ITUPublications

International Telecommunication Union
Development Sector

Digital Regulation Handbook

Co-published with:

THE WORLD BANK

Digital Regulation Handbook

ISBN:

978-92-61-31651-8 (Paper version)

978-92-61-31661-7 (Electronic version)

978-92-61-31671-6 (EPUB version)

978-92-61-31681-5 (Mobi version)

Foreword

Today's digital technologies are transforming almost every sector of the economy by presenting new business models, introducing innovative products and services – and, ultimately, changing the way countries around the world harness socioeconomic development. Digital technologies, and the benefits that they bring, can connect citizens to services and opportunities, and help them build a better future. However, for markets to function effectively, they must be accompanied by an enabling policy and regulatory environment.

The digital economy – comprising digital infrastructure, platforms, services, businesses and skills – has become an essential means of reducing poverty and improving the quality of the lives of the poor and vulnerable. Digital technologies and communication infrastructure are unlocking innovative solutions to complex challenges across a broad range of sectors including energy, health, education, transport, disaster risk management, and agriculture. The Internet and digital technologies have a profound impact on the way governments operate and interact with their citizens, creating increased transparency and more efficient service delivery, and in turn requiring greater cooperation across sectors and a collaborative approach to regulation. The ongoing wave of innovation has the potential to remove many of the barriers that stand between people and opportunity, especially for populations in poorer communities.

While digital technologies continue to transform markets through convergence and reorganization of various sectors of the economy, serious market gaps and questions still remain that must be addressed, such as protecting citizens' rights and individuals' data online, and finding ways to provide ubiquitous high-speed broadband connectivity services at affordable prices, including to remote areas.

The *Digital Regulation Handbook*, now in its third edition, serves as an essential guide to assist regulatory authorities and policy-makers in deciding on appropriate digital regulations, and evaluating the effectiveness of those regulations. The objective of this new edition of the Handbook is to provide online resources and analysis to assist ICT regulatory authorities worldwide to build capacity regarding topical regulatory issues and best practices related to the digital economy.

The World Bank and the International Telecommunication Union are pleased to make available the *Digital Regulation Handbook* and a new online *Digital Regulation Platform* to update and revise the *ICT Regulation Toolkit*. These resources can be used as references and collaborative platforms to create both an environment in which the transformative power of digital technologies can reach its full potential, and as a powerful enabling tool for supporting innovation and achieving inclusive sustainable development.

Boutheina Guermazi
Director, Digital Development, World Bank

Doreen Bogdan-Martin
Director, Telecommunication Development Bureau, International Telecommunication Union

Table of Contents

List of tables and figures

Tables

Figures

Boxes

Introduction

The World Bank and the International Telecommunication Union are pleased to present the *Digital Regulation Handbook*, the result of an ongoing collaboration over two decades between the two agencies. It aims to provide practical guidance and best practice for policy-makers and regulators across the globe concerned with harnessing the benefits of the digital economy and society for their citizens and firms. The content not only provides an update on the basics of ICT regulation in light of the digital transformation sweeping across sectors, but also includes new regulatory aspects and tools for ICT regulators to consider when making regulatory decisions. The Handbook will also be a useful reference for other stakeholders from industry, development agencies, citizen and consumer groups, and academia.

Alongside the *Digital Regulation Handbook*, a new online *Digital Regulation Platform* is being developed to update and revise the *ICT Regulation Toolkit*. The *Platform* builds on and extends the Handbook by providing more detailed guidance and case studies of best practice in regulation of the digital economy. The intention is that the Handbook provides a high-level snapshot of the current state of play in 2020, while the Platform will be dynamic and be continually updated over coming years to reflect the rapidly changing digital world.

Work on the original Handbook started in 2000 against a background of emerging trends towards privatization and liberalization of telecommunications markets, the primary aim being to promote and ensure fair competition; the major content therefore being licensing, interconnection of networks, price regulation, and universal service A decade later, in 2010, the tenth anniversary edition of the Handbook reflected the growing importance of telecommunications for national economies and the shaping of the regulatory landscape by the rapid take-up of the Internet and mobile cellular communications across the world, with new emphasis on spectrum management and value-added services. Now, while the fundamental aspects of telecommunications and ICT regulation remain important, the greatest regulatory challenges arise from the emergence of a data driven economy led by new technologies and applications, such as big data, the Internet of Things, and associated new business models.

Digital applications now permeate all aspects of the economy and society, enabling users to access government services, make mobile payments, play games, listen to music, watch movies, travel more efficiently, and so on. In this digital world, it is increasingly apparent that it is the use of data that is the driving force. Consequently, the greatest challenge we now face concerns the way we regulate who is responsible for data and how it is collected, stored, processed, and shared.

With digital transformation affecting every aspect of our lives, this also poses new challenges for regulatory structures that have traditional been organized on a sectoral or domain basis. Data protection, for example, is not just the preserve of the ICT sector and, as we look to the future, a more flexible approach will be needed involving either cooperation and collaboration between sectoral regulators or the establishment of new dedicated agencies to respond to the issues arising from the digital economy. The *Digital Regulation Handbook* addresses these and other issues to support policy-makers and regulators to navigate the emerging challenges associated with digital transformation.

Accordingly, the Handbook is structured as follows:

Chapter 1, on "Regulatory governance and independence" offers a forward-looking analysis of how ICT regulatory governance is changing to accommodate digital development. It reviews the evolution of regulation and policy implementation from the traditional telecommunication environment, through ICTs, and into digital technologies. The role and institutional design of the regulator address common regulatory structures found worldwide and traditional areas of regulation, including how the regulator's mandate may shift in a digital environment. The chapter addresses a key element of future regulation – regulatory collaboration – that involves coordination among various sectoral agencies and government institutions. Alternative models to regulation, such as self-regulation or industry/government collaboration, are also discussed.

Chapter 2, on "Competition and economics" provides an overview of the significant market and regulatory disruption caused by digital transformation. It reviews existing economic issues related digital regulation, and consider issues relating to regulation of markets, interconnection of networks, infrastructure sharing, price regulation, dispute resolution, licensing and authorization, mergers and acquisitions, and taxation.

Chapter 3, on "Access for all" discusses key challenges and policies to achieve universal access objectives within the context of digital transformation. The discussion focuses on three pillars: connectivity, which addresses challenges associated with funding broadband infrastructure expansion; pricing, which deals with affordability barriers to the take-up of digital services and end-user devices; and inclusion, which covers policies to develop digital skills, to respond to gender disparities and accessibility of services to people with disabilities, and to promote the creation of local digital content.

Chapter 4, on "Consumer affairs" discusses the consumer support framework within which ICT regulators work and, within this, the consumer-oriented actions likely to fall to ICT regulators. The chapter identifies the key consumer issues already arising in the digital economy, and outlines changing consumer horizons and needs.

Chapter 5, on "Data protection and trust" examines the nature of data protection regimes, focusing particularly on its regulatory aspects. It examines the extent to which emerging technology and services should, and could, be impacted, as well as the controls over the cross-border flow of personal data and the resultant trade implications. Data protection and privacy concerns particularly overlap when considering the need for special rules to govern communication activities. The complex intersection between data protection and information security is also examined.

Chapter 6, on "Spectrum management" is in two parts. The first provides overall guidance on the regulatory framework for national spectrum management starting by setting the international context and processes. The second part discusses key applications and regulatory considerations driving the future use of spectrum, highlighting some of the main points that regulators are invited to consider on the national level, based on the relevant experience of different country examples. It presents some of the mechanisms for spectrum allocation and licensing of new spectrum, with due consideration to the technology evolution. It also looks at promoting the use of spectrum for these key applications, as well as business models that can strengthen existing and new approaches for the deployment of wireless broadband.

Chapter 7, on "Regulatory responses to evolving technologies" discusses the general trend in redefining the roles of the various regulatory authorities in response to cloud computing,

AI, blockchain, big data, and the Internet of Things (IoT). While the desired outcomes – fair competition, consumer protection, and economic development – remain the same, the approaches to achieve them are changing across time and differ between countries. This chapter aims to provide a framework to identify a suitable regulatory approach in response to arising technologies.

Chapter 8, on "Technical regulation" covers two aspects: quality of service (QoS) and numbering, naming, addressing, and identification (NNAI). On QoS, the chapter explains the role of the regulator in informing users, restraining operators in strong competitive positions, ensuring efficient use of scarce resources, and assessing the national infrastructure. The activities of regulators related to QoS monitoring are explored including: selecting indicators; defining measurements; setting targets; making, auditing and publishing measurements; stimulating improvements; and reviewing developments. On NNAI, the chapter explains the importance of NNAI, outlines the key objectives of NNAI management, explores the impact of new technologies on NNAI and describes the instruments at the disposal of the regulator.

