencies have engaged in no collaboration at all (see figure 77). This leaves a total of 33 countries where regulatory collaboration has proven possible. The great majority, or 85 per cent of those including Armenia, Canada, Gabon and Pakistan, collaborate informally, while those involved in formal collaboration – either through an agreement or a joint committee – represent a mere 2 per cent of countries worldwide.[2] In UK, Ofcom, the ICT regulator, and the Information Commissioner's Office have concurrent powers over data

Figure 77: The state of regulatory collaboration between ICT regulators and data protection authorities, worldwide, 2018

Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 72 countries where an ICT regulator and a data protection authority exist.
2) In 7 countries, data protection and ICTs fall under the mandate of a multi-sector regulator.
3) In 104 countries, there is currently no scope for collaboration.
4) The research covered 194 countries; no data is currently available for 11 countries.
Source: ITU

privacy and have sealed their collaboration in a Letter of understanding.[3] In Norway, Nkom cooperates along with public sector agencies with Datatilsynet, the data protection authority, for the digitization of the public sector, with focus on data protection.[4]

Institutional fixtures have been slow to form to tackle issues of data security, privacy and data protection. Globally, six out of every ten countries have set up a data protection authority – however the remaining 40 per cent are lagging behind (see Figure 78). Europe and Asia-Pacific are ahead of the other regions, having a large majority of countries with a mature, or maturing, institutional structures in charge of the area. In the rest of the regions, the trend has yet to gain momentum.

What's more, significant numbers of ICT regulators in most regions are not engaged with their peers on data protection. A silo approach is still prevailing in around 40 per cent of countries in Europe and a third of CIS countries. Where practiced, collaboration is mainly informal, with 40 per cent of European regulators making up for the most active region. Europe is also the only region where formal collaboration has been taking place, involving one in ten European regulators. In Africa, Asia-Pacific and the Americas, mainly informal collaborative mechanisms are providing channels for streamlining regulatory action.

A few regulators have clear legal guidance on their respective areas of competence and required collaboration. In Belgium, CPVP, the data protection authority, is mandated to handle issues related to personal data while IBPT, the ICT regulator, is competent in the area of online privacy excluding spam – which is under the responsibility of SPF Economie, the Federal public service of Belgium. In Finland, the Office of the Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. FICORA, the Finnish Communications Regulatory Authority, on the other hand, supervises the data protection of electronic communications in the operations of telecommunication operators, corporates or associations and other communications providers' operations.[5] According to the Austrian telecommunications law, in cases within the competence of the Austrian Data Protection Authority, RTR, the ICT regulatory authority, is required to coordinate and share with them

Figure 78: Canvas for collaboration between the ICT and data protection regulators, by region, 2018
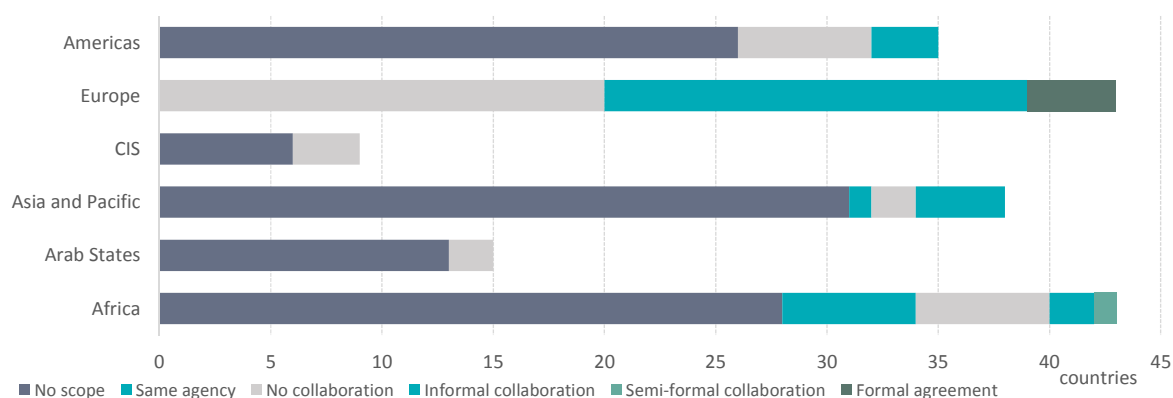
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 183 countries.
2) The research covered 194 countries; no data is currently available for 11 countries.
3) Agencies other than the ICT regulator and the data protection authority that may be in charge of privacy and data protection are not reflected in this research.
Source: ITU

any collected information.[6] In France, ARCEP has the right to seize CNIL, the data protection commission, on matters falling under their purview.

But even in the absence of explicit legal requirement, regulators in some countries may team up to face common challenges. In Ghana, both authorities worked together on revising the Code of conduct for telecommunications act for unsolicited electronic communications to ensure that the revised code is in line with the requirements under the Data protection act.[7] Likewise, when Malaysia faced a data breach in 2017, the Malaysian Communications and Multimedia Commission (MCMC) and the Personal Data Protection Commission jointly pledged to collaborate with different agencies for investigation.[8] In Italy, Agcom, the ICT regulator, the anti-trust authority and the data protection

authority started a joint investigation in 2017, with a view to defining a regulatory framework for the use of big data and promoting the protection of personal data, competition and consumer protection in digital markets.[9]

Every week brings more news of high-profile data breaches, or leaks on opaque business practices in user data management and digital identity theft – it is clear that data protection will be a major growth area for legal and institutional frameworks over the coming years. The overall impact of regulatory action – or inaction – also needs to be carefully assessed. With the onward march of AI and the burgeoning big data phenomena, the task at hand is highly-sensitive and global in scope. The degree of focus and coherence of the approach, pinpointed by regulatory collaboration, might in turn determine the degree of protection of personal data and consumers as a whole.

5.5. Power coupling: the ICT regulator and the financial regulator

Following the 2008 financial crisis, the financial sector is probably the most heavily regulated. It is also the sector with the largest number of separate regulatory authorities, 171 worldwide in 2018. At the nexus of communication technology and finance, mobile financial services and online transactions have grown ten-fold in a decade and have become an economic empowerment vector and a major field for tech and social innovation. The take-up of digital currencies has been equally impressive. Digital financial inclusion as a topic is high on political agendas – and national

Figure 79: The state of regulatory collaboration between ICT and financial regulators, worldwide, 2018
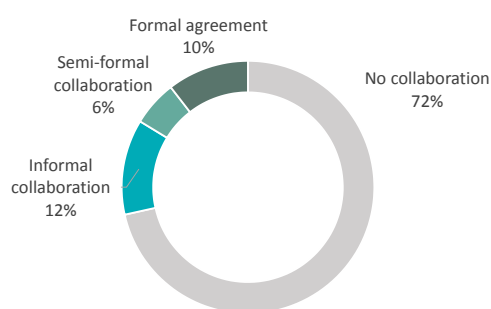
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 172 countries where an ICT and a financial regulators exist.
2) In 8 countries, there is currently no scope for collaboration.
3) The research covered 195 countries; no data is currently available for 15 countries.
Source: ITU

programmes have proliferated throughout the developing world.

However, collaboration between ICT and financial regulators has not yet taken root, despite a growing body of best practice guidance (see boxes 28 and 29).[10] Regulation from the two sectors is often fragmented and lacks coherence – weakening consumer protection and failing to provide predictability for digital financial markets. Only a quarter of regulators worldwide collaborate, and to a varying degree (see Figure 79). They are split equally between formal and informal collaboration, and one-off joint programmes and committees exist in only three countries (all in Africa). This low level of regulatory collaboration can be at least partly due to lack of institutional far-sight, as the mandates of the ICT and the financial regulators coincide in only 14 countries globally.[11]

In some regions, a lack of collaboration may be prevalent in up to 85 per cent of countries. Even regions with a well-established culture of institutional collaboration reflect a high rate of silo regulation. Looking at the regional figures (see Figure 80), the numbers are not encouraging. Against this gloomy backdrop, regulatory collaboration in digital financial markets in Africa deserves mention. Although half of the regulators in Africa still work independently, Africa registers the highest rate of collaboration among all regions.[12] Roughly half of African regulators involved in collaboration rely on formal legal instruments and structures, such as MoUs and temporary joint committees. This is the case in Ghana, Malawi, Swaziland and Zambia. Informal

---

Box 27: What are mobile financial services?

'Mobile financial services' is a catch-all term used to cover a wide range of financial services that can be provided over a mobile network, from mobile money services (including transfers and payments) to banking-type services (including deposits and borrowing), insurance and other services.

'Mobile banking' is usually used to refer to more traditional banking services provided over mobile devices. Such services may include deposits, withdrawals, loans, account transfers, bill payments and balance inquiries.

Source: ITU (2016), Digital financial services: Regulating for Financial Inclusion- An ICT Perspective, https://www.itu.int/pub/D-PREF-BB .REG_OUT02-2016

collaboration is, likewise, practiced by a quarter of African regulators.

The global trend is worrying; however, important new initiatives have been launched in a growing number of countries towards improving digital financial inclusion. Some developing countries have been building a solid shared regulatory portfolio between ICT and financial regulators, choosing the way of formal collaboration. In Angola, INACOM, the ICT regulator, the central bank (BNA) and the Ministry of Telecommunications and Information Technology have recently collaborated on mobile payments under a broader Memorandum of Understanding.[13] In Tanzania, the Bank of Tanzania and TCRA, the two regulators, partnered on mobile phone cash transfer controls.[14] In Pakistan, PTA and the State Bank have forged a joint regulatory framework to launch the Third Party Service Provider (TPSP) licensing framework that will introduce interoperability among the financial institutions and telecom operators.[15] In Singapore, a national consortium on fintech provides a platform for collaboration between the Infocomm Media Development Authority, the Monetary Authority of Singapore, SkillsFuture Singapore, six local universities and five financial associations,[16] under a Memorandum of Intent. Memoranda of Understanding (MoUs) provide an umbrella for regulatory collaboration also in the Dominican Republic, Rwanda, UAE, Vanuatu and US.[17]

Figure 80: Canvas for collaboration between the ICT and financial regulators, by region, 2018
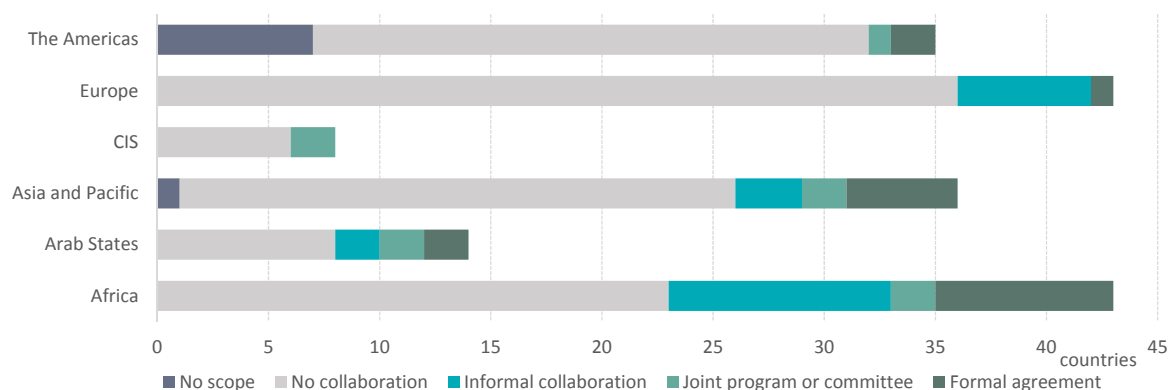
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 180 countries.
2) The research covered 195 countries; no data is currently available for 15 countries.
Source: ITU

The area of digital financial services is the one with the highest global number of joint programmes or committees among the areas of this research, nine semi-formal institutional structures intended to leverage regulatory collaboration. In Mozambique, the National Payment System Committee is an industry forum for discussions around NPS development and is comprised of the Bank of Mozambique, the Ministry of Finance, INCM, the ICT regulator, the Mozambican Stock Exchange, the Mozambican Bank Association, commercial banks and payment services providers.[18] In Morocco, Bank Al Maghreb, the central bank, has led the establishment of a strategic committee on mobile payments bringing together ANRT, the ICT regulator, other bank, the three national telecommunication operators and the ministries of economy and industrial cooperation.[19] In Trinidad and Tobago, a Payments systems council is in place, which includes the ICT regulator, TATT.[20] Joint committees exist also in Egypt, Eritrea, Ghana[21] and Kazakhstan.[22]

In the absence of separate ICT regulators, the ICT ministries in some countries have also established joint institutional fixtures. In Belarus, the National Bank is responsible for the ICT policy of the banking sector and collaborates with the Ministry of Communications and Informatization.[23] In China, the State administration for industry and commerce formal has launched joint initiatives with national financial regulation bodies and issues joint statements.[24]

Informal regulatory collaboration has powered important developments in countries in a few regions. In Kenya, one of the largest and most successful developing markets for mobile financial services, the two regulators have approved together a thin SIM technology to be deployed by Equity Bank.[25] In Lesotho, any institution willing to provide mobile financial services has to apply first to the ICT regulator and then to the central bank and both authorities exchange information in the process.[26] In Sierra Leone, the central bank launched the Digital financial services working group under the National strategy for financial inclusion 2017 – 2020.[27] Among the working group members are NATCOM, the ICT regulator, commercial banks, microfinance institutions, MNOs and Apex banks. In the Republic of Korea, the Financial Services Commission (FSC), has revised its guidelines regarding cryptocurrency, also consulting the Korea Communications Commission.[28] In Mauritius and Senegal, both authorities work together on issues related to financial inclusion on an informal basis.