Chapter 9, on "Emergency communications" examines the role of regulators in relation to different types of disasters, which include weather-related hazards, such as hurricanes, floods, and droughts, geological hazards, such as earthquakes, volcano eruptions, and biological hazards which include epidemics, and latterly also pandemics. The chapter examines the four phases of the disaster management process – mitigation, preparedness, response, and recovery – and the role of ICT and telecommunications in each of these phases.

Acknowledgements / About the authors

The *Digital Regulation Handbook* has been prepared by a team of authors directed by the International Telecommunication Union (Nancy Sundberg, Youlia Lozanova, and Sofie Maddens, Regulatory and Market Environment Division, under the overall coordination of Eun-Ju Kim, Chief a.i. Digital Knowledge Hub Department, ITU Telecommunication Development Bureau (BDT)), and the World Bank (Tim Kelly, Roku Fukui, and Ida Mboob of the Digital Development Global Practice) under the leadership of Doreen Bogdan-Martin, Director of the Telecommunication Development Bureau, ITU, and Boutheina Guermazi, Director Digital Development, World Bank Group. The authors of the chapters are:

Chapter 1, "Regulatory governance and independence:" Janet Hernandez, President, Telecommunications Management Group.

Chapter 2, "Competition and economics:" David Rogerson, Director, Incyte Consulting.

Chapter 3, "Access for all:" Janet Hernandez, President, Telecommunications Management Group.

Chapter 4, "Consumer affairs:" Claire Milne, Partner, Antelope Consulting.

Chapter 5, "Data protection and trust:" Ian Walden, Professor of Information and Communications Law and Director of the Centre for Commercial Law Studies, Queen Mary, University of London.

Chapter 6, "Spectrum management:" Part 1: ITU-R Study Group 1, Radiocommunication Sector of the ITU; Part 2: Geraldo Neto, Senior Technical and Policy Adviser, Telecommunications Management Group.

Chapter 7, "Regulatory responses to evolving technologies:" Christoph Stork, Partner, Research ICT Solutions.

Chapter 8, "Technical regulation: "Quality of service": Robert Milne, Partner, Antelope Consulting; "Numbering, naming, addressing, and identification (NNAI)": Phil Rushton, Director, Rushton Communications Consulting Ltd, with contributions from Robert Milne.

Chapter 9, "Emergency communications:" Juan Roldan, President of Luxon Consulting Group, LLC, with contributions from Robert Milne, Partner, Antelope Consulting.

The Handbook was edited by Colin Blackman, Director, Camford Associates.

In addition, thanks are due to the following for their support and assistance in reviewing the content of the Handbook: Martin Adolph, Cristina Bueti, Robert Clark, Maritza Delgado, Mijke Herthogs, Jean-Jacques Massima, Mythili Menon, Carmen Prado Wagner, Christine Sund, Diana Tomimura, Joanne Wilson and Jie Zhang (from ITU) and Jerome Bezzina, Tania Begazo Gomez, Petter Lundkvist and David Satola (of the World Bank Group).

Chapter 1. Regulatory governance and independence

1.1 Introduction

The regulatory framework, as well as the regulatory governance and independence of the institution, are key elements for effective regulation. Today, regulators and policy-makers face multiple challenges: they must address the traditional aspects of information and communication technologies (ICTs) and assess their appropriate roles in addressing the regulatory and policy issues arising from new digital technologies and services.

In addition to more traditional issues, such as connectivity and infrastructure development, the digital environment prompts consideration of a broader range of sectors beyond ICTs, such as health, finance, education, transportation, and energy. The issues to be addressed include content regulation, privacy, consumer protection, competition, and artificial intelligence (AI), among others. Depending on their competencies and capacity, traditional ICT regulators may be less familiar with these topics, have limited resources to address them, or lack clear authority to cover them or coordinate with other entities on these issues under their current mandates.

Overall, these discussions are still in nascent stages around the world. While some countries are already seeking to fit digital technologies into their regulatory frameworks, many others have yet to begin the process. Thus, there is ample space for countries to innovate, to adapt, and to evolve. Because there is no well-worn path forward that can easily apply across jurisdictions, outreach and open consultations are crucial to engaging stakeholders while evidence-based decision-making processes are essential for each country to find workable, reasonable, flexible solutions.

With these issues in mind, Chapter 1 of the *Digital Regulation Handbook* offers a forward-looking analysis of how ICT regulatory governance is changing to accommodate digital developments. The chapter begins by reviewing the evolution of regulation and policy implementation from the traditional telecommunication environment, through ICTs, and into digital technologies. The role and institutional design of the regulator address common regulatory structures found

worldwide and traditional areas of regulation. This analysis then focuses on how the regulator's mandate may shift in a digital environment, emphasizing the importance of inclusive and effective decision-making. Next, this chapter addresses a key element of future regulation – regulatory collaboration – that involves coordination among various sectoral agencies and government institutions. Alternative models to regulation, such as self-regulation or industry/government collaboration, are also discussed. Finally, the chapter highlights some of the main factors for building digital frameworks, including issues relating to network and service licensing, spectrum authorization, and innovative, evidence-based approaches to sector regulation.[1]

1.2 Policy and implementation

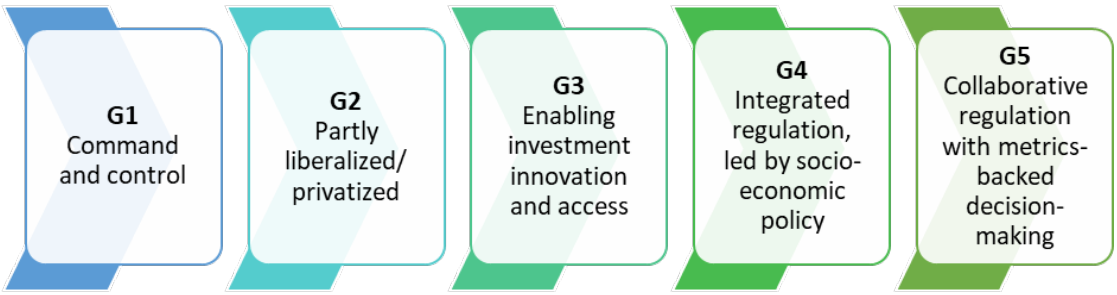
Evolution of regulation

Sector regulation has evolved over the past three decades, beginning with the development of telecommunication regulatory frameworks as countries started opening their markets to competition. Regulation then expanded to encompass ICTs to address new technologies and services enabled by the Internet. Now, the transformation from ICTs to the digital space is underway, leading policy-makers and regulators to examine the wide-reaching social and economic impacts of online platforms, 5G, cloud computing, and the Internet of Things (IoT), among other emerging technologies that engage all sectors of the economy.

From traditional telecommunication environment to digital landscape

The ITU has developed a comprehensive model to assess regulatory evolution, which tracks generations of regulation (see Figure 1.1). Generation 1 (G1) to Generation 4 (G4) presents the evolution in telecommunication and ICT regulation, starting from the command and control regime typically associated with state-owned monopolies, through privatization and liberalization, the need to encourage investment, and the shift to meeting socioeconomic objectives. Generation 5 (G5) is reflected as the latest generation, but is "seen as complementary to the previous generations", highlighting the increased importance of more flexible and collaborative regulatory frameworks capable of addressing the broad impacts of the digital economy across sectors (ITU 2020, 26).

Figure 1.1. Generations of regulation: G1 to G5



Source: ITU, ICT Regulatory Tracker 2018, https://www.itu.int/net4/itu-d/irt/#/generations-of-regulation; ITU 2020.

Note: **Generations 1 through 4 are measured through the ICT Regulatory Tracker. Generation 5 is measured through the G5 Benchmark.**

[1] For more detailed examination of the topics covered in this chapter, see relevant thematic sections on the *Digital Regulation Platform*.

The Organisation for Economic Co-operation and Development (OECD) similarly recommends that "[d]igital transformation policies need to be coordinated among all policy domains and actors affected by (and affecting) digital transformation" (OECD 2019, 147). The OECD also recognizes that there is no single solution for governance, which must be adapted based on each country's institutions and regulatory culture and capacity, as well as understanding that these structures will continue to change over time.

An important tool in moving to G5 frameworks is to cultivate agile regulation. This entails developing flexible sectoral legislation and regulation to respond to rapidly changing technologies, services, and markets (ITU 2019; World Bank and ITU 2021 (forthcoming)). Policy-makers can adopt an agile regulatory approach that works with industry players to leverage their knowledge and expertise, whereby regulators can play a collaborative or facilitator role.