Despite the strong social and economic motivation for ICT and financial regulators to collaborate, there has been little real progress on how and if they collaborate. As a policy paper from the Financial Intelligence Unit of Bangladesh has argued recently, a successful regulatory outcome requires a participatory approach among all stakeholders – especially regulators, banking supervisors, and the banking and telecom industries.[29] Much is at stake: the outcome of regulation of digital financial services affects

Box 29: G20 High Level Principles for Digital Financial Inclusion

In 2016, the G20's Global Partnership for Financial Inclusion (GPFI) published High Level Principles for Digital Financial Inclusion which aimed to catalyze government actions to drive financial inclusion through a focus on digital technologies:

High Level Principle 1 in particular calls for promoting digital financial services as a priority to drive development of inclusive financial systems, including through coordinated national strategies and action plans. It emphasizes the need for policy leadership and coordination across the public and private sectors as critical for expanding financial inclusion, and stresses the importance of leading by example in the push for digital solutions.

High Level Principle 4, on the other hand, stresses the need for policymakers and industry to work together to achieve a robust, open and efficient digital infrastructure, including a widely accessible retail payments system and ICT infrastructure.

Source: GPFI, 2016

ITU's work on digital financial inclusion

The 'Financial Inclusion Global Initiative' (FIGI) is a three-year programme of collective action to advance research in digital finance and accelerate digital financial inclusion in developing countries. FIJI is led by ITU, the World Bank Group and the Committee on Payments and Market Infrastructures, with financial support from the Bill & Melinda Gates Foundation. FIGI's operational work stream provides technical assistance to China, Egypt and Mexico to support their efforts to create policy environments capable of stimulating digital financial inclusion. FIGI's knowledge work stream—led by three Working Groups—advances research in three fields of critical importance to digital financial inclusion:

1. Digital payment acceptance by merchants and their customers;
2. The relationship between reliable identification systems and financial inclusion; and,
3. Security of, and trust in, digital financial services.

Past initiatives:

- ITU Focus Group on Digital Financial Services
- Global Dialogue on Digital Financial Inclusion (GDDFI)

social and financial inclusion, unlocking economic opportunities for the lower-income population.[30]

Regulating digital markets has become a central issue in economic policies for digital transformation, affecting both innovation and investment. With digital financial markets becoming more global, interconnected and complex, the overlaps and gaps in regulation and enforcement will have an important impact on consumers, businesses and, ultimately, governments. A more dynamic, collaborative approach to regulation can help prevent future crises and strengthen market forces.

5.6. Power coupling: the ICT regulator and the energy regulator

As with digital markets, the energy sector in many countries is experiencing rapid change. The challenges are many – from rising fuel costs to the demand for greener energies – impacting investment decisions and business practices alike. Driven by digitization and innovation, opportunities in the sector exist for new ICT-enabled models for generation, storage, distribution of energy and enhanced user control. Smart grids and meters are central elements in the infrastructure for the digital economy. Ambitious policy objectives are in place to improve the competitiveness, security, efficiency and sustainability of the energy sector in developed and developing countries alike. The potential of the energy sector to dramatically reduce its carbon footprint is boosted by digitization, feeding into high-level policy and progress towards sustainability goals.

The potential benefits of digital transformation in the energy sector are huge. Collaboration among ICT and energy regulators can help shape an enabling framework for smart grids (see Figure 81 above). However, in the majority of countries, collaboration isn't happening (see Figure 82) and only for one-fifth of regulators, collaboration is an established practice. Informal regulation is slightly more popular than semi-formal, both engaging roughly one out of ten regulators. Compared to most other sectors, regulatory collaboration in the

energy sector more often takes the form of a joint programme or committee, with around 10 per cent of regulators engaged in one-off or occasional initiatives. Formal agreements provide a sound framework for collaboration between regulators in a mere one per cent of countries with a regulator.

The degree of collaboration between ICT and energy regulators is similar across most regions, including Africa, Asia-Pacific, the Americas and Europe (see Figure 83). Three-quarters or more of regulators in these regions have not yet established institutional channels for collaboration or have failed to find the political will and common ground to start a joint regulatory process. In Arab States and CIS, over half of countries lack regulatory collaboration, too. Among the few collaborating institutions, there is no clear trend and practices diverge. In Africa, Asia-Pacific and the Americas, informal collaboration is more popular than semi-formal. In Arab States and Europe, the opposite trend holds true and in CIS both practices are equally used. Across all regions, formal collaboration is lagging behind as no country has formalized the institutional partnership between regulators.

From Côte d'Ivoire and Madagascar in Africa to Bhutan and Mongolia in Asia-Pacific to Kazakhstan and Ukraine in CIS – informal collaboration powers a new breed of regulatory partnership between ICT and energy regulators coming together on cross-sector matters. Jordan, Italy and Uruguay are also following the trail towards more coherent,

Figure 81: The case for collaboration between ICT and energy regulators

- ✔ ICT enables decentralized energy generation integrating renewable energy source
- ✔ ICT helps to operate and maintain power grids;
- ✔ ICT helps to identify and rectify technical and non-technical revenue losses
- ✔ ICT enables new decentralized trading, e.g. via blockchain
- ✔ ICT enables new payment models for mini-, micro-, off-grids solutions
- ✔ Smart meters and adjacent services require ICT to function

Generation **Operation** **Trading** **Retail**

- ✔ ICT helps to make power grids more reliable and resilient
- ✔ ICT is essential to integrate to integrate renewables, new storage, demand management, e-mobility, etc. to the grid
- ✔ ICT provide consumers with tailored information to improve their consumption and save energy

Source: For a full analysis on the topic, see ICT for ENERGY – Telecom and Energy Working Together for Sustainable Development, 2017

better regulation through informal channels of collaboration.[31]

Across all regions, a growing number of regulators have established joint committees. The Swedish Environmental Management Council has a broad mandate to contribute to sustainable development by supporting businesses and public administrations in their environmental work; both PTS and Energy agency are Council members.[32] In Ecuador, continuous efforts have been made towards the power and communications sectors modernization with the support of international donor organizations, also leveraging the collaboration between CONATEL and CENACE.[33]

Looking at the canvas for collaboration between the ICT and the energy regulators (see Figure 83), multi-sector regulatory agencies oversee both the ICT and energy sectors in 18 countries worldwide, mainly in the Americas and Europe.

Created in 2005, the *Bundesnetzagentur* (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, or BNetzA) in Germany is a separate higher federal authority bringing together various sectors and agencies. Interestingly, the Cartel office (BKartA) is responsible for competition law intervention. Although there are no concurrent powers between both agencies, meaning that there is no application of general competition law by BNetzA, such elements are directly incorporated as provisions in the Telecommunications Act and the Energy

Figure 82: The state of regulatory collaboration between ICT and energy regulators, worldwide, 2018
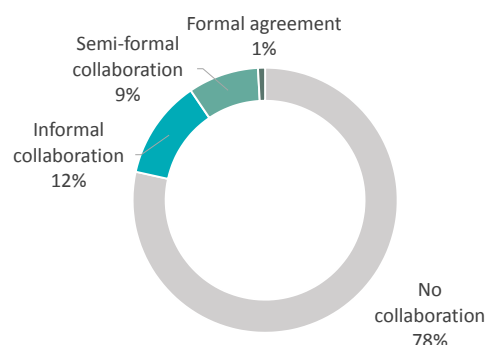
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 116 countries where ICT and energy regulators exist.
2) In 18 countries, energy and ICT regulation fall under the mandate of a multi-sector regulator.
3) In 54 countries, there is currently no scope for collaboration.
4) The research covered 195 countries; no data is currently available for 3 countries.
Source: ITU

Industry Act. The relevant laws, however, provide for information exchange to ensure legal certainty and avoid duplication or uncertainty.[34]

In Eastern Europe, multisector regulators active in both the ICT and energy sectors include the Public Utilities Commission (PUC) of Latvia, the Energy and Public Utility Regulatory Authority of Hungary and the Agency for Communication Networks and Services of the Republic of Slovenia.[35] Across the

Figure 83: Canvas for collaboration between the ICT and the energy regulators, by region, 2018

Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 192 countries.
2) The research covered 195 countries; no data is currently available for 3 countries.
Source: ITU

Caribbean, utilities regulators are also in charge of the sectors in Antigua and Barbuda, the Bahamas, Barbados and Belize.[36]

A single multi-sector regulatory structure can provide the proximity and interaction advantage for regulatory collaboration across silo sectors. It cannot, nevertheless, guarantee its effectiveness. We will be exploring the commonalities and differences between regulatory structures in terms of the scope for and the outcome of collaboration in the next edition of the Global ICT Regulatory Outlook.

Collaboration between ICT and energy regulators will not necessarily lead to a joint regulatory outcome. But collaborative regulatory processes will inform policy choices made by energy regulators and will provide cross-sector benchmarks and expertise. When crises arise, the advice of the ICT regulator will likely shape regulatory solutions, too, as in the case of cyber threats to the smart grid. Overall, collaborating on harmonizing regulatory rules, shaping an enabling framework and undertaking regulatory reporting and impact assessment – these are all key in preparing for the next stage in digital transformation, and can help set the stage for greater efficiency and growth across all economic sectors.

5.7. Power coupling: the ICT regulator and the broadcasting authority

Broadcasting undergone transformation over the past two decades, accelerating hard on the digital highway. The transition from analogue-to-digital brings consumers the opportunity to access more channels, better quality and new services such as high and ultra-high definition TV (HDTV and UHDTV), and 3DTV. To broadcasters, digital television transmission allows for better spectrum efficiency and reduced costs. Remaining in the analogue world is no longer an option.[37]

Digital television broadcasting has been in service for over a decade and the technologies have now fully matured. The transition to digital has been progressing steadily, across all regions. By the end of 2017, ITU figures on digital terrestrial television broadcasting (DTT) worldwide show 56 countries have completed the transition and in 68 countries the transition to DTT is ongoing.[38]

Historically, broadcasting has been a core part of the mandate of telecom regulators in the majority of countries worldwide. Today, ICT regulators in 117 countries include various aspects of radio and TV broadcasting transmission or content as part of their regulatory portfolio; they are converged regulators – despite the fact that separate broadcasting authorities exist in 96 countries worldwide. In fact, only 17 ICT regulators report having an overlapping mandate with the main broadcasting authority.[39]

However, the scope for collaboration between ICT and broadcasting authorities goes beyond those 17 jurisdictions. With broadband networks carrying broadcasting content and determining the quality of service for digital audiences, institutional collaboration can be a powerful asset for both sides. It has the potential to address regulatory issues in a meaningful, faster and holistic way. On a range of key issues, however, such as consumer protection and redress, other specialized agencies might also be required to seal a dynamic partnership – such as consumer protection authorities or agencies in charge of Internet-related issues.

Figure 84: The state of regulatory collaboration between ICT and broadcasting regulators, worldwide, 2018

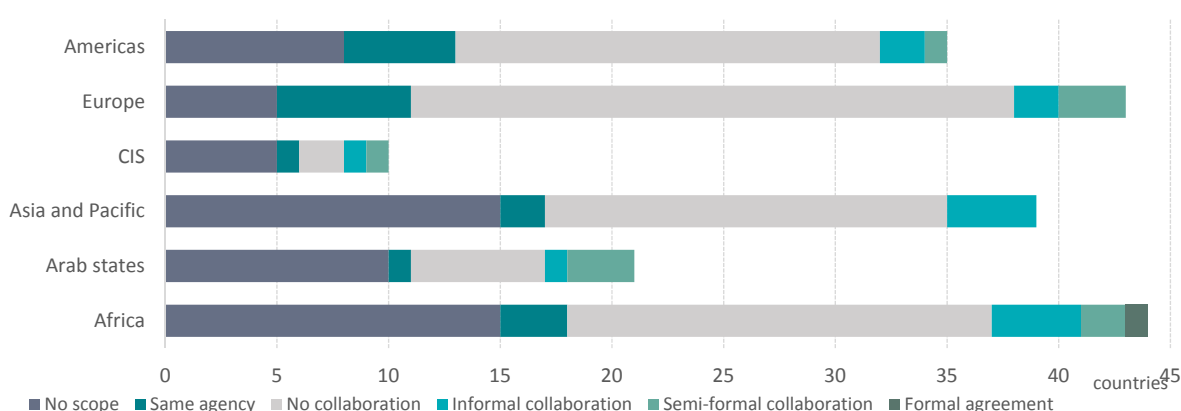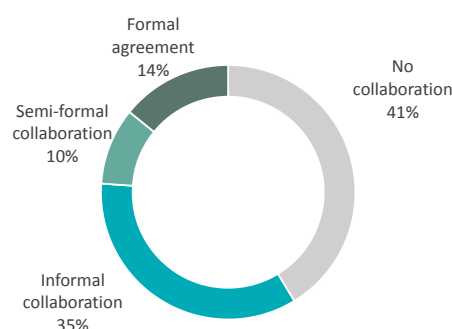Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 92 countries where ICT and broadcasting regulators exist.
2) In 63 countries, broadcasting and ICT regulation fall under the mandate of a multi-sector regulator.
3) In 29 countries, there is currently no scope for collaboration.
4) The research covered 195 countries; no data is currently available for 11 countries.
Source: ITU

Is collaboration happening?

Indeed, broadcasting might be one of the most collaborative regulatory areas currently. Our research showed that in close to one-third of countries, a converged regulator deals exclusively with ICTs and broadcasting (see Figure 84). Historically, these two areas have evolved in parallel and it can reasonably be assumed that cross-sector collaboration is an established practice in such authorities. Formal agreements have been established in a dozen countries and joint committees or programmes in a further eight countries. Informal collaboration is, as in most other areas, more often practiced than formal, with a sixth of regulators worldwide collaborating on their own initiative and exceeding their job requirements.

Regrettably, a fifth of countries worldwide do not currently benefit from cross-sector collaboration in the area of broadcasting. This is, nevertheless, the second lowest ratio compared to the other key cross-cutting areas discussed here.

Regional practices vary widely with regard to the institutional set-up for broadcasting regulation and actual collaboration practices. In the Americas, two-thirds of countries have a converged regulator dealing exclusively with broadcasting and ICTs, compared with only a sixth of European countries

(see Figure 85). This is also the case in a third of countries in Africa and Asia-Pacific and none in Arab States and CIS. Formal agreements are most popular in Europe, where a sixth of ICT regulators have signed an MoU with their broadcasting peers, likely as a substitute for the relatively low number of converged regulators in the region.

Across all regions, informal collaboration is the norm. A third of European countries, a fifth of African countries and Arab States and a tenth of CIS and Americas countries are relying on informal collaboration for designing regulatory rules and enforcement. Africa is the region with the highest ratio of joint programmes or committees, established in a tenth of countries. Asia-Pacific is the region with the lowest level of regulatory collaboration in broadcasting – only 5 per cent of countries collaborate although in over 60 per cent of countries there is scope for collaboration.

In the area of informal collaboration, ICT and broadcasting regulators have been involved to varying degrees and on a wide array of issues. In Burkina Faso, the ICT and media regulators have collaborated on a joint awareness raising campaign for better use of media by citizens.[40] In Mauritius, ICTA and the Independent Broadcasting Authority (IBA) have conducted a joint study on the state of digital television migration.[41] In Turkey, the broadcasting authority is required by law to notify the ICT regulator about cases of suspension of broadcasters.[42]

In some countries, ICT and broadcasting regulators have worked together on major regulatory projects. In Nigeria, the Nigerian communications commission and the National broadcasting corporation have collaborated in the process of analogue to digital migration.[43] In Slovakia, the Regulatory authority for electronic communications and postal services, RÚ, is in charge of updating the plans for utilization of the broadcasting spectrum every two years in cooperation with the Council for broadcasting and retransmission, RVR.[44] Informal regulatory collaboration in the field of broadcasting is also practiced in France, Iran and Kuwait.

Joint programmes or committees exist in Croatia, Lithuania and Malta bringing together sectoral authorities and building a coherent, holistic framework for electronic communications and broadcasting services.

It is worth noting that the same activities may be the focus of regulatory collaboration in the area of broadcasting under either informal or formal collaboration schemes. In Romania and Sweden, the ICT and the broadcasting regulators work together in granting licences for broadcasting services,[45,46] through informal collaboration.[47] In Morocco, a broad formal agreement for collaboration has been signed in 2006 between ANRT, the ICT regulator, and HACA, the broadcasting regulator, also covering licensing issues; the MoU has been revised and collaboration reinforced in 2017.[48]

Figure 85: Canvas for collaboration between ICT and the broadcasting regulators, by region, 2018
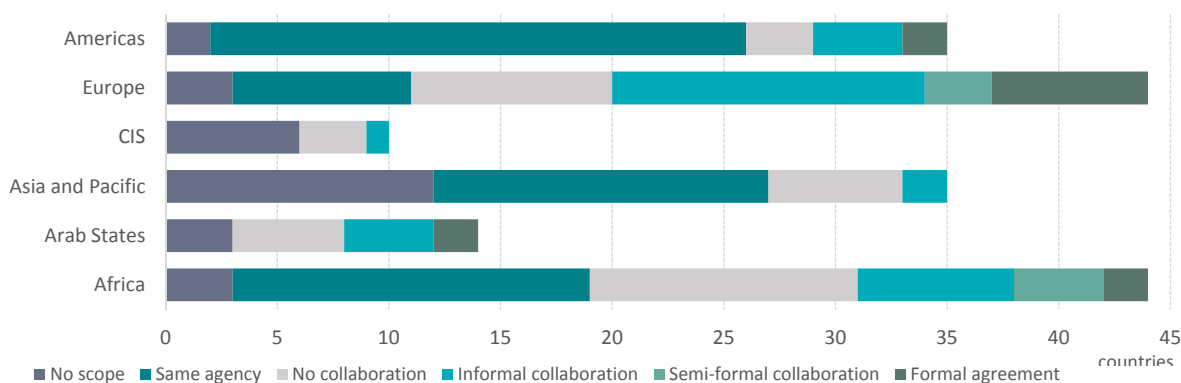
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 184 countries.
2) The research covered 195 countries; no data is currently available for 11 countries.
Source: ITU

Formal collaboration, nevertheless, remains much less used in broadcasting than informal and mainly G4 countries fall in this category. In Montenegro, mechanisms for regulatory collaboration in the area of broadcasting are prescribed by the national laws on electronic communications, electronic media and digital broadcasting.[49] In UAE, the National media council has been building partnerships with various institutions, including the Telecommunications regulatory authority (TRA), to create an integrated media environment meeting world standards.[50] The regulators in Albania, Brazil and Rwanda are also routinely collaborating in a formal framework.

High-profile national institutional structures have been established in a handful of countries as a central place for regulatory collaboration in view of ensuring policy harmonization. In the Netherlands, the Authority for Consumers and Markets, also the ICT regulator, and the Dutch Media Authority share membership in the Consultation forum of regulatory bodies since 2009, in addition to cooperation protocols.[51] In Viet Nam, the Ministry of information and communications acts as umbrella structure that coordinates autonomous agencies, such as VNTA and the Authority for broadcasting and electronic information.[52] Going a step further, the ICT regulator of Bosnia and

Herzegovina and the broadcasting authority of Serbia have signed an MoU to recognize the value and give a higher status to their collaboration.[53]

With the convergence of technologies, institutions and regulation, regulatory collaboration in the area of broadcasting will remain key to delivering safe, secure and varied content to consumers worldwide. Taking collaboration to the next level and building strategic institutional partnerships will ensure a more consistent regulatory environment for broadcasting and electronic communications providers and provide a better regulatory shield for consumers.

Although the ITU World Radiocommunication Conference 2019 (WRC-19) has no agenda items related to digital broadcasting or the digital dividend, an agenda item is proposed for WRC-23 that refers to the UHF band,[54] which is likely to affect both digital broadcasting and the digital dividend. The global multi-stakeholder debate will help influence the direction that digital broadcasting will take in the future.

5.8. Power coupling: the ICT regulator and the spectrum regulator

Mobile broadband made history by connecting billions of people to the Internet, and ultimately to governments, customers, patients and more broadly to each other. Mobile technologies are reshaping economies and societies and their impact is valued in billions of dollars annually (see also section 2.1 on the impact of broadband). Likewise, so is radio spectrum.

There are many concerns related to spectrum management: promoting spectrum access and efficient use; resolving conflicting demands; managing change; enhancing coordination and avoiding interference; fostering communication and consultation; and ensuring that data and information are shared (see also Box 30).[55]

Policy-makers and regulators have been focusing on spectrum regulation, seeking to strike a balance between the certainty needed to ensure stable roll-out of services on one hand and, on the other, flexibility (or light-handed regulation) leading to improvements in cost, services and the use of innovative technologies.[56] With convergence becoming prevalent in both digital markets and regulation, spectrum management decisions could

have even greater impact on market dynamics and consumers' welfare.

While the task is daunting, regulatory collaboration in this area is more within reach than in others. Historically, spectrum management regulation has been combined with ICT and broadcasting regulation, and the three functions have evolved in dynamic interplay for over two decades. Spectrum has traditionally been seen as a prime area for government regulation, subject to rigorous regulatory oversight and multiple layers of rules and regulations. Although this vision of spectrum management is bound to evolve towards more agile, open and efficient regulatory principles, it is likely to remain a key focus of converged regulation – and regulatory collaboration – for years to come.

Our research found that in three-quarters of countries, spectrum allocation and assignment is the responsibility of the ICT regulator (see Figure 86). Institutional unity is a sound basis for fluid, genuine collaboration which is also likely to move more quickly. The high policy priority given to spectrum with the sustained evolution of mobile broadband technology from 3G to 4G and, imminently, to 5G, can drive collaboration. It is difficult to imagine how complex, politically-sensitive issues such as spectrum allocation and assignment can be regulated in silos. Indeed, this is

---

Box 30: Spectrum management : regulatory functions

Core spectrum regulatory functions include:

- Spectrum planning of the future steps required to achieve optimal spectrum use, by charting the major trends and developments in technology and considering the needs of current and future users of the radio spectrum.

- Spectrum engineering, including the evaluating of information, capabilities and technology choices to support decisions affecting the allocation, allotment and assignment of radio spectrum. Identifying solutions to interference problems and technical compatibility among radio systems are key areas of focus.

- Spectrum authorization involves licensing of radiocommunication equipment and the assigning of frequency.

- Spectrum monitoring and compliance activities help by avoiding incompatible frequency usage and through identification of sources of harmful interference.

Source: ICT Regulation Toolkit

the case of only one per cent of countries globally, by far the lowest ratio across all areas discussed here.

In slightly more than 10 per cent of countries, separate spectrum agencies have been given a spectrum management regulatory function. Our research finds that the mandates of the ICT regulator and the spectrum agency overlap in only six countries, including Algeria and Viet Nam. Nevertheless, all spectrum agencies are reportedly engaged to a certain degree in collaboration with the ICT regulator to a certain degree. Such collaboration is predominantly informal as in the case of Colombia, Greece and Latvia; however, in countries such as Gabon, Jamaica and Togo, it is formalized by an MoU between the regulators.[57]

Patterns of collaboration in the area of spectrum are global rather than regional. In all regions, the large majority of countries have appointed the ICT regulator to lead spectrum management allocation and assignment, consistent with the worldwide trend (see Figure 87). Informal collaboration is most practiced in Europe, which is also the region with the highest number of spectrum agencies (seven), followed by the Americas and CIS.

Different institutional patterns have shaped regulatory collaboration in the area of spectrum management. In some countries, the spectrum agency makes allocations of frequency bands to the ICT regulator, which then assigns them to ICT operators; the agencies collaborate in the process on an informal basis. This is the case of Algeria,

Figure 86: The state of regulatory collaboration between ICT and spectrum regulators, worldwide, 2018
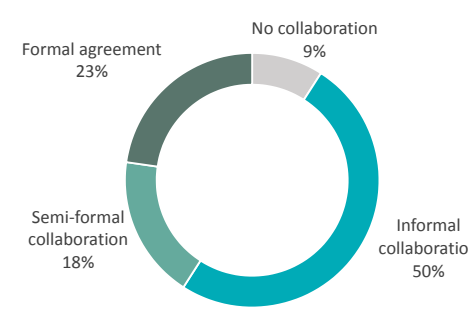
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 22 countries where ICT and spectrum regulators exist.
2) In 140 countries, spectrum management and ICT regulation fall under the mandate of a multi-sector regulator.
3) In 21 countries, there is currently no scope for collaboration.
4) The research covered 193 countries; no data is currently available for 10 countries.
Source: ITU

Czech Republic, Costa Rica and Côte d'Ivoire.[58] In other countries, the spectrum agency has the exclusive authority to allocate and assign radio frequency spectrum to the government, ICT service providers and broadcasters, in informal consultation with the ICT regulator. This is the institutional practice in Pakistan.[59] Yet elsewhere, there is clear division of responsibilities in the mandates of the two agencies. In the US, FCC, the ICT regulator, administers spectrum for non-federal use[60] and works in conjunction with the

Figure 87: Canvas for collaboration between ICT and spectrum regulators, by region, 2018
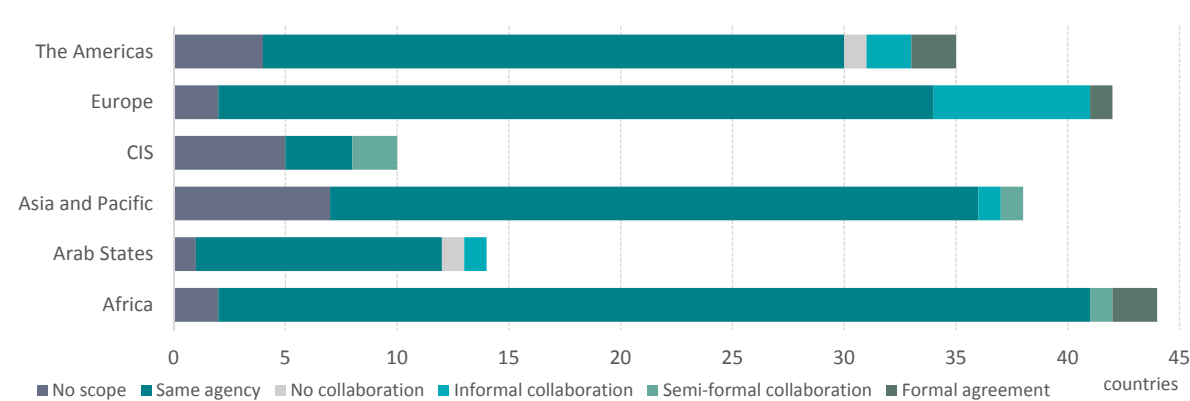
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 183 countries.
2) The research covered 193 countries; no data is currently available for 10 countries.
Source: ITU

National telecommunications and information administration (NTIA) operating under the Department of Commerce, which administers spectrum for federal use.[61,62]

Formal collaboration in the area of national spectrum management is yet to become mainstream. Nevertheless, a handful of countries are leading the way. In the Netherlands, the Authority for consumers and markets, the College of the independent post and telecommunications authority (OPTA) and Agentschap Telecom, part of the Ministry of Economic Affairs, have committed in an MoU to make every effort to support and strengthen each other and take their collaboration beyond the exchange of information and use it to enhance regulatory outcome.[63]

In Russian Federation, the State commission for radio frequencies is an inter-agency coordination body under the Ministry of communications and mass media with full authority in regulation of radio spectrum while Roskomnadzor is a federal executive authority in charge of spectrum licensing and supervision of ICT services.[64] The agencies collaborate informally on an ongoing basis on a range of spectrum-related issues.

In many countries, ICT and spectrum regulators may decide to cross paths in order to prepare together for the introduction of 5G in national markets. In France, ARCEP and ANFR, the spectrum

regulator, have been reviewing together the terms and conditions of use for unlicensed bands,[65] to increase power ratings and duty cycles.[66]

With expected 5G roll-out and anticipated deployment of massive IoT commercial services and applications, spectrum reallocation and optimization will remain a major focus for spectrum managers. Since such services and applications cut across adjacent areas – importantly, competition and consumer protection – collaboration with the relevant regulatory sources of expertise will intensify. Regulatory collaboration within converged agencies and among sectoral authorities will be driven by economic, social and political incentives.