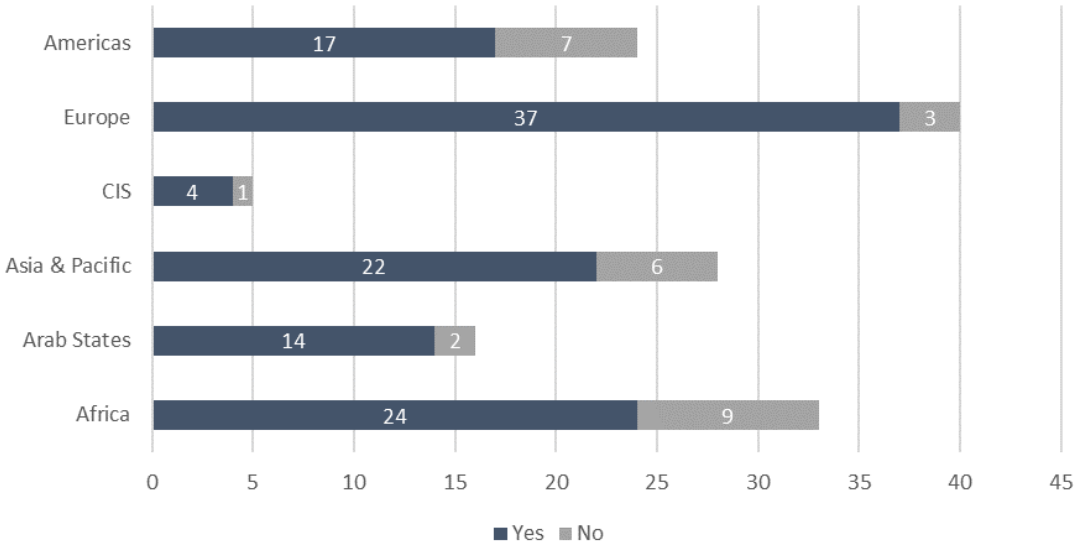
While recognizing that the new shift in regulatory perspectives is important, the regulatory frameworks of many countries still lack fundamental elements. These limitations impede the development of their ICT sector. *The State of Broadband 2019* report from the Broadband Commission for Sustainable Development noted that 72 countries are still at either a G1 basic level of ICT regulatory policy with regulated public monopolies and a command-and-control regime or entering a G2 level with the beginning of market liberalization, partial liberalization, or privatization (Broadband Commission for Sustainable Development 2019). These countries may miss out on development opportunities, leading them to further lag behind G3 and G4 countries that have enabled innovation and integrated ICTs into socio-economic policy. The adoption of comprehensive digital strategies, as addressed below, are key tools, but reform of the underlying systems and structures may need updating as well.

Implementation of comprehensive and technology-specific digital strategies

Digital strategies, plans, and roadmaps help identify policy goals and set targets. At least 73 countries have adopted a digital strategy or plan (ITU 2020), including Colombia, Uruguay, Niger, and Kenya. For example, in Colombia, the Ministry of Telecommunications and Information Technologies (MINTIC) released a new ICT Plan 2018-2022, *The Digital Future is for Everyone* (MINTIC 2018). Similarly, in Uruguay, the Digital Agenda 2020 seeks to advance the country's digital transformation in an inclusive and sustainable manner with "proximity government" as one of the main objectives. Proximity government encourages different methods of approaching the relationship between citizens and the state, while promoting transparency, accountability, participation, and the development of better services. This is intended to generate direct contact channels between citizens and government and improve the quality of care in services provided (AGESIC 2017). In the African region, numerous countries have also issued digital plans. In 2017, the Nigerian government adopted the *Smart Nigeria Digital Economy Project* aimed at improving economic opportunity and competitiveness. This project includes ICT-related initiatives, such as expanding broadband connectivity, while also focusing on digital solutions, such as increasing e-government, engaging young Nigerians in innovation, training engineers in software development, and fostering e-commerce (World Bank 2019). Kenya, too, adopted a *Digital Economy Blueprint* in 2019, as a roadmap for its digital transformation journey, to ensure that the digital economy benefits become their reality (Republic of Kenya 2019). The blueprint proposes five pillars as foundations for the growth of a digital economy: digital government; digital business; infrastructure; innovation-driven entrepreneurship; and digital skills and values. Beyond the digital-specific, at least 118 countries

have a national development strategy, digital agenda, or economic stimulus strategy that includes broadband (see Figure 1.2).

Figure 1.2. Countries with/without overall national development strategy, digital agenda, or economic stimulus strategy including broadband



Note: **only showing countries with information that is available.**

Source: ITU, Data from global survey regarding broadband policies and incentives.

Although some of these digital strategies may not contain certain key components, such as application across multiple sectors or addressing international development goals, countries are increasingly implementing comprehensive plans that encompass all sectors. Moreover, these plans are key mechanisms for setting connectivity targets and goals, and reinforcing the importance of the digital space in the overall economic and social spheres of a country. They are also valuable tools to advocate for collaborative regulation and the engagement of multiple stakeholders, promoting a holistic approach to digital development and planning.

Another recent trend is for countries to adopt strategies tailored to specific technologies or issues, such as automation, robotics, 5G, AI, and the IoT. In 2017, for example, Malaysia's Ministry of Science, Technology and Innovation (MOSTI) adopted a *National IoT Strategic Roadmap* focusing on three key goals: create a conducive IoT industry ecosystem; strengthen technology entrepreneur capabilities; and become a regional development hub for the IoT (MOSTI 2017). Numerous countries, including Germany, have published artificial intelligence strategies. Australia, Germany, the United Kingdom, and Singapore, among others, have adopted 5G policies or strategy documents. In 2015, the government of Japan issued a *New Robot Strategy*, which includes measures for "realizing the robot revolution", as well as a five-year plan addressing cross-cutting and specific sector issues (Headquarters for Japan's Economic Revitalization 2015).

Assessing the need to modernize and streamline

As policy-makers start to implement their digital plans and adapt their regulatory frameworks to the digital economy, it is crucial that they avoid the mere extrapolation or expansion of

existing, potentially outdated laws and regulations to new players or new topics. Instead, policy-makers should adopt measures – which may include deregulation, a self-regulation, or a coregulatory approach – that will lead to greater innovation, easier deployment of new and emerging technologies, incentivize investment, and focus on inclusivity and collaboration.

Not only does this entail a regulatory impact assessment approach to decision-making, the full scope of past, current, and emerging risks should be reviewed in terms of how well they will meet the country's targets. This will better position regulators to introduce flexible policies that support investment and innovation, thereby promoting a strong digital economy (ICC 2016).

In this sense, governments should shift from a rules-based to a principles-based approach. In the digital era, guidance by high-level principles "are better suited for finding balanced, sound solutions, especially in complex areas" (ITU 2020, 7). The United Kingdom's House of Lords, for instance, proposed in 2019 ten principles for regulating in a digital world, including parity, accountability, privacy, and ethical design (House of Lords 2019).

1.3 Role and institutional design of regulator

Institutional structure of regulator

There are three primary institutional design models for regulators overseeing the ICT sector – the sector-specific regulator, the multisector regulator, and the converged regulator. Traditionally, single-focus, sector-specific regulators were common for the telecommunication sector. In today's ICT and digital landscapes, regulators tasked solely with overseeing telecommunications are less common than converged or multisector regulators. Telecommunication regulators tend to also manage postal services or be responsible for spectrum management. For instance, the Afghanistan Telecom Regulatory Authority (ATRA) and the Barbados Telecoms Unit (TU) manage both telecommunication and spectrum matters.[2]

In addition, multisector regulators, which typically involve a utilities-based regulatory authority, were often established before liberalization of the telecommunication sector. One example is the Office of Utilities Regulation (OUR) in Jamaica, which oversees the telecommunication, power, water, and transportation sectors, although spectrum and broadcasting are handled by two separate agencies.[3] Notably, between 2014 and 2016, Jamaica drafted a bill to create a converged ICT regulator, and this effort remains a goal of the Ministry of Science, Energy and Technology (MSET) (Angus 2014).[4] Other countries with multisector regulators include Denmark (Danish Energy Agency), Bahamas (Utilities Regulation and Competition Authority), and Belize (Public Utilities Commission).