Looking at 2019, the expected outcome of WRC-19 is the identification of globally harmonized frequency bands above 6 GHz for 5G. Besides the work of the conference, the ITU-R Working Party 5D (IMT Systems) is currently standardizing 5G systems and the work should be completed by 2020. Like for digital broadcasting, the global multi-stakeholder debate will help shape the direction that spectrum management will take in the future.

5.9. Power coupling: the ICT regulator and the agency responsible for Internet-related issues

Internet has become perhaps the most characteristic phenomenon of the new millennium, feeding into virtually all areas of our economies, societies and lives and cutting across sectors and geographies. But its regulation hasn't – and considering the major role it has played in the vast digital transformation of the past two decades, many aspects of the Internet remain largely under-regulated. Compared with other major sectors of national economies such as finance and energy, regulatory frameworks tackling fundamental issues related to the Internet such as Internet content and the protection of consumers of digital services have been globally less common, lighter, less intrusive and with less enforcement. This, arguably, has allowed Internet to take up and disrupt traditional business models and services. In many countries, Internet services are subject to existing general laws relating to electronic communications; in others, regulatory frameworks for the Internet are only now starting to take shape on issues such as protection of personal data and net neutrality.

The maturing of the Internet, on one side, and the growing number of documented questionable practices of Internet players, on the other, build the case for sturdier rules and enforcement. Initially, the benefits of global digital platforms clearly outweighed the risks; now however, calls for tighter regulation have become stronger. Such a regulatory perspective would seek to guarantee that the Internet remains an enabler of welfare and progress. While there seems to be a legitimate case for more consistent regulation in order to reduce regulatory arbitrage, it is less obvious that we need more or tighter regulation. The global debate evolves – and so far national regulatory frameworks have been slow to respond to market realities.

Although aspects of Internet regulation are part of the mandate of three-quarters of ICT regulators (see Figure 88), the Internet portfolio of the majority of them remains slim. Our research shows that not all Internet issues are specified under the mandate of the ICT regulator, and in many cases, ICT regulators are only minimally involved. This low degree of involvement is <u>not</u> consistent with the high level of ICT regulator involvement in key

digital markets such as broadband infrastructure, competition and market entry. There has been much recent debate about the importance of a holistic approach to regulating digital markets. Holistic regulation that is both consistent and sound can help ensure delivery of reliable, affordable, safe and varied digital services to consumers.

The main challenge is to reconcile telecom regulatory policies and those governing digital markets. The historically well-structured, comprehensive regulatory frameworks for telecom services stops short of addressing some of the new issues brought about by digital platforms. Currently, there is a two-speed regulatory track in many countries for operators and digital players, and the latter have enjoyed a competitive advantage while spurring innovation and unleashing new consumer experiences. The level playing field has been disrupted and requires a new regulatory balance. Too much regulatory scrutiny might stifle innovation and investment and ultimately make digital markets worse off. Keeping the current laissez-faire regulatory approach might, on the other hand, worsen market tensions and impact consumers negatively. So instead, governments need to think of measures that regulators can take only if and when market failures arise. This muted regulatory

Figure 88: The state of regulatory collaboration between the ICT regulator and the agency in charge of Internet-related issues, worldwide, 2018
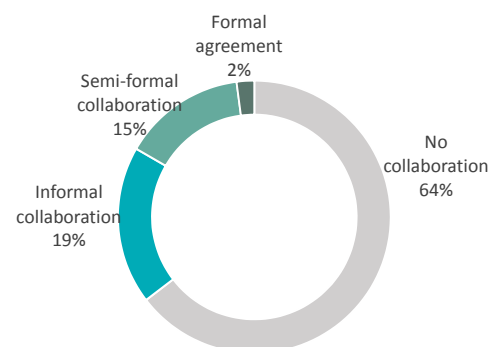
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 8 countries where ICT and Internet regulators exist.
2) In 120 countries, Internet, in general terms, and ICT regulation fall under the mandate of a multi-sector regulator.
3) In 21 countries, there is currently no scope for collaboration.
4) The research covered 195 countries; no data is currently available for 6 countries.
Source: ITU

approach can provide fixes to specific market issues without overburdening entire industries (see also the discussion on muted regulation in section 4.4). Fast-changing digital markets call for a dynamic regulatory touch led by market failures and success.

Regulatory collaboration seems the natural path to address regulatory treatment of Internet services and digital players. Who needs to be involved to arrive at a holistic view of issues, while pooling the expertise to tackle some of the most complex, high-impact regulatory decisions? Specialized agencies in charge of regulating different aspects of Internet have been created in more than 115 countries worldwide, as of 2018 (see Figure 19).

Computer Incident Response Teams (CIRTs) are operational in 104 countries worldwide, such as in Montenegro, Sudan, the Philippines, Tanzania and Venezuela,[67] and national cybersecurity agencies with a broader mandate exist in at least of a dozen more countries, including in Albania and Indonesia. Some of the day-to-day Internet business management activities have been outsourced to the private sector.[68] In over 70 countries, there are multiple national ICANN-accredited registrars for Internet domain names. In Guatemala, Universidad del Valle de Guatemala, a private university, has been mandated by the Government to handle domain names registration.

In a handful of countries, the mandate of specialized government agencies cover multiple areas. In Estonia, the Information System Authority is responsible for public key infrastructure (PKI) and cybersecurity and the French CNIL (Commission Nationale de l'Informatique et des Libertés) has a dual mandate for data protection and other consumer protection issues related to social media and online advertising.

A few countries have further integrated Internet issues into a holistic national framework by expanding the mandate of key national cross-sector agencies and laying the ground for a consistent, comprehensive approach to Internet-related issues in the national context. In Croatia, the State Intellectual Property Office handles various issues related to online services. Similarly, the National Security Authority is also dealing with cybersecurity. In Sweden, the Swedish Civil Contingencies Agency (MSB) responsible for issues concerning civil protection, public safety, emergency management and civil defense can also handle issues related to the Internet as long as no other authority has been given jurisdiction.

Of those specialized agencies dealing with specific Internet issues, more than half do not collaborate with ICT regulators (see Figure 88). Only 17 countries have established institutional mechanisms for collaboration between the agency in charge of Internet-related issues and the ICT regulator. Only one country, Romania, has formalized this cooperation.

Figure 89: Canvas for collaboration between and ICT regulator and the agency responsible for Internet-related issues, by region, 2018
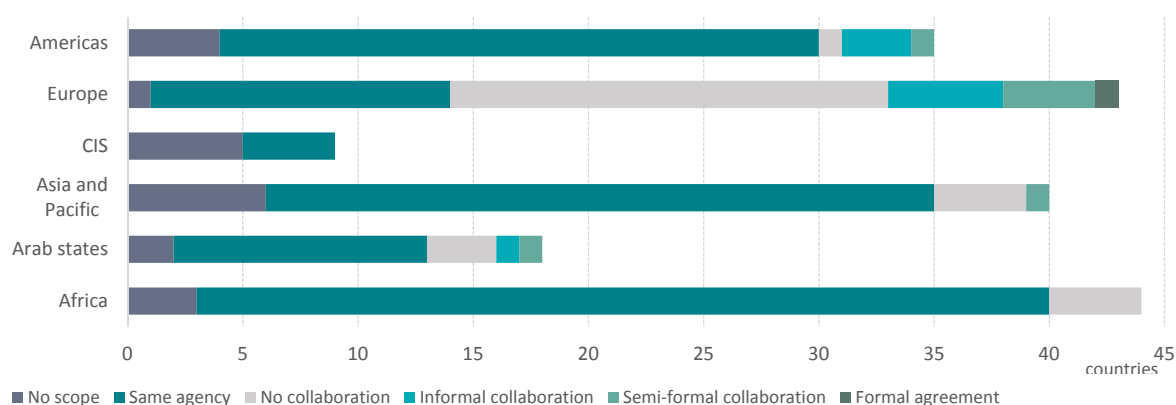
Legend: See Box 26 (Degrees of collaboration explained)
Data notes:
1) The graph is based on data for 189 countries.
2) The research covered 195 countries; no data is currently available for 6 countries.
Source: ITU

In a nutshell, it appears that very few national regulatory agencies worldwide have the institutional capacity and collaborative outreach to formulate Internet rules. Europe is the region with a largest number of collaborating agencies (ten countries, see Figure 89), although it is also the region with the greatest scope for collaboration since regulators in 17 countries still do not collaborate with their Internet counterparts. Regulatory collaboration in the other regions is nascent and mainly informal at this stage.

A major question for governments will be whether it makes sense to create separate agencies in charge of Internet-native issues, and which would collaborate with ICT regulators on core issues related to broadband infrastructure, sector structure and openness, among others. Alternatively, the mandate of existing ICT regulators could be reinforced in order to elect national regulatory champions dealing with all, or at least some, aspects of digital markets. The

gains in terms of regulatory harmonization and simplicity deserve further thought. Both scenarios could provide viable mechanisms to fill in the gaps and enhance the consistency of current regulatory frameworks. New regulatory models could also emerge in the coming years. Collaboration will need to be extended across the board and involve a range of sector authorities, such as the competition and consumer protection authorities. The greater involvement of digital players in the regulatory process must be accelerated. Collaborative regulation and its well-appointed toolbox can pave the way forward in regulating in the digital transformation era.

It is clear that rethinking existing regulatory perspectives on the Internet and redefining regulatory collaboration in this area are both key to taking Internet to the next level – to the Internet for social and economic good, and one which will help bring the Sustainable Development Goals within reach.

5.10. Collaborative regulation worldwide – medal winners and missed opportunities

All indications emphatically underline that we need more collaboration – better channels and more bandwidth. Although there has been unequivocally agreement on the benefits of collaboration, progress has been stalled by power battles, lack of resources and misconceptions. In 2019, we will investigate the causes of this limited take-up of collaboration and its impact. However, we have a pressing message for regulators across the board: solid progress towards inclusive and collaborative regulation is needed for the good of all users of digital services, now and into the future.

In preparing this report, we conducted extensive research and have had direct contact with

---

Box 31: Which countries are leading the way in shaping digital markets through regulatory collaboration?

As one might expect, such countries include regional leaders and those countries already categorized as G4, or on the verge of attaining this level:

- Botswana, Burkina Faso and Malawi, three African countries in the regional top 5 have established collaboration practices, including formal collaboration, involving single-sector and multi-sector regulators.

- In Brazil and Chile, informal regulatory collaboration enriches no fewer than five areas from competition to energy, and underpins a national network for policy-making.

- Regulators in Jamaica and the US enjoy more formal regulatory collaboration in at least half of the eight areas in our research.

- Some regions offer a more diverse though very positive picture of regulatory collaboration: Sudan and UAE (both G3 regulators) join Morocco and Oman (G4 regulators) as leaders in collaboration.

- Armenia is the only CIS country engaged in regulatory collaboration across several areas.

- All top 5 countries in Asia-Pacific have a consistent record of informal regulatory collaboration in half of the researched areas. Beyond these countries however, little collaboration is occurring.

- Europe is the most advanced region in regulatory collaboration, with 29 countries engaged in some form of collaboration. In France and Spain, the ICT regulator is involved in collaboration in seven areas while the vast majority of European regulators cover four or more areas. From Bosnia and Herzegovina to Ireland and from Malta to Turkey, various regulators and country sizes engage in collaboration, making a strong case for the benefits it can deliver.

- The Netherlands and Norway set the gold standard in 2018 and top the global list for regulatory collaboration, covering most areas and with formal mechanisms in place.

- Our extensive research and analysis show that countries in G1 and G2 categories generally do not engage in collaboration, and those in the G3 category are rare. G4 countries engage far more in collaboration across all regions, and point the way forward to G5, wholly collaborative regulation.

Source: ITU

---

regulators. We gathered conclusive evidence on the breadth and depth of regulatory collaboration. Our findings are helpful in drawing the global map of regulatory collaboration, allowing us to pinpoint achievements and gaps – and help provide guidance on where to concentrate efforts and resources. The evidence also makes the case for sound collaboration across governments.

The critical threshold of regulatory collaboration today covers between 10 and 40 per cent of existing ICT regulators, depending on the thematic area (see Figure 90).

Areas where collaboration is thriving include consumer protection, competition and broadcasting, where there is a long-standing record of shared challenges and regulatory thinking. These three agencies together with the ICT regulator, to borrow an analogy from the Olympics, take the gold medal in regulatory collaboration.

In regard to spectrum, collaboration has occurred mainly as a matter of internal policy, since 85 per cent of ICT regulators also have a role in national spectrum management. Collaborating on spectrum may be a useful model for developing a shared approach to Internet-related issues, since three-quarters of ICT regulators are eligible to regulate aspects of the Internet – although at this time, the majority have not taken up this mandate. Both agencies, jointly with the ICT regulator, take the silver medal in making progress on our shared journey towards improved digital markets.

In regard to data protection, just over 30 countries have seen collaboration between the specialized authority and the ICT regulator. Conversely, around half of countries have yet to establish a data protection authority, an absolute pillar of digital markets and societies. Collaboration between energy and ICT regulators remains rare too, despite the possible synergies and efficiencies – it is however worth noting in this context that

Figure 90: The state of regulatory collaboration in 2018, by area

Competition
29
38
54
63
Total: 184 countries

Consumer protection
3
78
35
66
Total: 182 countries

Data protection
7
104
39
33
Total: 183 countries

Financial
8
123
49
Total: 180 countries

Broadcasting
29
38
54
63
Total: 184 countries

Spectrum
21
2
20
140
Total: 183 countries

Internet
21
31
6
120
Total: 178 countries

Energy
18
58
91
25
Total: 192 countries

Legend:
■ No institutional setup
□ Do not collaborate
■ Collaborate
■ Same agency

Legend:
No institutional set-up = no ICT regulator or a specialized agency in the focus areas, or either
No collaboration = no track for regulatory collaboration between the ICT regulator and sector-specific or multi-sector regulators
Collaborate = a total figure for countries engaged in some form of collaboration (informal, semi-formal or formal)
Same agency = the ICT regulator is part of a converged or multi-sector regulator
Note: Figures give the number of countries in each category.
Source: ITU

over a quarter of countries worldwide have neither an ICT or energy regulator, reducing the scope of collaboration. Nevertheless, progress has occurred over the past couple of years and recent joint projects deserve an encouraging bronze medal.