Jamaica's path to a converged ICT regulator is in line with a decades-long trend towards converged regulatory authorities whereby one regulator is responsible for telecommunications, spectrum, and broadcasting/media. In 2007, converged regulators made up about one-third of institutional structures globally (ITU 2018a). By 2017, over 70 per cent of regulators worldwide were converged. Some countries that have established converged regulators over the past several years include Botswana and Singapore. In Singapore's case, the creation of a converged

2 ITU, National Telecommunication Agencies, https://www.itu.int/en/ITU-D/Statistics/Pages/links/nta.aspx .
3 *Ibid*.
4 Ministry of Science, Energy, and Technology (MSET). Invest in Technology, https://www.mset.gov.jm/invest-in-technology/.

regulator provided an improved way to navigate "advances in technology that have blurred the distinction between broadcasting and telecommunications" (MCI 2016). Likewise, in 2013, the Botswana Communications Regulatory Authority (BOCRA) was created from the Botswana Telecommunications Authority and the National Broadcasting Board to address all matters relating to ICTs, broadcasting, Internet, spectrum, and postal services (Botswana 2012).

Traditional areas of responsibilities

Under the first three generations of regulation(G1-G3), and somewhat in G4, the telecommunication or ICT regulator's areas of responsibilities centre on setting and enforcing relatively stringent rules deemed necessary to protect competition and consumers as countries transition from monopoly telecommunication markets. Licensing has been the cornerstone of the regulator's responsibility, often involving extensive application processes to ensure that new entrants possess the needed technical and financial capacity to be successful.

Regulators have also traditionally imposed a range of obligations. Tariff-filing requirements, for example, require providers to submit prices and rates for regulatory approval, which are intended to protect consumers against unfair charges. Interconnection obligations and termination rates have been imposed to ensure that operators, especially new entrants, can access one another's networks. This has also protected consumers by making sure that they can connect to any other person, regardless of which operator provides their service. Regulators often become dispute resolution bodies in cases where parties cannot come to an interconnection agreement, as well as to resolve consumer complaints.

Other traditional areas of regulation include spectrum management and broadcasting, although these responsibilities may be hosted within separate authorities outside of the ICT regulator. Spectrum regulation is essential to protecting against harmful interference and to promote efficient use of spectrum resources while broadcasting has generally focused on content issues.

Shifting mandate/roles of regulators and policy-makers in the digital era

The regulator's traditional areas of responsibilities and institutional design are expected to largely continue in the digital environment. However, implementation of regulation should become less rigid and more flexible. Similarly, regulators' mandates and roles may need to be amended to fully capture the new digital realities, as highlighted starting in G4.

With the increasing prevalence of digital services, regulators are finding that they must address a host of new issues and potentially new areas of responsibility. Many of these focus on online services, such as online Voice over Internet Protocol (VoIP) or online video, and other digital platforms, as well as navigating the IoT, AI, data privacy, competition, cybersecurity, and other technological challenges.

These new areas are not always clearly incorporated into existing regulatory frameworks. Many countries are debating whether their ICT and broadcasting regulators possess the jurisdictional authority to address digital services, digital platforms, and other emerging technologies. As countries begin assessing whether to adapt telecommunication or content regulation to digital services, determining the scope of a regulator's authority can be complex without clear legislative guidance, as highlighted in Box 1.1.

Box 1.1. Jurisdictional challenges for OTT video in India

In India, various courts have been examining whether online video is subject to the Cinematograph Act and therefore within the regulatory purview of the Ministry of Information and Broadcasting (MIB), particularly for certification/licensing requirements. In August 2019, the High Court of Karnataka dismissed a case against several over-the-top (OTT) video providers on the grounds that OTT video is not subject to the Cinematograph Act. Rather than adopt a regulatory framework, the MIB stated in March 2020 that the OTT video industry should create a code of conduct and an adjudicatory authority by mid-2020 (see section on "Self-regulatory models").

Source: Dutta 2020, Oka 2019.

Governments are taking different approaches to ensure that regulators hold jurisdictional authority. Some countries are reforming their legislative frameworks to clearly accommodate new digital services, as the European Union has done with the European Electronic Communications Code (EECC) (see section on "Provider perspectives: managing regulatory compliance"). Another option is to review regulators' competencies to determine whether it is appropriate to expand their mandate or establish a new digital regulator. This is further detailed in the section on "Digital regulators".

Whether a country expands a regulator's jurisdiction or chooses to merge different regulatory authorities, it is important to ensure that the regulator possesses adequate resources to execute its role. This includes staffing considerations in order to have qualified administrators and trained employees. Merging existing authorities into a converged regulator means that experienced staff in different areas, such as broadcasting and ICTs, can be brought together with relative ease. Integration of the staff is essential to help establish a cohesive team. Where a regulator's mandate is expanded, training and capacity-building are vital to ensure that staff understand the various stakeholder positions and underlying legal and market issues. The use of open consultations, stakeholder outreach, and other collaborative, evidence-based decision-making mechanisms are key components to building sound, effective regulatory teams. When it is not feasible to expand the regulator's mandate, cooperation mechanisms to implement collaboration with other agencies may be an alternative to increase knowledge and resources.

Advancing the regulator's skills, independence, and accountability

According to ITU data, in over 80 per cent of countries, the regulatory authority for telecommunications and ICTs is independent from the sectoral ministry in terms of its financing, structure, and decision-making, as of the end of 2018.[5] The regulator's sources of funding can strongly influence its level of autonomy. Generally, a financially independent regulator obtains direct funding through legislative and budgetary allocations, allowing the regulator to identify its budget requirements in a transparent manner. In addition to direct budget allocations, regulators may be funded by licensing and other fees. Particularly if fees from licensees is the regulator's sole source of funding, they face the challenge of setting the appropriate fee for cost recovery that balances adequate funding while not imposing unnecessarily high fees on

[5] ITU, ICT-Eye: Key ICT Data and Statistics 2018, https://www.itu.int/net4/itu-d/icteye/Topics.aspx?TopicID=12 .

licensees. A third mechanism is to allocate government appropriations to the ministry that oversees the regulator and, in turn, the ministry distributes funding to the regulator. However, this mechanism risks decreasing the regulator's independence by introducing the possibility of greater political influence in the regulator's decision-making processes.

In traditional, converged, and digital regulatory settings, an independent regulator is crucial to promoting objective, well-reasoned, and predictable decision-making. In the digital era, an independent regulator is particularly important to ensuring that it can effectively collaborate with other cross-sector agencies, as well as conduct open consultations. These matters are further addressed in the section on "Decision-making and rule-making in a multistakeholder environment".

In addition to independence, regulators should be accountable by remaining free from undue political or market influence. An element of accountability is the publication of all laws, rules, guidelines, and other legal texts – both in draft and final form. In the digital environment, stakeholders from an array of sectors are likely to participate, making online publication the main mechanism for promoting inclusion and collaborative decision-making.

To fully realize the potential of an independent and accountable regulator, its staff should have the necessary skills. Regulators must introduce mechanisms to keep up-to-date on sector developments, both domestically and globally, to understand the financial, legal, social, and technical setting in which they operate. Furthermore, this knowledge must be rooted in experience dealing with these issues to serve as case studies – not exact blueprints – for how to respond to new challenges. They must then put this knowledge to use through effective leadership. This leadership means having the ability to choose the path that fosters innovation and the introduction of new technologies benefits consumers through decision-making and rule-making in a multistakeholder environment, as expanded on further below.

Appropriate institutional structure for digital environment

A handful of governments have begun assessing whether their current regulatory authorities are properly equipped to handle issues relating to a digital environment. Although these discussions are generally in the early stages, analysis involves assessing whether a new separate regulatory body solely dedicated to digital issues is required, whether to expand the functions/mandate of an existing ICT regulator, and/or whether the better model is an ICT regulator with other government authorities responsible for consumer protection, privacy, and cybersecurity, respectively. Examples include Australia, Ireland, and the United Kingdom, as highlighted in Box 1.2. This trend may shift over the coming years as more countries begin reviewing the existing regulator's mandate given the digital transformation.

Box 1.2. Review of digital regulators in Australia, Ireland, and the United Kingdom

Australia. In 2018, the Australian Competition and Consumer Commission (ACCC) launched a digital platforms inquiry in 2018 that consulted on market power issues of digital platforms, including social media, search engines, and other online content platforms (ACCC 2018). In the final report issued in July 2019, the ACCC tasked itself with addressing competition issues in the context of digital platforms while entrusting the Australian Communications and Media Authority (ACMA) with numerous key roles (ACCC 2019).

Ireland. In January 2020, the Irish government tabled the draft Online Safety and Media Regulation Bill in the legislature (DCCAE 2020). Rather than create a new regulator to oversee digital content, one of the bill's key proposals was to replace the existing Broadcasting Authority of Ireland (BAI) with a new Media Commission. The Media Commission would regulate broadcasting and take on the additional role of regulating the audiovisual media sector, including online video.