Finally, no medal is deserved in the area of digital financial inclusion, with grave impact on those at the bottom of the pyramid. Although there are positive developments, many challenges remain. The institutional set-up in this area has been mature for a long time and financial regulators outnumber even their ICT peers. Despite this fertile ground for collaboration however, those who collaborate are two and a half times fewer than those who do not. As a result, 123 countries have missed out on their 'M-Pesa opportunity' due to a lack of regulatory collaboration.

We hope that this stocktaking of collaborative practices in ICT regulation will help inform and ignite the global debate on collaboration, and will provide an evidence-based blueprint for decision-makers as they formulate policy for the decades ahead. Our worldwide mapping should help facilitate reflection on collaboration as a powerful means for enabling digital markets that are safe, competitive, accessible and efficient – and at the same time addressing the inadequacies of silo and legacy regulation.

Collaboration is without doubt a central element in facilitating digital transformation across all economies. With almost half of the world's population remaining beyond digital reach, policy-makers everywhere – and particularly those in G2 and G3 countries – need to embrace collaborative regulation and make strides towards achieving the Sustainable Development Goals.

A refined view of regulatory collaboration and its impact on innovation and market development will be featured during the next Global Symposium for Regulators (GSR), to be held 9-12 July 2019 in Vanuatu.

Endnotes

1   Opengov Asia (2018): https://www.opengovasia.com/singapore-government-launching-centralised-api-exchange-for -convenient-and-secure-inter-agency-data-sharing/

2   Or 6 per cent of countries having both an ICT and a data protection authority.

3   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

4   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

6   https://www.rtr.at/en/tk/TKG2003/Telecommunications_Act_2003__unofficial_.pdf

7   https://www.dataguidance.com/ghana-ncas-revised-unsolicited-communications-code-requires-work/

8   https://www.nst.com.my/news/nation/2017/10/295269/joint-effort-track-down-those-behind-personal-data-leak-online

9   https://www.lexology.com/library/detail.aspx?g=b0d59778-e917-45f5-aaf0-1d89f03e27a0

10   See, for example, the GSR16 Best Practice Guidelines on Collaborative Regulation for Digital Financial Inclusion: https:// www.itu.int/en/ITU-D/Regulatory-Market/Pages/bestpractices.aspx

11   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

12   Arab States are not counted here because of the very high proportion of countries with unavailable data.

13   http://www.angop.ao/angola/pt_pt/noticias/economia/2017/5/26/Angola-BNA-Ministerio-das-telecomunicacoes -assinam-acordo-cooperacao,64a806e2-5561-4a20-bc7d-2ab52b9a1645.html

14   https://www.balancingact-africa.com/news/telecoms-en/21148/bank-of-tanzania-tcra-partner-on-mobile-phone-cash -transfers-control-in-tanzania

15   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

16   https://www.theedgesingapore.com/consortium-led-imda-mas-skillsfuture-sign-agreement-tesa-fintech-collective, also http://fst.net.au/news/mas-urges-retailers-embrace-qr-payments

17   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

18   http://www.finmark.org.za/wp-content/uploads/2016/01/Rep_RPSMMZ_Moz07121.pdf

19   https://www.infomediaire.net/paiements-mobile-un-nouveau-marche-de-400-mmdh-au-maroc/

20   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

21   https://www.nca.org.gh/assets/Uploads/Press-Release-2018-World-Telcom-Day-Marked.pdf

22   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx

23   http://www.intelligentsia-consultants.com/docs/National_ICT_sector_and_Policy_Appraisal_Report_BELARUS_Dec10 .pdf

24   http://home.saic.gov.cn/gkml/auto3743/auto3753/201709/t20170918_269181.html

25   http://www.ca.go.ke/index.php/component/content/article/94-news/269-ca-cbk-approves-use-of-thin-sim-technology-in -kenya

26   World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/ RegulatorySurvey.aspx https://www.centralbank.org.ls/images/Financial_Stability/Policy_Framework/Mobile_Money _Guideline_2013.pdf

27   http://www.uncdf.org/article/1679/sierra-leone-launches-the-digital-financial-services-working-group--migration

28   https://news.bitcoin.com/korean-regulations-policy-easing-crypto-classification-central-bank-report/

29   Bangladesh Financial Intelligence Unit, AML/CFT Regulations for Mobile Money: Policy Options for Bangladesh: https:// www.bb.org.bd/pub/research/sp_research_work/srw1704.pdf

30   Bangladesh Financial Intelligence Unit, AML/CFT Regulations for Mobile Money: Policy Options for Bangladesh: https:// www.bb.org.bd/pub/research/sp_research_work/srw1704.pdf

31   World Telecommunication/ICT Regulatory Survey 2018

32 https://www.government.se/49b758/contentassets/f496d0e0cc864e8fa57b22ea247a829e/report-ict-and-energy-efficiency-in-sweden

33 http://documents.worldbank.org/curated/en/133611468770358510/Ecuador-Power-and-Communications-Sectors-Modernization-and-Rural-Services-Project

34 http://www.regulatel.org/wordpress/wp-content/uploads/2015/05/Pro_competitive_electronic_communications_Alemania.pdf

35 OECD (2014): http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/RPC/NER(2014)6&docLanguage=En

36 World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx

37 Based on ITU, "Digital Dividend: Insights for spectrum decisions", 2018

38 Based on ITU, "Digital Dividend: Insights for spectrum decisions", 2018

39 2017 ITU World Telecommunication/ICT Regulatory Survey

40 https://docplayer.fr/25160608-Campagne-d-education-aux-medias-pour-une-meilleure-utilisation-des-medias-par-les-citoyens.html

41 https://www.icta.mu/mediaoffice/2013/DTT_migration.htm

42 https://www.rtuk.gov.tr/en/audio-visual-media-law/5350/5139/the-law-no6112-on-the-establishment-of-radio-and-television-enterprises-and-their-media-services-march-3-2011.html

43 https://itpulse.com.ng/2018/07/05/internet-nig-exco-pays-courtesy-call-on-ncc-others/

44 https://medialandscapes.org/country/slovakia/policies/regulatory-authorities

45 http://www.ancom.org.ro/en/radio-spectrum_2749

46 https://www.mprt.se/Documents/Tillst%C3%A5ndsprocesser/Analog%20kommersiell%20radio%202018/Strategy%20for%20the%20Authoritys%20licensing%20for%20analogue%20commercial%20radio%202018-2026.pdf?epslanguage=en

47 World Telecommunication/ICT Regulatory Survey 2018

48 http://www.leseco.ma/maroc/60439-haca-anrt-les-deux-regulateurs-cherchent-un-nouveau-cadre-de-coordination.html

49 World Telecommunication/ICT Regulatory Survey 2018

50 http://www.nmc.gov.ae/ar-ae/NMC/Pages/Our-Partners.aspx

51 World Telecommunication/ICT Regulatory Survey 2018

52 World Telecommunication/ICT Regulatory Survey 2018

53 http://www.ratel.rs/upload/RATEL_-_Annual_Report_2016.pdf

54 "to review the spectrum use and spectrum needs of existing services in the frequency band 470-960 MHz in Region 1 and consider possible regulatory actions in the frequency band 470 694 MHz in Region 1 on the basis of the review in accordance with Resolution 235 (WRC 15)"

55 ICT Regulation Toolkit: http://www.ictregulationtoolkit.org/toolkit/5.8

56 http://www.ictregulationtoolkit.org/toolkit/5.8

57 World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx

58 World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx

59 World Telecommunication/ICT Regulatory Survey 2018, http://www.fab.gov.pk/category/functions

60 e.g., state and local government, commercial, private internal business use, and personal use

61 e.g., use by the military, the Department of Justice

62 World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx

63 https://zoek.officielebekendmakingen.nl/stcrt-2015-7210.html

64 World Telecommunication/ICT Regulatory Survey 2018, https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx

[65]   870- 876 MHz and 915- 921 MHz bands

[66]   https://www.arcep.fr/uploads/tx_gspublication/white_paper_IoT-02-orientations-071116-eng.pdf

[67]   ITU (2018): https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf

[68]   ICANN (2018): https://www.icann.org/registrar-reports/accredited-list.html

6. Closing remarks

This edition of the Global ICT Regulatory Outlook is a snapshot of how regulation is working in markets in the midst of digital transformation. We hope that it provides insight, inspiration and informed analysis that can help address the challenges ahead.

Our research throws up as many questions as it answers. What should we focus on in regulation? What tools can replace those that have failed? Should we regulate simply because we can? Should we opt for light regulation and fall in behind the mantra of 'less-is-more'? We will continue to seek answers, knowing that more questions will come in this ever-changing, fast-paced digital world.

Diversity and harmonization have been the yin and yang of regulation since the era of the telegraph. Regulatory response has driven the rise and fall of technologies – and arrivals and departures of market players. The pursuit of harmonization across geographies, market players and sectors has enabled the global digital transformation. But the chacteristics of diversity and harmonization change over time, driven by technology and its impact on economy and society. One constant element remains unaffected – the human being in the midst of the change – and the focus is increasingly on providing maximum benefit while minimizing adverse effects.

The digital world is one in which opportunities and challenges multiply exponentially. How can regulation keep pace with markets and with consumer needs?

Based on our evidence, analysis and intuition, we argue that the following five vectors will define the future of regulation – embodied in the 5th generation of regulation:

- **Holistic reach for greater impact**: silo-style ICT sector regulation isn't viable in the digital world. G5 regulation will mirror the interplay between digital infrastructure, services and content across industries and national borders. What drives G5 is the impact of enforced rules based on a sound understanding of the realities of digital markets and the linkages among industries.

- **Adaptive, agile focus**: Rather than the traditional focus on specific issues or players, G5 regulation will strive to troubleshoot and repair market failures or gaps in consumer protection 'on the go'. G5 rules will not be less precise, but they will vary according to context and market behaviours, leveraging muted regulatory response only when and where it is needed.

- **Trust-based compact**: Trust will be the glue of G5 teams and the guarantee for success of regulatory response. Trust among regulators and the regulated is not negotiable and makes the traditional hierarchy fade. It is the beginning of a more positive, more equal relationship built on shared values, transparency and a new generation of incentives.

- **Participative leadership**: G5 is about leadership, not about command. It requires an active, open attitude since G5 regulators cannot afford to stand still. They are in need of expression that can speak loudly when necessary or keep its counsel, too. G5 regulators are the trailblazers of the digital transformation.

- **Collaboration is the leading vector**, the transformer of regulation into G5. Broad and constant collaboration, structured and unstructured, is essential for ensuring that regulation makes sense and can deliver positive market and consumer outcomes. Everyone has a seat at the consultation table, from government sector and multi-sector regulators to all breeds of market players to consumer associations. Although government agencies will remain in the driving seat, contributions from all parties are of value in the quest to find the shortest, least challenging path to the digital future.

Looking ahead, the 2019 edition of the Global ICT Regulatory Outlook will continue to explore the 5th generation of regulation – collaborative regulation – spelling out for the first time the tools, repair strategies and new regulatory techniques available under this umbrella concept. As always, it will continue to take the pulse of regulatory collaboration across the world.

NOTE ON METHODOLOGY – ICT REGULATORY TRACKER

What is the ICT Regulatory Tracker?

The ICT Regulatory Tracker is an evidence-based tool to help decision-makers and regulators make sense of the rapid evolution of ICT regulation. The Tracker enables various analytical features to pinpoint the changes taking place in the ICT regulatory environment. Using both quantitative and qualitative data, the Tracker makes possible benchmarking and the identification of trends in ICT legal and regulatory frameworks. It likewise helps identify the gaps in existing regulatory frameworks, making the case for further regulatory reform towards achieving a vibrant and inclusive ICT sector.

Scope

The ICT Regulatory Tracker is composed of a total of 50 indicators (11 composite, see full list in Table 23) grouped into four pillars (see also Table 22):

1) the regulatory authority (focusing on the functioning of the separate regulator),

2) regulatory mandates (who regulates what),

3) the regulatory regime (what regulation exists in major areas) and

4) the competition framework in the ICT sector (level of competition in the main market segments).

Table 22: ICT Regulatory Tracker structure and scoring, 2007-2017

Pillar	Name	Number of indicators	Max score	Countries ranked if min indicators
1	Regulatory authority	10	20	3
2	Regulatory mandates	11	22	3
3	Regulatory regime	15	30	4
4	Competition framework	14	28	4
	ICT Regulatory Tracker	**50**	**100**	**14**

Source: ITU

The Tracker is currently available for the period 2007-2017. It covers:

• 187 countries and economies over the period 2007 – 2009;

• 188 countries and economies over the period 2010 – 2013 (adding Solomon Islands);

• 189 countries and economies in 2014 (adding Nauru); and

• 190 countries and economies over the period 2015 – 2017 (adding Somalia).

The full list of countries is available in Annex 1.