United Kingdom. In April 2019, the United Kingdom's Department for Digital, Culture, Media and Sport (DCMS) launched a consultation that called for an independent regulator to implement, oversee, and enforce a proposed new regulatory framework to address illegal or harmful content online (DCMS 2019). In February 2020, the DCMS responded to the consultation comments, finding that the existing ICT regulator, Ofcom, was the only regulator referenced as a possible candidate for the online harms regulator. The DCMS reasoned that expanding Ofcom's authority – rather than create a new agency – would enable Ofcom to leverage its expertise, avoid fragmentation of the regulatory landscape, and enable quick progress on the issues (DCMS 2020).

Source: ACCC 2018; ACCC 2019; Department of Communications, Climate Action and Environment (DCCAE), General Scheme Online Safety Media Regulation Bill 2019, https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx ; DCMS 2019; DCMS, Online Harms White Paper: Initial Consultation Response, https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response .

The European Commission (EC) is also in the early stages of considering digital regulation. In its 2020 Work Programme, the EC stated its plan to publish a proposed Digital Services Act (DSA) for public consultation in late 2020 (European Commission 2020). The proposed DSA will update the European Union (EU) e-Commerce Directive and is expected to include digital platform regulation. According to media reports in August 2019, the EC has at least considered various types of digital authorities to "ensure oversight and enforcement of the rules", which could be a "central regulator, a decentralised system, or an extension of powers of existing regulatory authorities" (Fanta 2019). Although it is too soon to determine how the EC will propose to structure the authority in the DSA, it highlights the various options available.

Decision-making and rule-making in a multistakeholder environment

Evidence-based decision-making, regulatory impact analysis, open consultations

Effective regulators ensure that their decisions are sound and reached as objectively as possible to promote regulatory certainty while minimizing legal challenges. Stakeholder confidence in regulatory decisions may be instilled through various key components, including the use of evidence-based decision-making, regulatory impact analyses (RIAs) that assess the likely positive and negative effects of the proposed rule, public consultations, and a commitment to transparency and non-discrimination (OECD 2020). Together, these practices are founded on data collection and analysis, which afford regulators substantial, high-quality information from a wide range of interested parties so that they can base their decisions on sound policy rationales. In contrast, decisions made hastily or through closed-door proceedings can undermine the regulator's credibility and create a perception of undue influence. Figure 1.3 highlights effective processes adopted in Brazil, Colombia, Qatar, and Singapore.

Figure 1.3. Examples of decision-making processes in Brazil, Colombia, Qatar, and Singapore

Brazil	• National Agency of Telecommunications (ANATEL) must conduct an RIA prior to adopting any normative acts, except in situations that are expressly justified.
Colombia	• Communications Regulatory Commission (CRC) must follow specific procedures to adopt regulations, which include publishing draft decisions for at least 30 days to allow for public comments.
Qatar	• Communications Regulatory Authority (CRA) in Qatar publishes all consultations and states that its "decisions must be based on evidence and take into account the views of people and organizations with an interest in the outcome".
Singapore	• Infocomm and Media Development Authority (IMDA) publishes all consultations and regularly engages stakeholders in order to "ensure that guidelines, codes, and standards are up to date and in line with community standards and social norms".

Source: National Agency of Telecommunications (ANATEL), Resolution 612/2013, https://www.anatel.gov.br/legislacao/resolucoes/2013/450-resolucao-612 ; Ministry of Information Technology and Communications (MINTIC), Decree 2696 of 2004, https://www.mintic.gov.co/portal/inicio/14705:Decreto-2696-de-2004 ; Communications Regulatory Authority (CRA), https://www.cra.gov.qa/en/Regulatory-Framework/Public-Consultations ; Infocomm Media Development Authority (IMDA), https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations.

Engaging the full range of stakeholders through open consultations is particularly important when adopting digital regulation because impacted parties extend beyond traditional telecommunication providers. Stakeholders in this setting include consumers, digital platforms, commercial players in other sectors, such as finance, transportation, and health, as well as other government agencies with overlapping interests and jurisdictions.

Regulator perspective: managing internal procedures and monitoring

An important part of the decision-making process is determining how the outcomes will be implemented. Effective regulators must manage the internal procedures for assessing

compliance, which may be accomplished through regular reporting requirements or other inquiries. Regulators should also monitor the progress of implementation. This includes monitoring regulated entities to ensure that they are complying with the rules and covers periodic review of the rules to determine whether they are effective and serving their intended purpose.

Monitoring can challenge many countries, particularly where the regulator has a limited budget, staff, or other necessary resources. These challenges are compounded in a digital environment in which multiple stakeholders must be managed and monitored. Thus, capacity building is a crucial element for an effective regulator.

Provider perspective: managing regulatory compliance

From the providers' perspective, managing regulatory compliance can be a burden, especially for newcomers unaccustomed to the highly regulated telecommunication sector. Expanded definitions of telecommunication services add to these challenges. For example, the EU overhauled its telecommunication framework in 2018 with the adoption of the EECC (European Union 2018). The EECC redefined electronic communications services to include all voice communications, even if they do not use public telephone numbers, as well as to include transmission services for IoT, machine-to-machine communications, connected cars, and other digital activities outside of the traditional ICT sector (see Box 1.3). EU Member States must transpose the EECC into national law by the end of 2020. It will be incumbent on digital players to determine whether – and how – these new rules will impact them.

Box 1.3. Expanded definition of electronic communications services in the EECC

Article 2 of the EECC defines electronic communications service as: "a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

(a) 'Internet access service';
(b) interpersonal communications service; and
(c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting."

Interpersonal communications services (ICS) that do not use public telephone numbers are classified as number-independent ICS (NI-ICS). Although NI-ICS are subject to lighter regulation than number-based ICS (e.g. NI-ICS are not required to obtain a general authorization), many online VoIP providers are facing the prospect of regulatory compliance requirements that they have not encountered before.

Source: European Union 2018.

In addition to expanding the definition of regulated activities, current and new regulated entities must comply with a host of compliance requirements. Although obtaining relevant information, such as revenues, subscriber data, and network deployment data, is an important

role of the regulator in order to understand market developments, regulators should be aware of the costs that unnecessary reporting requirements impose on providers. Thus, reporting requirements should be streamlined and based on a reasoned, well-articulated need for information. Further, reporting and other compliance obligations should be fit-for-purpose and target the appropriate entities. For example, in 2017, the U.S. Federal Communications Commission (FCC) eliminated an onerous annual reporting obligation requiring international telecommunication service providers to submit revenue and traffic data (FCC 2017). The FCC had used this data for decades to monitor competition among international carriers. The FCC reasoned that collection of this information from every international carrier was "no longer necessary as the costs of this data collection now exceed its benefits" (FCC 2017, 2). Instead, the FCC now relies on commercially available data and makes targeted data collection requests to specific providers, if needed.

New stakeholders in the digital regulatory environment must also manage compliance on a potentially global basis. Unlike traditional telecommunication providers that build networks in countries where they have a local presence, digital players often make their services available through the Internet, enabling anyone with an Internet connection anywhere in the world to access the services. The challenge is that digital providers may become subject to domestic law if a country determines that making an online service available to users in the country is sufficient. These new players face the additional challenge of navigating patchworks of regulations where various jurisdictions adopt different, or even contradictory, rules. This underscores the importance of intergovernmental cooperation and collaboration to ensure consistency and predictability for the private sector.

Enforcement and sanctions in the digital landscape

Regulators should approach enforcement similarly to the rule-making process – that is, they should be systematic, objective, and clearly identify the reasons for their decisions only after a thorough investigation. Any sanctions should be proportional to the violation and sanctioned parties should have access to timely review and appeals processes to help hold regulators accountable also. These principles also apply to dispute resolution mechanisms overseen by the regulator.

Policy-makers play an important role in enforcement, even if they are not directly engaged in issuing penalties. This entails ensuring that regulators have sufficient enforcement authority to conduct necessary investigations to find wrongdoing, as well as powers to effectively remedy contraventions. Both policy-makers and regulators may need to clarify procedures with other regulatory agencies, and sometimes courts, where there is sectoral overlap, such as data privacy, cybersecurity, law enforcement, finance, transportation, or competition authorities. This cross-sectoral cooperation can help to safeguard against conflicting outcomes among regulators, as highlighted in Box 1.4.

Box 1.4. The Netherlands: Cross-sectoral cooperation in enforcement

The Dutch ICT regulator, the Authority for Consumers and Markets (ACM), and the Authority for Data Protection (DPA) have a long-standing collaborative arrangement for enforcement of data privacy matters. Under the EU e-Privacy Directive, the ACM is tasked with enforcing "cookies" rules. The DPA is responsible for enforcing the non-telecommunication portions of the e-Privacy Directive, as well as the data protection law. In 2017, for example, the ACM and DPA coordinated an investigation into a website administrator regarding the use of advertising cookies (DPA 2017). While no penalties were assessed, the ACM used its enforcement authority to order the website administrator to remove the use of cookies without obtaining the user's consent. Because the website administrator also processed data on its users' political preferences, the DPA ordered that this data may only be processed for advertising purposes with the users' explicit consent.

Source: DPA 2017.

1.4 Regulatory collaboration

The ubiquity of ICTs across all sectors calls for greater regulatory collaboration among ministries, sector and multisector regulators, and a multitude of stakeholders in order to effectively address the impacts and promote the progress of digitalization. The ITU's concept of collaborative regulation under the five generations of regulation model offers mechanisms and targets for implementing regulatory collaboration at domestic, regional, and international levels.

At the 2016 Global Symposium for Regulators (GSR-16), the ITU introduced the concept of collaborative, or G5, regulation to describe a cross-sectoral approach toward regulation that allows stakeholders to shape a common digital future (ITU 2016). As previously noted, G5 regulation does not mean more regulation, but instead involves more inclusive, evidence-based, and decision-oriented regulation between the ICT regulator and other sectoral agencies.

Box 1.5. G5 definition of regulatory collaboration

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.

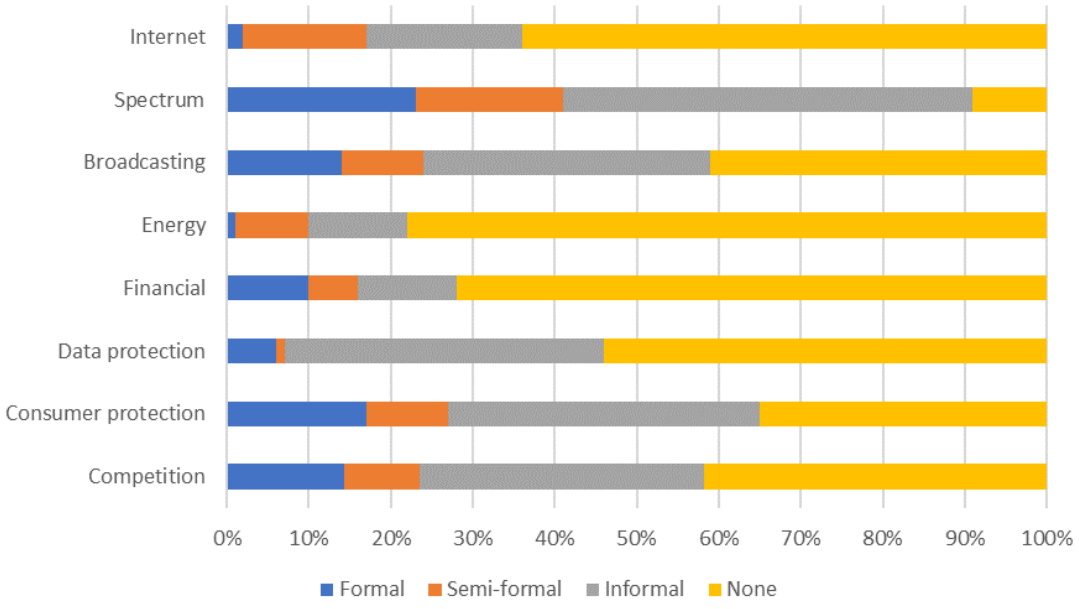
Source: ITU 2018a, 129.

In line with this definition, governments should strive to establish meaningful and sustainable regulatory collaboration between ICT and other regulators.

Formalized and informal collaboration occurring across governments

Government institutions can work together along a spectrum of informal, semi-formal, and formal collaboration mechanisms. Informal collaboration results from outreach between regulators due to mutual interests and capacity building rather than from a planned, institutional framework. Conversely, formal collaboration "…involves systematic efforts to collaborate and define terms of engagement…", such as through memoranda of understanding or legislative means (ITU 2018a). Semi-formal collaboration involves elements of both and is often part of the evolution from an informal to formal structure. Figure 1.4 provides an overview of the state of regulatory collaboration between the ICT regulator and agencies in charge of other matters in countries around the world, with these relationships further detailed below. This data is based on self-reported information from the ITU World Telecommunication/ICT Regulatory Survey 2017 and 2018 (ITU 2018b).

Figure 1.4. State of regulatory collaboration between ICT regulators and other authorities in cases where both exist and are separate entities, worldwide, 2018



Source: ITU 2018a, 130-150.

Note: **Country sample size in order from top to bottom: 48, 22, 92, 116, 172, 72, 101, 92.**

Competition

Competition authorities and ICT regulators often have long-standing coordination arrangements to address overlapping areas of jurisdiction, particularly mergers or market dominance in the telecommunication and ICT sector. Formal collaboration is already the norm among many regulators, including in Namibia, Serbia, and the United Kingdom.[6] Ireland, Romania, and

[6] In the United Kingdom, concurrency arrangements were introduced in their current form by the Enterprise and Regulatory Reform Act 2013 and took effect from April 1, 2014. They created a framework within which the Competition and Markets Authority (CMA) and sector regulators might more effectively work together to improve competition and competition law enforcement in the regulated sectors.

Saudi Arabia are among the countries with a joint programme or committee between the competition and ICT regulators.[7]

Consumer protection

As consumer protection authorities typically are not concerned with one specific sector, their roles have generally relied on collaboration and/or support with other sector-specific regulators. Trends in data privacy and protection, net neutrality, and consumer use of ICT services have all paved the way for collaboration between ICT regulators and consumer protection authorities. As of 2018, two-thirds of existing ICT and consumer protection regulators collaborate in some manner – half of them doing so through an informal framework.[8] Croatia, the Dominican Republic, the Arab Republic of Egypt, Iran, and Moldova use an informal collaboration, while Armenia, Jamaica, Norway, and Thailand, for instance, have formal arrangements.[9]

Data protection

Digitalization relies on data flows. Whether for commercial, government, health, or other institutional purposes, ensuring that information may be collected and processed is crucial to a digital economy but must be balanced with protecting users' privacy rights. Given the role data plays in all aspects of the digital economy, collaboration between data protection authorities and other topic/sector-specific regulators is paramount to creating properly scoped and harmonized digital regulation. Countries have adopted a wide range of data protection frameworks, with the EU model based on the General Data Protection Regulation (GDPR) setting the international trend (European Union 2016). Under the GDPR, which came into effect in May 2018, a stand-alone data protection authority (DPA) sets and enforces the rules. The DPA generally has a clear mandate without significant jurisdictional overlap with the ICT regulator. Although some ICT regulators and DPAs may collaborate, the majority do not have formal mechanisms for collaboration in place, as highlighted in Figure 1.3. Where practised, collaboration is typically informal. In many jurisdictions, an independent DPA is fairly new so this continues to be an area where greater cooperation may evolve.[10]

Other sectors

Collaboration between ICT regulators and other sectoral regulators is also important. Innovation accelerated by ICTs are disrupting and reshaping all sectors and markets. Governments should carefully consider the roles that ICTs play in each sector and what level of collaboration is required between regulators. Table 1.1 presents some of the many topics that ICT regulators should consider for collaboration with other regulators.[11]

---

7 These issues are detailed further in Chapter 2 on "Competition and economics" and Chapter 8 on "Technical regulation".
8 ITU, ICT Regulatory Tracker 2018, https://www.itu.int/net4/itu-d/irt/#/generations-of-regulation .
9 Chapter 4 on "Consumer affairs" delves further into these issues.
10 See Chapter 5 on "Data protection and trust" for more information.
11 These issues are addressed in greater depth in Chapter 7 on "Regulatory response to evolving technologies".

Table 1.1. Example points of collaboration between ICT regulators and other agencies

Non-ICT regulator	Topics of potential collaboration with the ICT regulator
Commerce/trade	Digital taxation, online digital services
Cybersecurity	Data use, end-user devices, IoT
Education	Child online protection, digital divide
Energy	AI, blockchain, IoT
Finance	Blockchain, cybersecurity, financial inclusion, mobile financial services, privacy
Transportation	Cybersecurity, IoT, privacy

Source: TMG 2020.

Singapore has recently stepped up collaborative efforts between the ICT regulator and data protection authority in order to enhance mutually relevant efforts concerning AI, as shown in Box 1.6.

Box 1.6. Singapore government collaborates on artificial intelligence

The Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA) jointly published the first edition of the *Model Artificial Intelligence Governance Framework* in January 2019, intending to frame discussions around the challenges and possible solutions to harnessing AI in a responsible manner. The model framework seeks to collect a set of principles, organize them around key themes, and compile them into an easily understandable and applicable structure. It provides guidance on measures promoting responsible AI usage that organizations should adopt in four key areas: internal governance structures and measures, determining an AI decision-making model, operations management, and customer relationship management.