Figure 91: Evolution dynamics of the ICT Regulatory Tracker, 2007 – 2017
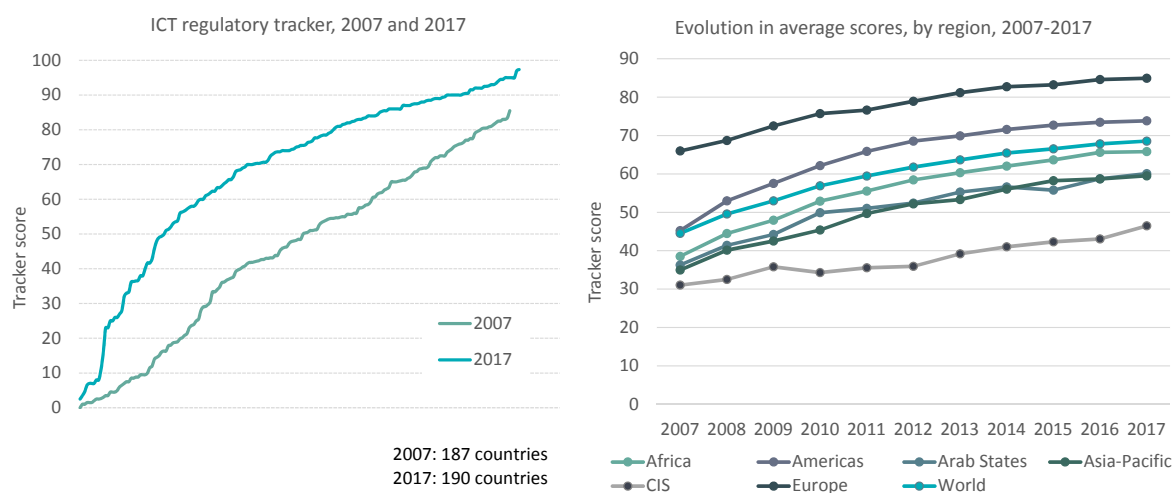
Source: ITU

Data mechanics: coding & scores

After coding the originally qualitative information, all indicators are given a score between 0 and 2. The benchmark for the scoring is what is considered the best possible scenario based on the internationally recognized regulatory best practices that were adopted by the global community of regulators at the annual ITU Global Symposiums for Regulators.

Source of data

The Tracker is based on self-reported information gathered yearly via the ITU World Telecommunication Regulatory Survey and the ITU Tariff Policies Survey as well as desktop research and direct outreach to national telecom/ICT regulatory authorities. For years when questions were left blank or when the survey was not answered by a country, the latest available data for the indicator is retrieved or, whenever possible, data gaps are filled through desktop research based on official sources.

Indicators

The full set of indicators is shown in Table 23.

Detailed methodology

The matrix with the detailed methodology of the ICT Regulatory Tracker is available in Annex 2 and can be downloaded online at itu.int/go/tracker, (About the Tracker). It provides detailed information on the choice, composition and scoring of each indicator.

Table 23: ICT Regulatory Tracker indicators, per pillar

ICT REGULATORY TRACKER	
Pillar 1: Regulatory Authority	1. Separate telecom/ICT regulator
	2. Autonomy in decision-making
	3. Accountability
	4. Percentage of diversified funding
	5. Public consultations mandatory before decisions
	6. Enforcement power
	7. Sanctions or penalties imposed by regulator
	8. Dispute resolution mechanism
	9. Appeals to decisions
	10. Existence of Competition Authority
Pillar 2: Regulatory Mandate	*Who is in charge of regulating the following?*
	11. Quality of Service obligations measures and service quality monitoring
	12. Licensing
	13. Interconnection rates and price regulation
	14. Radio frequency allocation and assignment
	15. Spectrum monitoring and enforcement
	16. Universal service/access
	17. Broadcasting (radio and TV transmission)
	18. Broadcasting content
	19. Internet content
	20. IT
	21. Consumer issues

Table 23: ICT Regulatory Tracker indicators, per pillar (continued)

ICT REGULATORY TRACKER	
Pillar 3: Regulatory Regime	22. Types of licenses
	23. License exempt
	24. Operators required to publish Reference Interconnection Offer
	25. Interconnection prices made public
	26. Quality of Service monitoring required
	27. Infrastructure sharing for mobile operators permitted
	28. Infrastructure sharing mandated
	29. Co-location/site sharing mandated
	30. Unbundled access to the local loop required
	31. Secondary spectrum trading allowed
	32. Band migration allowed
	33. Number portability required from fixed-line operators
	34. Number portability required from mobile operators
	35. Individual users allowed to use VoIP
	36. National plan that involves broadband
Pillar 4: Competition Framework	*Competition exists in the following market segments:* 37. Local and long distance (domestic and international) fixed line services
	38. IMT (3G, 4G, etc.) services
	39. Cable modem, DSL, fixed wireless broadband
	40. Leased lines
	41. International Gateways
	42. Status of the main fixed line operator (public, partially or fully private)
	43. Legal concept of dominance or SMP
	44. Criteria used in determining dominance or SMP
	Foreign participation/ownership in:
	45. Facilities-based operators
	46. Spectrum-based operators
	47. Local service operators/long-distance service operators
	48. International service operators
	49. Internet Service Providers (ISPs)
	50. Value-added service providers

Source: ITU

Figure 92: Generations of regulation in the ICT Regulatory Tracker

Regulated public monopolies– command and control approach

Basic reform – partial liberalization and privatization across the layers

Enabling investment, innovation and access – dual focus on stimulating competition in service and content delivery, and consumer protection

Integrated regulation – led by economic and social policy goals

Openness and Flexibility

G1

G2

G3

G4

ICT Regulatory Tracker
Score breakdown
G1: ≥ 0 <40
G2: ≥ 40   < 70
G3: ≥ 70   < 85
G4: ≥ 85   ≤ 100

Effectiveness

Source: ITU

Generations of regulation

To help analyse the evolution of ICT regulation worldwide, identify progress areas as well as gaps and measure those, the countries included in the Tracker are split into score thresholds that relate to generations of regulation, for any given year.

Using the concept of generations of regulation (see Figure 92), the Tracker can be used to showcase progress within the same country over time, compare between countries and regions or track the ICT regulatory trends in specific areas at the national, regional and global level.

Feedback & contact

If you are an ITU Member State Administration and you wish to provide recent or historic data for your country's ICT regulation, please write to us at treg[at]itu.int.

If you would like to know more about the Tracker or have queries or suggestions, please get back to us at treg[at]itu.int.

ANNEX 1: LIST OF COUNTRIES, ICT REGULATORY TRACKER 2007-2017

Afghanistan	Canada
Albania	Central African Rep.
Algeria	Chad
Andorra	Chile
Angola	China
Antigua and Barbuda	Colombia
Argentina	Comoros
Armenia	Congo (Rep. of the)
Australia	Costa Rica
Austria	Côte d'Ivoire
Azerbaijan	Croatia
Bahamas	Cuba
Bahrain	Cyprus
Bangladesh	Czech Republic
Barbados	Dem. Rep. of the Congo
Belarus	Denmark
Belgium	Djibouti
Belize	Dominica
Benin	Dominican Rep.
Bhutan	Ecuador
Bolivia (Plurinational State of)	Egypt
Bosnia and Herzegovina	El Salvador
Botswana	Equatorial Guinea
Brazil	Eritrea
Brunei Darussalam	Estonia
Bulgaria	Ethiopia
Burkina Faso	Fiji
Burundi	Finland
Cabo Verde	France
Cambodia	Gabon
Cameroon	Gambia

Georgia	Lebanon
Germany	Lesotho
Ghana	Liberia
Greece	Libya
Grenada	Liechtenstein
Guatemala	Lithuania
Guinea	Luxembourg
Guinea-Bissau	Madagascar
Guyana	Malawi
Haiti	Malaysia
Honduras	Maldives
Hong Kong, China	Mali
Hungary	Malta
Iceland	Marshall Islands
India	Mauritania
Indonesia	Mauritius
Iran (Islamic Republic of)	Mexico
Iraq	Micronesia
Ireland	Moldova
Israel	Monaco
Italy	Mongolia
Jamaica	Montenegro
Japan	Morocco
Jordan	Mozambique
Kazakhstan	Myanmar
Kenya	Namibia
Kiribati	Nauru *(since 2014)*
Korea (Rep. of)	Nepal (Republic of)
Kuwait	Netherlands
Kyrgyzstan	New Zealand
Lao P.D.R.	Nicaragua
Latvia	Niger

Nigeria	Sri Lanka
Norway	Sudan
Oman	Suriname
Pakistan	Swaziland (now Eswatini)
Panama	Sweden
Papua New Guinea	Switzerland
Paraguay	Syrian Arab Republic
Peru	Tajikistan
Philippines	Tanzania
Poland	Thailand
Portugal	The Former Yugoslav Rep. of Macedonia
Qatar	Timor-Leste
Romania	Togo
Russian Federation	Tonga
Rwanda	Trinidad and Tobago
Saint Lucia	Tunisia
Saint Vincent and the Grenadines	Turkey
Samoa	Turkmenistan
San Marino	Tuvalu
Sao Tome and Principe	Uganda
Saudi Arabia	Ukraine
Senegal	United Arab Emirates
Serbia	United Kingdom
Seychelles	United States
Sierra Leone	Uruguay
Singapore	Uzbekistan
Slovakia	Vanuatu
Slovenia	Venezuela
Solomon Islands *(since 2010)*	Viet Nam
Somalia *(since 2015)*	Yemen
South Africa	Zambia
Spain	Zimbabwe

ANNEX 2: **DETAILED METHODOLOGY OF THE ICT REGULATORY TRACKER**

1. Regulatory authority

Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
1 Does a separate (independent in terms of finance, structure, and decision making from the operator(s) and the sector Ministry) Regulatory Authority exist for Telecommunication or Information and Communication Technology (ICT) in your country?	**Separate telecom/ICT regulator**	Having a separate Regulatory Authority (i.e. independent in terms of finance, structure, and decision-making from the operator(s) and the sector Ministry) is in line with international best practices. Independence heightens the effectiveness of a regulator, with regards to both procedural matters and easier maneuver of funding and actions to achieve the desired social and economic goals. Separation from other governmental agencies/ministries and service providers is generally seen as a factor that enables decisions to be taken in an impartial, fair and transparent manner. This does not negate, however, that in particular circumstances regulators that are not separate may be effective.	"Yes"; "No"	-	2	No	-	Yes
2 Is the Regulatory Authority autonomous in decision-making?	**Autonomy in decision making**	Autonomy is relevant to both the accountability and independence of the regulatory authority. It ensures that decisions are made consciously and with impartiality. As the specialized body with knowledge of the market, autonomy grants the regulatory authority with the tools to increase its efficiency and serve as a neutral broker in the market.	"Yes"; "No"	-	2	No	-	Yes

(continued)

#	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
	What are the reporting requirements of the Regulatory Authority?		Notwithstanding the need of independence, the regulatory authorities should be accountable for their actions to ensure effectiveness in legislation and enforcement of rules as well as impartiality in decision making. Having different governmental bodies deciding over the regulatory authority's structure and funding, in addition to the Head or the Board of the regulatory authority, avoids concentration of power and influence from one of the branches of the government over the regulatory decision. Particularly with regard to financial resources, appointment of the head of the regulator and reporting requirements, it is important to have another branch of the government reviewing the regulator's decisions. By doing so, the government will be implementing a system of checks and balances that is likely to prevent a regulator from, on one hand, over-spending (or over-charging the regulated entities) as well as, on the other hand, from conflicts of interest and lack of accountability. Although such controls may be seen as diminishing the regulator's ability to independently make decisions, it will result in the regulator implementing policies and programs needed by the telecommunications sectors and regulated entities are likely to feel a sense of regulatory security and transparency.	"Report to legislature"; "Report to Government (or Prime minister)"; "Report to other ministry"; "Annual report to the sector Ministry"; "No reporting requirements"; "Other" // "Parliament", "Government", "Head of government", "Sector minister", "Head of the regulator", "Other, please specify" // "Head of state", "Government Head of government", "Sector minister", "Parliament", "Other, please specify"	Pre-coding: (In each sub-indicator:) for "Report to legislature" or "Parliament", code as "P"; "Report to Government (or Prime Minister)", "Report to sector Ministry", "Government", "Head of Government" or "Sector Minister", code as "G"; "No reporting" or "Head of regulator", code as "NR". Coding: 3 different answers = 2; 2 different answers = 1; 3 identic answers = 0. Note: "Government" and "Head of Government" can be considered as the same	2	Coding in all sub-indicators is identical	Coding in two sub-indicators is different	Coding in all three sub-indicators is different
3	Who is responsible for approving the budget of the regulator? Who appoints the Members and the Head?	Accountability							

(continued)

Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
4 With regards to the last financial year, please indicate the sources of the Regulator's annual budget and the percentage of annual budget financed from each source	**Percentage of diversified funding**	The funding sources can directly impact the regulator's independence and political influence should be minimized to the extent possible. Having multiple sources of funding and not just financial sources from government appropriations is in line with international best practices. The funding sources and budgeting processes of regulators (i) may impact on independence, efficiency and cost of regulation and (ii) may directly impact the degree of a regulator's autonomy and competence when carrying out its responsibilities. Multiple sources of funding are generally associated with providing the regulator with more financial independence and greater autonomy in decision-making.	"Percentage of Award/ auction of mobile license"; "Percentage of Award/auction of other license"; "Percentage of License fees"; "Percentage of Government appropriation"; "Percentage of Numbering fees"; "Percentage of Spectrum fees"	Consider only the percentage of government appropriation. If it represents between 0 and 33% of the annual budget, classify as "minimal influence" = 2; If it represents between 34 and 66% of the annual budget, classify as "moderate influence" = 1; If it represents more than 66% of the authority's annual budget, classify it as "strong influence" = 0.	2	Strong influence	Moderate influence	Minimal influence