Source: TMG 2020.

Self-regulatory models

A self-regulatory model allows the government to offload much of its regulatory responsibility to the players most impacted by regulation. These frameworks often stem from a government ultimatum: either industry regulates itself in a satisfactory manner or the government will step in. In India, for instance, the MIB is favouring a self-regulatory model for online video streaming services content. In response, some members of the Internet and Mobile Association of India (IAMAI) are preparing a Voluntary Code of Conduct to be overseen by a Digital Content Complaint Council that will act as an adjudicatory body for digital content matters.

Industry and government collaboration

Representing a bridge between self-regulation and traditional full regulation, the industry-regulatory collaboration model offers governments some control while maintaining industry

autonomy. For example, the COVID-19 pandemic has further highlighted the importance of industry and regulator collaboration. To maintain network stability while an unprecedented number of individuals work, learn, and shelter-in-place in their homes, governments have worked to increase the flexibility of their regulatory frameworks and rely on industry-guided efforts. For example, on March 19, 2020, the EC and Body of European Regulatory for Electronic Communications (BEREC) issued, a joint statement on how to cope with increased broadband network demand as a result of the COVID-19 pandemic. BEREC and the EC stated that Internet service providers are authorized to take necessary measures to mitigate traffic congestion – representing a shift toward a more collaborative regulatory approach (BEREC 2020, European Commission 2020). Simultaneously, digital service providers, such as Netflix, Facebook, Microsoft, and Google, have taken steps to reduce the amount of bandwidth consumed by their services both of their own accord and at the request of regulators. Notably, the ITU has begun curating other examples of these actions and facilitating collaborative discussions through its Reg4Covid initiative.[12]

1.5 Building frameworks for digital regulation

The rise of digital services can impact how telecommunication services are defined and regulated. Amending the definition of telecommunications to encompass new digital services may expand the scope of which types of activities are subject to regulation. For example, whether and how to regulate various types of VoIP services has sparked policy debate worldwide. Although governments may opt for a light-touch regulatory approach, changes to who is regulated and how have broader implications on licensing, competition, and other compliance obligations.[13]

Licensing frameworks for networks, services, and applications

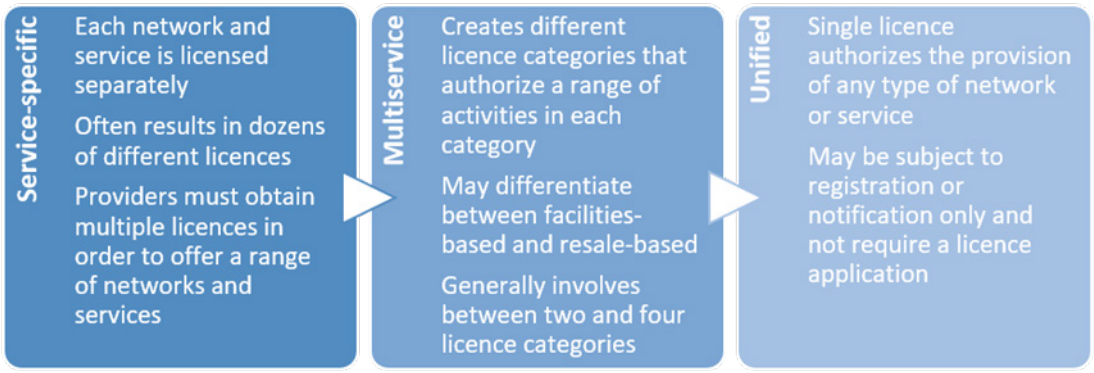
The licensing framework and approach to licensing are key factors determining how easy or difficult market entry is in a country. Choices on licensing regimes and approaches are generally set through high-level policy decisions and adopted in telecommunication legislation, which are then implemented through rules and regulations.

Network/service licences

The type of licensing framework that a country selects can directly impact growth in the sector. Service-specific licensing can restrict market entry by requiring a licensee to obtain a new license each time it wants to add a network or service to its offerings. While service-specific licensing remains in use around the world, multiservice and unified licensing frameworks have emerged as international best practice because they can better streamline licensing, promote technological convergence, and encourage competition. Figure 1.5 highlights the characteristics of these frameworks.

[12] ITU, Reg4Covid, https://reg4covid.itu.int/ (accessed May 13, 2020)
[13] These issues are detailed in Chapter 2 on the "Competition and economics" and Chapter 7 on the "Regulatory response to evolving technologies".

Figure 1.5. Three main types of licensing frameworks



Source: TMG.

For example, between 2013 and 2015, Myanmar reformed its telecommunication sector by moving from a service-specific regime to a multiservice framework involving three main licence categories, differentiating between whether or not the activity is facilities-based (Seint Seint Aye 2015). These reforms led to a digital boom in Myanmar, with mobile penetration rates increasing dramatically from 13 per cent in 2014 to 124 per cent in 2019 (Liu 2019).

These licensing frameworks are oriented for a telecommunications environment rather than a digital, environment. As discussed in the section on "Shifting mandate/roles of regulators and policy-makers in the digital era, how digital services fit into licensing schemes depends on their characteristics and whether their regulation even falls within the mandate of the ICT regulator.

Spectrum licensing

There are multiple ways to authorize the use of spectrum, including through individual licensing of spectrum on a first-come, first-served basis; an administrative award; a competitive mechanism, such as an auction or beauty contest; a class or blanket licence that authorizes a large number of devices (e.g. terminals for satellite broadband or satellite TV dishes); or by identifying certain frequency bands as licence-exempt or unlicensed. For example, in June 2019, the European Conference of Postal and Telecommunications Administrations (CEPT) issued recommendations to European regulators to allow for unlicensed use of the 60 GHz band for 5G services under specified technical conditions (CEPT 2019).[14]

Generally, policy-makers use competitive award procedures for spectrum in which demand exceeds supply. Mobile spectrum, for example, is typically awarded by auction or beauty contest because it is both in high-demand and of high-value. With the promise of 5G technologies, countries worldwide are awarding a large amount of spectrum for 5G, including in Germany, Japan, Singapore, and the Republic of Korea (MIC 2019, IMDA 2020, MSIT 2018).[15]

[14] Chapters 6 on "Spectrum management" examines the various mechanisms for authorizing the use of spectrum, as well as the benefits and drawbacks of each approach.

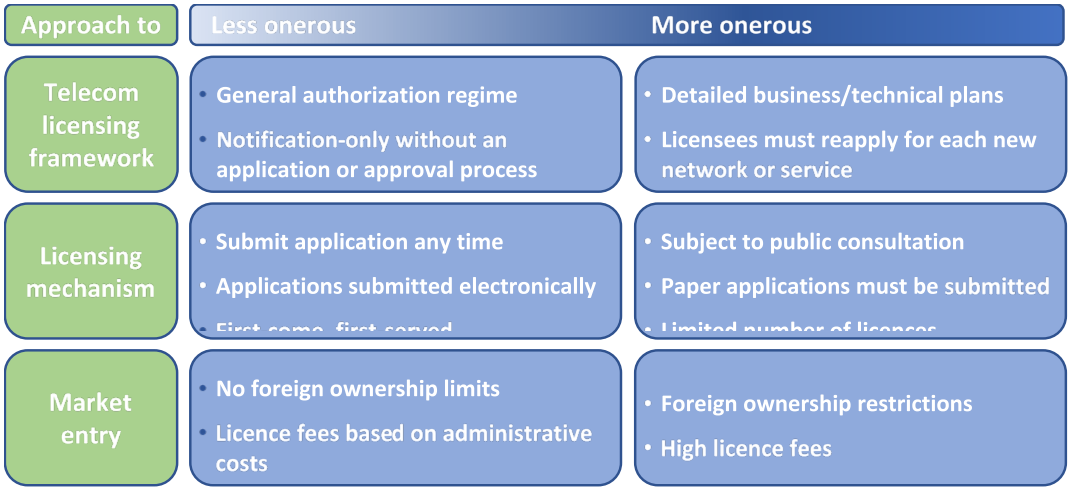
[15] Bundesnetzagentur (BNetzA). Frequenzauktion 2019. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html?nn=267664; Infocomm Media Development Authority (IMDA), Close of 5G Call for Proposal, https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/Close-of-5G-Call-for-Proposal .

Alternative approaches to licensing

In addition to the licensing framework, the approach taken to licensing and regulation impact market entry, competition, and availability of networks and services. The chosen approach should be based on a review of international best practices, meeting regulatory needs without imposing burdensome requirements that unnecessarily impede entry. Even under unified licensing frameworks with quick approval timeframes of one week or less, onerous information requirements can require new entrants to expend large amounts of resources – time and money – simply to prepare application forms.

In some instances, more stringent approaches may be adopted to achieve specific public policy goals, such as coverage obligations in mobile licences. However, a light-touch approach is generally preferred to encourage greater sectoral growth, with any regulatory interventions implemented in a targeted and reasonable manner. Thus, the overall goal is to adopt the least rigid regulatory measures possible to meet policy goals. Figure 1.6 identifies several approaches to licensing frameworks, licensing mechanisms, and market entry in terms of less to more onerous requirements.

Figure 1.6. Licensing approaches: less to more onerous



Innovative approaches to sector regulation

Simply applying existing – and potentially outdated – regulation to new technologies and services risks stifling innovation. To better keep pace with technological developments, policy-makers are examining different measures to provide clear, flexible, and objectively applied rules that avoid hampering progress. These styles of digital regulation include innovative ways to use spectrum, license new technologies, and facilitate universal access.

Innovative spectrum use rules

As new wireless technologies enter the field with existing services, there is an ever-increasing demand for spectrum, including for commercial 5G, satellite services, and fixed wireless, as well as increased spectrum needs for government use. More than ever, rules are needed to ensure efficient

use of scarce spectrum resources. Table 1.2 briefly describes some of these creative approaches, including spectrum sharing, unlicensed spectrum, and private-use licences for the IoT.[16]

Table 1.2. Creative approaches to spectrum use rules

Spectrum use rules	Description	Benefits	Challenges
Spectrum sharing	Multiple users of different applications/ technologies share the same band	Accommodates many users for more efficient spectrum use	Requires some level of management with potential for interference
Unlicensed spectrum	No limit on the number of users in the band on a licence-exempt basis	Enables easy access to spectrum for new and varied uses	No spectrum management means higher potential for interference
Private uses for IoT	Enables local network use for specific industrial functions, such as mining, ports, or health care	Supports IoT for a range of sectors with relatively low risk of interference owing to localized use	May limit the availability of 5G spectrum for wider commercial use

Source: Sayed 2019, Bedi 2018, LVM 2020.

Creative licensing to spur deployment of emerging technologies

Governments are seeking new licensing models to encourage market players, including from outside traditional telecommunication operators, to test and develop technologies. These models include the "regulatory sandbox" and streamlining of demonstration or trial licences. Evolved from the fintech industry, regulatory sandboxes in the telecommunication sector enable technologies and business models to be tested for a specified period. Sandbox licensees are generally not subject to the full regulatory regime but may receive more regulatory guidance than standard licensees. The flexibility of such an approach may also prove valuable in times of crises as temporary measures to test innovative solutions to ensure connectivity. Regulators may also reduce or eliminate fees to further encourage players. Countries pursuing this approach include France and Thailand, as shown in Figure 1.7.

[16] Chapter 7 on "Regulatory response to evolving technologies" and Chapter 6 on "Spectrum management" detail these and other spectrum matters.

Figure 1.7. Elements of the regulatory sandbox model in France and Thailand

Sandbox elements	France	Thailand
Compliance	Full or partial exemption from regulation, on case-by-case basis	Reduced regulation, but must not charge fees or connect to networks
Timeframe	Sandbox licence valid up to two years	Sandbox licence valid up to two years
Regulatory guidance	Regulator assists with administrative procedures until full licence award	Licensees must report on progress to regulator every three months
Examples	Aerospace company testing communications on-board aircraft	Utility company testing microgrid for power and water services

Source: Regulatory Authority for Electronic Communications and Posts (ARCEP). Bac à sable réglementaire (Regulatory Sandbox), https://www.arcep.fr/professionnels/startups-entrepreneurs/bac-a-sable-reglementaire.html ; NBTC 2019.

Creative mechanisms to facilitate universal access

To facilitate access to digital technologies and services, governments continue to use conventional universal service programmes driven by universal access and service funds (UASFs) along with other financing mechanisms. However, because of difficulties with accountability or oversight in implementing UASFs in many countries, other financial mechanisms are preferred, such as pay-or-play arrangements or smart subsidies.

Thus, legacy UASF-based initiatives may be supplemented or replaced with market-based solutions, such as in-kind contributions, to promote demand and reduce operator costs. For example, winning bidders from Germany's 5G auction held in 2019 must comply with extensive coverage obligations, including a requirement to set up 500 base stations in unserved rural areas, called white spots (BNetzA 2019). Licensees must build out the base stations to white spot areas by the end of 2022.

During the COVID-19 crisis, some countries are assigning high-demand mobile spectrum on a temporary basis to ensure access. The Independent Communications Authority of South Africa (ICASA), for instance, announced in April 2020 that it is temporarily assigning spectrum in the 700 MHz, 800 MHz, 2600 MHz, and 3500 MHz bands to existing mobile network operators (MNOs) "for the duration of the national state of disaster in order to ease network congestion, maintain good quality of broadband services, and enable licensees to lower cost of access to consumers".[17]

Chapter 3 on "Access for all" details UAS mechanisms, further analysing trends and best practices to connect the unconnected.

[17] Independent Communications Authority of South Africa (ICASA), Emergency Release of Spectrum to Meet the Spike in Broadband Services Demand due to COVID-19, https://www.icasa.org.za/news/2020/emergency-release-of-spectrum-to-meet-the-spike-in-broadband-services-demand-due-to-covid-19 .

1.6 Key findings

Development of national digital strategies and roadmaps

- National ICT policies and digital strategies, implemented in many countries, are key mechanisms for setting connectivity targets and goals, and reinforcing the importance of the digital space in the overall economic and social spheres of a country. They are also valuable tools to advocate for collaborative regulation and the engagement of multiple stakeholders – promoting a holistic approach to digital development and planning.

Institutional structure and role of regulator

- The ICT regulator, regardless of the institutional structure, requires appropriate independence in terms of funding and day-to-day operations and making decisions, but its framework should recognize and encourage that it plays a collaborative role, sometimes primary, other times secondary, in developing the appropriate framework for a digital landscape.
- Given the impact of ICT in multiple sectors and the broad range of issues brought on by a digital economy, the digital landscape depends on a collaborative and interdependent environment between the regulator, other relevant government authorities, industry, and other key stakeholders.
- Governments need to establish mechanisms – formal and informal – to collaborate with industry and consumer groups on setting policies, rules, and guidelines. Many of the technologies and innovations being deployed are nascent and merit a tempered regulatory environment in order to better assess the appropriate path to promote innovation while protecting against consumer harm.
- Whenever possible, regulators should encourage industry to develop its own guidelines and codes of conduct before taking enforceable measures, since industry often is better equipped to handle dynamic and new issues.
- Policy-makers and regulators should take this digital environment as an opportunity to reassess the need for existing, potentially outdated laws and regulations and should adopt measures—which may include deregulation, self-regulation, or a co-regulatory approach – that will lead to greater innovation, easier deployment of new and emerging technologies, incentivize investment, and focus on inclusivity and collaboration.
- While G5 or collaborative regulation is a key component in developing inclusive policies for a digital environment, certain fundamental regulatory tools will remain under the primary purview of the ICT regulator, such as developing regulations to facilitate connectivity, infrastructure development and foster a competitive sector.
- Regulators should continue to make evidence-based decisions after holding public consultations. Robust consultations are crucial for digital regulation that involves multiple types of stakeholders, which may hail from sectors outside of traditional telecommunication players.
- Implementation and monitoring of regulations is important, both to ensure that regulated entities are complying with the rules and that the rules themselves are achieving their intended purpose. Expanding rules to cover digital services should be carefully considered, including the potential impact of imposing a patchwork of regulation.
- Enforcement should be subject to systematic and objective investigation prior to imposing sanctions while any remedies should be proportional to the violation. Cooperation with other sectoral agencies is useful to ensure consistent outcomes.

Building frameworks for digital regulation

- Licensing frameworks for networks and services should be as streamlined as possible and focus on easing market entry with unified or multiservice licensing representing best practices. For spectrum resources, there are various authorization mechanisms with each serving different policy needs.
- Regardless of the licensing framework, regulators should adopt licensing approaches that achieve regulatory goals without imposing burdensome requirements that impede market entry and growth. Generally, a light-touch regulatory approach is preferred, particularly for digital regulation that now encompasses a broad range of players.
- Emerging technologies and services may be fostered through innovative approaches to regulation, such as spectrum sharing, regulatory sandboxes, or alternatives to UASF mechanisms to achieve universal service. Regulators are positioned to adopt clear, flexible, and objectively applied rules to promote innovation.

References

ACCC (Australian Competition and Consumer Commission). 2018. *Digital Platforms Inquiry: Issues Paper*