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
5	Are public consultations mandatory before regulatory decisions are made?	**Public consultations mandatory before decisions**	It is in line with international best practices for the law or regulation to generally require the regulator to conduct public consultations before issuing regulatory decisions. This requirement may specify that consultations are required for regulatory decisions likely to have a significant impact on the market and/or on end users. Public consultations allow for a democratic environment that takes into account in the decision-making process the opinions of consumer associations and individual consumers, the views of established or potential investors as well as other interested parties. They also increase the transparency of the regulatory authority's actions and decisions, and allow for a buy-in from all parties involved in the market.	"Yes", "In certain cases", "No"	-	2	No	In certain cases	Yes
6	Does the Regulatory Authority have enforcement power?	**Enforcement power**	Granting the regulator sufficient enforcement powers under the law is in line with best regulatory practice. To avoid political interference and ambiguous decisions influenced by the interests of market players, the regulatory authority should be empowered to enforce its decisions and regulations and thus ensure compliance with the rules set, improve the predictability of the regulatory frameworks in place and grow a level-playing field. Particularly, regulators should have sufficient powers to (i) enforce procedures in place; (ii) enforce regulations and licence conditions; and (iii) issue orders, directions to operators to carry out or cease certain activities, and (iv) impose sanctions, fines and other penalties for breach of legal/regulatory obligations.	"Yes", "No"	-	2	No	-	Yes

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
7	What sanctions or penalties can the Regulatory Authority impose?	**Sanctions or penalties imposed by regulator**	Empowering the regulator to enforce punitive measures, regulations or licence conditions by imposing penalties or sanctions for violations is in line with international best practices. Providing the regulator with sufficient legal grounding to exercise its enforcement functions is a key factor to ensure the legality/validity of the regulator's actions and decisions and to provide legal certainty to the sector.	"Monetary fines"; "Additional licence obligations"; "Modification of licence"; "Licence suspension"; "Licence revocation"	Sub-group "No sanction"; Sub-group "Moderate sanction" ("Monetary fines"; "Additional licence obligations"; "Modification of licence"); Sub-group "Strong sanction" ("Licence suspension"; "Licence revocation")	2	No sanction	Moderate sanction	Strong sanction
8	Does the regulatory framework set up a clear dispute resolution mechanism(s) to resolve disputes (e.g. on interconnection issues, customer complaints, etc.)?	**Dispute resolution mechanism**	As the ICT sector continues to evolve and become increasingly competitive, it is necessary to establish an effective dispute resolution system. Failure to resolve disputes can quickly limit competition, cause delays in the introduction of new services and technologies, block or reduce investment in the sector, and impede liberalization and development of the sector. Establishing clear dispute resolution mechanisms is in line with international practice. These procedures are critical to guarantee timely and effective intervention from regulators and contribute to the efficient functioning of competitive ICT markets as well as to the protection of consumers' rights.	"Yes"; "No"	-	2	No	-	Yes

(continued)

Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
9 Are appeals to the decision of the Regulatory Authority (entity in charge of regulation) allowed?	**Appeals to decisions**	Establishing clear and detailed procedures for appealing the regulator's major dispute resolution and enforcement decisions is consistent with good regulatory practices and is an important part of a comprehensive and effective regulatory framework. Allowing interested parties to appeal the regulator's decisions helps to ensure that the regulator is sufficiently accountable to stakeholders, including the state, service providers and consumers and affirms its credibility while providing the market players with the assurance of fairness and rule of law throughout the process.	"Yes"; "No"	-	2	No	-	Yes
10 Does your country have a Competition Authority?	**Existence of Competition authority**	Competition authorities overlook multiple market segments in order to avoid anticompetitive actions taken by operators with significant market power, actions which would harm other market players, potential new entrants as well as consumers.	"Yes"; "No"	-	2	No	-	Yes

20

2. Regulatory mandate

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
11	Please indicate below which entities have responsibility for: - Enforcement of quality of service obligations measures - Service quality monitoring	**Traditional mandate: entity in charge of quality of service obligations measures and service quality monitoring**	Service quality monitoring is a tool to aid in decisions in order to help customers make informed choices, to understand the state of the market (and help operators achieve fair competition), to maintain or improve quality in presence or absence of competition, and also to make interconnected networks work well together. It is equally as important to establish measures for controlling/monitoring quality of service to set achievable and appropriate targets. We consider that an unbiased and independent regulatory authority is the most capable body to be in charge of service quality monitoring.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Combined and cumulative. Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 0.5 and "Regulatory Authority" scores 1	2			According to sub-groups cumulative answer
12	Please indicate below which entities have responsibility for licensing	**Traditional mandate: entity in charge of licensing**	Development and implementation of authorization policies determine the structure, adaptability and level of competition of ICT services. We consider that an unbiased and independent regulatory authority has the knowledge and tools to best allocate authorizations with the goal of maximizing market productivity and efficiency.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2	2	Sub-group "Not regulated"	Sub-group "Government"	"Regulatory Authority"

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
13	Please indicate below which entities have responsibility for: - Interconnection rates - Price regulation	**Traditional mandate: entity in charge of interconnection rates and price regulation**	There is a consensus among economists and regulators that interconnection prices should promote economic efficiency, actively promoting competition, and additionally help achieve universal service. In the presence of market failures, price regulation is also important to avoid the exercise of market power, promote economic efficiency and competition and ensure that the prices are fair given the quality of service provided. We consider that an unbiased and independent regulatory authority is the most capable body to be in charge of interconnection rates and price regulation.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Combined and cumulative. Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 0.5 and "Regulatory Authority" scores 1	2			According to sub-groups cumulative answer
14	Please indicate below which entities have responsibility for: Spectrum Management- Radio frequency allocation and assignment (licensing)	**Spectrum: Entity in charge of radio frequency allocation and assignment**	Spectrum is a scarce resource and its efficient use can make an impact upon economic prosperity. Specific technical and service rules govern spectrum allocations and, as a result, they are a crucial determinant of the structure and performance of industry and of institutions devoted to ensuring public safety, security and national defense. We consider that an unbiased and independent regulatory authority has the knowledge to best allocate spectrum authorizations	"Sector Ministry "; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2	2	Sub-group Not regulated	Sub-group Government	Regulatory Authority

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
15	Please indicate below which entities have responsibility for the functions listed: Spectrum Management - Monitoring and Enforcement	**Entity in charge of Spectrum Monitoring and Enforcement**	Spectrum monitoring aids spectrum managers to plan and use frequencies, avoids incompatible usage and identifies sources of harmful interference. Spectrum use planning and resolution of spectrum scarcity issues can be accomplished through study and analysis of spectrum occupancy data. We consider the regulatory authority to be the best suited body to deal with compliance regarding rules and regulations, interference issues, frequency use and occupancy.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2	2	Sub-group Not regulated	Sub-group Government	Regulatory Authority
16	Please indicate below which entities have responsibility for: Universal Service/ Access	**Entity in charge of universal service/access**	Telecommunications markets are dynamic, new technologies are constantly emerging and new services rapidly become popular and then indispensable. Thus, UAS aspirations rise over time and effective regulation could help fulfilling some of these aspirations. We consider the regulatory authority the body most suitable to be responsible for UAS for its industry sector expertise and skilled technical, economic and financial staff; moreover it has a degree of independence perceived to be one step removed from politics and also holds credibility with the industry (the main partner in the implementation of UAS policy).	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2	2	Sub-group Not regulated	Sub-group Government	Regulatory Authority

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
17	Please indicate below which entities have responsibility for: Entity in charge of broadcasting (radio and TV transmission)	**New mandate: entity in charge of broadcasting (radio and TV transmission)**	Having a converged regulator with authority over ICT and media/broadcasting is in line with international best practices. Since a single authority is charged with regulating these services, the need for formal coordination processes between agencies/authorities is no longer present, often allowing for more efficiency at planning and introducing converged technologies and services to the market. Because of this, converged regulators are conducive to enabling market integration in a converged environment.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2		Sub-group Not regulated	Sub-group Government	Regulatory Authority
18	Please indicate below which entities have responsibility for the functions listed: Entity in charge of broadcasting content	**New mandate: entity in charge of broadcasting content**	Cf. description of question 17.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2		Sub-group Not regulated	Sub-group Government	Regulatory Authority
19	Please indicate below which entities have responsibility for: Internet content	**New mandate: entity in charge of Internet content**	Cf. description of question 17.	"Sector Ministry"; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator, "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2		Sub-group Not regulated	Sub-group Government	Regulatory Authority

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
20	Please indicate below which entities have responsibility for: Information Technology	**New mandate: entity in charge of IT**	Cf. description of question 17.	"Sector Ministry "; "Other Ministry or Government body"; "Regulatory Authority"; "Operator"; "Not regulated"	Sub-group "Not regulated" ("Operator", "Not regulated") scores 0, Sub-group Government ("Sector Ministry", "Other Ministry or Government") scores 1 and "Regulatory Authority" scores 2.	2	Sub-group Not regulated	Sub-group Government	Regulatory Authority
21	Is the Regulatory Authority responsible for: 1a. Providing comparative tariff information 1b. Informing consumers of their rights (consumer education) 2. Handling consumer complaints	**Consumer issues: entity responsible for comparative tariff information, consumer education and handling consumer complaints**	If the regulator does not have the ability to demand information from operators, particularly incumbent operators, to assess overall market performance and/or investigate alleged violations, then service providers can engage in anti-competitive practices to the detriment of consumers. As a result, the entire regulatory system can be undermined, thus creating uncertainty and constraining market development. Regulators that have the ability to address consumer complaints, allowing consumers another avenue of redress for complaints that are not resolved directly with the operators, ensure transparecy and increased social welfare.	"Yes"; "No"	Combined and cumulative: - for questions 1a and 1b, "Yes" scores 0.5 and "No" scores 0 - for question 2, "Yes" scores 1 and "No" scores 0	2		According to cumulative score.	

3. Regulatory regime

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
22	What types of licences are provided in your country	**Types of licences provided**	Issuing service-specific licenses, which refer to a particular type of service over a specific type of network, is a customized and lenghty process that does not keep up with the innovations and developments of the ICT sector. Multi-service individual licenses represent a further, although not optimal, step into dropping the barriers for service innovations. General, unified/ global licenses stand for increased market liberalization and the application of equal conditions to all service providers, enabling a more competitive environment. It should be noted that issuing individual licences for the radio spectrum authorizations remains a common practice throughout the world, particularly where the demand for the use of a particular frequency band exceeds availability.	"Service-specific individual licences", "Multi-service individual licenses"; "Unified/global licences"; "General authorizations"; "Simple notification"; "Licence exempt "	Although the question allows multiple answers, the scoring is not cumulative, the highest score (1 or 2) is taken only once.	2	Only Service-specific individual licenses	Only Multi-service individual licenses	Unified/global licences, General authorizations or Simple notification

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
23	What types of licences are provided in your country	**License exempt**	An open entry market allows for competitive behaviour and self-regulating, thus ever-adapting, market conditions. Without the licensing barrier to overcome, service providers can focus their investment into infrastructure building, innovation and competitive services.	Service-specific individual licences; "Multi-service individual licenses"; "Unified/global licences"; "General authorizations"; "Simple notification"; "Licence exempt"	Only the option "Licence exempt" was taken into account; all other answers were considered as blank.	2	-	-	Licence exempt
24	Do you require any operators to publish Reference Interconnection Offer (RIO)?	**Operators required to publish Reference Interconnection Offer (RIO)**	When operators are required to publish RIO, new entrants have sufficient information about the network to allow for decision-making, thus reducing entry time, and to provide a baseline for negotiation. The publication of a standard offer, in the form of a RIO, narrows the scope for a dominant operator to discriminate among applicants for interconnection.	"Yes"; "No"	-	2	No	-	Yes
25	Are interconnection prices made public?	**Interconnection prices made public**	Making interconnection agreements public opens the discussion to other parties that might have issues at stake, it also ensures transparency for both the population and other market players about the interconnection environment.	"Yes"; "No"	-	2	No	-	Yes
26	Is quality of service monitoring required?	**Quality of service monitoring required**	Measuring the quality of service of operators helps consumers make their choices considering not only pricing but also the service standards provided by the operator. Moreover, QoS monitoring helps portray the market standards in a realistic way and assists operators in achieving fair competition, especially in the case of secondary trading and infrastructure sharing.	"Yes"; "No"		2	No	-	Yes

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
27	Is infrastructure sharing for mobile operators permitted (e.g. Mobile Virtual Network Operators)?	**Infrastructure sharing for mobile operators permitted**	Network-sharing agreements can optimize the use of the coverage for operators, generally reducing costs, thus being beneficial for both the service providers and the consumers. It can also serve as incentive to network deployment. MVNOs allow for other market players- operators- to resell existing products and services from another provider or even bulkbuying minutes and data, increasing the profitability of the market.	"Yes", "No"	-	2	No	-	Yes
28	Is infrastructure sharing mandated (towers, base stations, posts, ducts, etc.)?	**Infrastructure sharing mandated**	Infrastructure sharing between market operators or with other industries can decrease expenditures by the joint deployment and maintenance of facilities as well as increase productivity of the usage of scarce resources.	"Yes", "No"	-	2	No	-	Yes
29	Is co-location/site sharing mandated?	**Co-location/site sharing mandated**	Passive infrastructure sharing is aesthetically, enviromentally and economically positive. It provides the opportunity for investment on the improvement of services, greater coverage and innovation due to reduced fixed costs.	"Yes", "No"	-	2	No	-	Yes
30	Is unbundled access to the local loop required?	**Unbundled access to the local loop required**	Unbundling reduces infrastructure deployment costs and avoids unnecessary duplication of sections of the incumbent's infrastructure. By reducing the amount of initial investment- fixed costs-, market entry is stimulated, driving competition forward.	"Yes", "No"	-	2	No	-	Yes
31	Is secondary spectrum trading allowed?	**Secondary trading allowed**	Secondary trading promotes optimal, thus more economically productive, use of spectrum. It also helps to create a self-regulating environment given the more effective usage of the frequency bands, both by the new entrant and the network operator who already possesses the rights.	"Yes", "No"	-	2	No	-	Yes

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
32	Is band migration allowed?	**Band migration allowed**	If band migration is allowed, the market participants can provide new services within their existing license. This increases incentives for innovation and more efficient use of the networks, as well as decreasing the cost of a new license.	"Yes", "No"	-	2	No	-	Yes
33	Is number portability required from: a) Fixed-line operators?/ If yes, is this service currently available to fixed subscribers?	**Number portability available to consumers and required from fixed-line operators**	Number portability increases competition and quality of services among service providers in order to retain their current clients (which are no longer held back by the imposition of a new telephone number).	"Yes", "No" // "Yes", "No"	If both answers are "No" or one is "No" and the other blank, code as "No"; if number portability is required but not available code as "Partial". Finally, if both answers are "Yes", code as "Yes".	2	No	Partial	Yes
34	Is number portability required from: b) Mobile operators?/ If yes, is this service currently available to subscribers?	**Number portability available to consumers and required from mobile operators**	Cf. description of question 33.	"Yes", "No" // "Yes", "No"	If both answers are "No" or one is "No" and the other blank, code as "No"; if number portability is required but not available code as "Partial". Finally, if both answers are "Yes", code as "Yes".	2	No	Partial	Yes
35	Are individual users allowed to make voice over IP (VoIP) or Internet telephony phone calls?	**Individual users allowed to use VoIP**	As an option to the traditional telephony, the VoIP services represent a different way of placing calls that has been improving over time and imposing competition on the historical market players. It stimulates traditional business models to become more efficient, innovative and reduce costs in order to keep their places in the market.	"Yes", "No"		2	No	-	Yes

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
36	Has your country adopted a national plan (initiative, policy, strategy, etc) to promote broadband?	**National plan that involves broadband**	The adoption of a national plan that includes broadband reinforces the necessity of a consensus and coordination for both the infrastructure deployment and the regulation of the services to be provided. A more coordinated and accountable environment, in turn, accelerates innovation, boosts investment and raises productivity, all of which, along with the universal access goal of the broadband plan, contribute to higher penetration and competition levels.	"Yes"; "No"		2	No	-	Yes

4. Competition framework

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
37	Level of competition: Basic services (Local fixed line services, Domestic fixed long distance, International fixed long distance)	**Level of competition in local and long distance (domestic and international) fixed line services**	International best practices favor competition over monopolies in the ICT market since competitive markets are known to increase consumer welfare by lowering prices, promoting innovation, improving consumer choice and raising the quality of services. Note: the question refers to what is legally permissible in each member state.	"Monopoly"; "Partial competition"; "Full competition" // "Monopoly"; "Partial competition"; "Full competition" // "Monopoly"; "Partial competition"; "Full competition"	For each sub-indicator, score 0 for "Monopoly"; 1 for "Partial competition", and 2 for "Competition". Take average of the three scorings.	2		Average score of the three sub-indicators	
38	Level of competition: IMT (3G, 4G, etc.)	**Level of competition in IMT (3G, 4G, etc.) services**	Cf. description of question 37.	"Monopoly"; "Partial competition"; "Full competition"		2	Monopoly	Partial competition	Competition
39	Level of competition: Broadband services (DSL, Cable modem, Fixed Wireless Broadband)	**Level of competition in cable modem, DSL, fixed wireless broadband**	Cf. description of question 37.	"Monopoly"; "Partial competition"; "Full competition" // "Monopoly"; "Partial competition"; "Full competition" // "Monopoly"; "Partial competition"; "Full competition" // "Monopoly"; "Partial competition"; "Full competition"	For each sub-indicator, score 0 for "Monopoly"; 1 for "Partial competition", and 2 for "Competition". Take average of the three scorings.	2		Average score of the four sub-indicators	
40	Level of competition: Leased lines	**Level of competition in leased lines**	Cf. description of question 37.	"Monopoly"; "Partial competition"; "Full competition"		2	Monopoly	Partial competition	Competition
41	Level of competition: International Gateways	**Level of competition in International Gateways**	Cf. description of question 37.	"Monopoly"; "Partial competition"; "Full competition"		2	Monopoly	Partial competition	Competition
42	Status of the main fixed line operator (public, partially privatized/partially private, fully privatized/private)	**Status of the main fixed line operator**	Both the regulatory authority and the incumbent being overseen by the same entity is not optimal as the decision-making process could be biased to lean towards the interests of the incumbent rather than promote market competition, quality of services and greater welfare for the population.	"State-owned", "Partially privatized", "Partially private", "Fully privatized", "Fully Private"		2	State-owned	Partially privatized/ Partially private	Fully privatized/ Private

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
43	National anti-trust/ competition law recognizes the concept of "dominance" or Significant Market Power (SMP)	**Legal concept of dominance or SMP**	Defining the concept of Significant Market Power (SMP) is an important step to avoid anticompetitive behaviour. When operators are classified as having significant market power, it is possible for the regulator to impose ex ante regulations (i.e. mandatory publication of Reference Interconnection Offers) to avoid erroneous use of this power.	"Yes"; "No"		2	No	-	Yes
44	Criteria used in determining "dominance" or SMP (geographical, market share, control of essential facilities, easy access to financial resources, strength of the countervailing power of consumers, economies of scale and scope)	**Criteria used in determining dominance or SMP**	Because market share by itself does not imply significant market power, it is important to have multiple criteria contributing to the definition of SMP - thus increasing the chances of recognizing those operators with power enough to impose anticompetitive environment to other market players.	"Geographical"; "Market share"; "Control of essential facilities"; "Easy access to financial resources"; "Strength of the countervailing power of consumers"; "Economies of scale and scope"		2	Blank	One of any answer or two different answers	Three or more different answers
45	Restrictions to foreign participation/ ownership: Facilities-based operators	**Foreign participation/ ownership in facilities-based operators**	Foreign investment facilitates the growth and development of the telecommunications sector, increasing access to capital for network development and modernization, and allowing for the transfer of technology and know-how leading to increased productivity, innovation and competitiveness.	"No restriction"; "Controlling interest"; "50%"; "Minority interest"; "No foreign ownership allowed"	For "No restriction" or "Controlling interest" code as "Loose control"; for "50%" or "Minority Interest" code as "Moderate control"; and for "No foreing ownership allowed" code as "Full control".	2	Full control	Moderate control	Loose control

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
46	Restrictions to foreign participation/ ownership: Spectrum-based operators	**Foreign participation/ ownership in spectrum-based operators**	Cf. description of question 45.	"No restriction"; "Controlling interest"; "50%"; "Minority interest"; "No foreign ownership allowed"	For "No restriction" or "Controlling interest" code as "Loose control"; for "50%" or "Minority Interest" code as "Moderate control"; and for "No foreing ownership allowed" code as "Full control".	2	Full control	Moderate control	Loose control
47	Restrictions to foreign participation/ ownership: National service operators (Local service operators & Long-distance service operators)	**Foreign participation/ ownership in local service operators/long-distance service operators**	Cf. description of question 45.	"No restriction"; "Controlling interest"; "50%"; "Minority interest"; "No foreign ownership allowed" // "No restriction"; "Controlling interest"; "50%"; "Minority interest"; "No foreign ownership allowed"	For each sub-indicator, score 0 for "No restriction" or "Controlling interest"; score 1 for "50%" or "Minority Interest" score 1; and 2 for "No foreing ownership allowed". Take average average of the two scorings.	2	Average score of the two sub-indicators		

(continued)

Indicator		Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
48	Restrictions to foreign participation/ ownership: International service operators	**Foreign participation/ ownership in international service operators**	Cf. description of question 45.	"No restriction", "Controlling interest", "50%"; "Minority interest"; "No foreign ownership allowed"	For "No restriction" or "Controlling interest" code as "Loose control", for "50%" or "Minority Interest" code as "Moderate control"; and for "No foreing ownership allowed" code as "Full control".	2	Full control	Moderate control	Loose control
49	Restrictions to foreign participation/ ownership: Internet Service Providers (ISP)	**Foreign participation/ ownership in Internet Service Providers (ISPs)**	Cf. description of question 45.	"No restriction", "Controlling interest", "50%"; "Minority interest"; "No foreign ownership allowed"	For "No restriction" or "Controlling interest" code as "Loose control", for "50%" or "Minority Interest" code as "Moderate control"; and for "No foreing ownership allowed" code as "Full control".	2	Full control	Moderate control	Loose control

(continued)

	Indicator	Area	Description	Raw Values	Coding	Benchmark	0 pts	1 pt	2 pts
50	Restrictions to foreign participation/ ownership: Value-added service providers	**Foreign participation/ ownership in value-added service providers**	Cf. description of question 45.	"No restriction"; "Controlling interest"; "50%"; "Minority interest"; "No foreign ownership allowed"	For "No restriction" or "Controlling interest" code as "Loose control"; for "50%" or "Minority Interest" code as "Moderate control"; and for "No foreing ownership allowed" code as "Full control".	2	Full control	Moderate control	Loose control

28

Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.:   +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and Director，Administration and Operations Coordination Department (DDR)	**Infrastructure Enabling Environmnent and e-Applications Department (IEE)**	**Innovation and Partnership Department (IP)**	**Project Support and Knowledge Management Department (PKM)**
Email: bdtdeputydir@itu.int	Email: bdtiee@itu.int	Email: bdtip@itu.int	Email: bdtpkm@itu.int
Tel.: +41 22 730 5784	Tel.: +41 22 730 5421	Tel.: +41 22 730 5900	Tel.: +41 22 730 5447
Fax: +41 22 730 5484	Fax: +41 22 730 5484	Fax: +41 22 730 5484	Fax: +41 22 730 5484

Africa

Ethiopia	Cameroon	Senegal	Zimbabwe
International Telecommunication Union (ITU) Regional Office	**Union internationale des télécommunications (UIT) Bureau de zone**	**Union internationale des télécommunications (UIT) Bureau de zone**	**International Telecommunication Union (ITU) Area Office**
P.O. Box 60 005	Immeuble CAMPOST, 3e étage	19, Rue Parchappe x Amadou	TelOne Centre for Learning
Gambia Rd., Leghar ETC Building	Boulevard du 20 mai	Assane Ndoye	Corner Samora Machel and
3rd floor	Boîte postale 11017	Immeuble Fayçal, 4e étage	Hampton Road
Addis Ababa – Ethiopia	Yaoundé – Cameroun	B.P. 50202 Dakar RP	P.O. Box BE 792 Belvedere
		Dakar – Sénégal	Harare – Zimbabwe
Email: itu-addis@itu.int	Email: itu-yaounde@itu.int	Email: itu-dakar@itu.int	Email: itu-harare@itu.int
Tel.: +251 11 551 4977	Tel.: + 237 22 22 9292	Tel.: +221 33 849 7720	Tel.: +263 4 77 5939
Tel.: +251 11 551 4855	Tel.: + 237 22 22 9291	Fax: +221 33 822 8013	Tel.: +263 4 77 5941
Tel.: +251 11 551 8328	Fax: + 237 22 22 9297		Fax: +263 4 77 1257
Fax: +251 11 551 7299			

Americas

Brazil	Barbados	Chile	Honduras
União Internacional de Telecomunicações (UIT) Regional Office	**International Telecommunication Union (ITU) Area Office**	**Unión Internacional de Telecomunicaciones (UIT)**	**Unión Internacional de Telecomunicaciones (UIT)**
SAUS Quadra 06, Bloco "E"	United Nations House	Oficina de Representación de Área	Oficina de Representación de Área
11º andar, Ala Sul	Marine Gardens	Merced 753, Piso 4	Colonia Palmira, Avenida Brasil
Ed. Luis Eduardo Magalhães (Anatel)	Hastings, Christ Church	Casilla 50484, Plaza de Armas	Ed. COMTELCA/UIT, 4.º piso
70070-940 Brasilia, DF – Brazil	P.O. Box 1047	Santiago de Chile – Chile	P.O. Box 976
	Bridgetown – Barbados		Tegucigalpa – Honduras
Email: itubrasilia@itu.int	Email: itubridgetown@itu.int	Email: itusantiago@itu.int	Email: itutegucigalpa@itu.int
Tel.: +55 61 2312 2730-1	Tel.: +1 246 431 0343/4	Tel.: +56 2 632 6134/6147	Tel.: +504 22 201 074
Tel.: +55 61 2312 2733-5	Fax: +1 246 437 7403	Fax: +56 2 632 6154	Fax: +504 22 201 075
Fax: +55 61 2312 2738			

Arab States
Asia and the Pacific
CIS countries

Egypt	Thailand	Indonesia	Russian Federation
International Telecommunication Union (ITU) Regional Office	**International Telecommunication Union (ITU) Regional Office**	**International Telecommunication Union (ITU) Area Office**	**International Telecommunication Union (ITU) Regional Office**
Smart Village, Building B 147, 3rd floor	Thailand Post Training Center, 5th floor,	Sapta Pesona Building, 13th floor	4, Building 1
Km 28 Cairo – Alexandria Desert Road	111 Chaengwattana Road, Laksi	Jl. Merdan Merdeka Barat No. 17	Sergiy Radonezhsky Str.
Giza Governorate	Bangkok 10210 – Thailand	Jakarta 10001 – Indonesia	Moscow 105120
Cairo – Egypt			Russian Federation
	Mailing address	Mailing address:	Mailing address:
	P.O. Box 178, Laksi Post Office	c/o UNDP – P.O. Box 2338	P.O. Box 25 – Moscow 105120
	Laksi, Bangkok 10210 – Thailand	Jakarta 10001 – Indonesia	Russian Federation
Email: itucairo@itu.int	Email: itubangkok@itu.int	Email: itujakarta@itu.int	Email: itumoskow@itu.int
Tel.: +202 3537 1777	Tel.: +66 2 575 0055	Tel.: +62 21 381 3572	Tel.: +7 495 926 6070
Fax: +202 3537 1888	Fax: +66 2 575 3507	Tel.: +62 21 380 2322	Fax: +7 495 926 6073
		Tel.: +62 21 380 2324	
		Fax: +62 21 389 05521	

Europe

Switzerland
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland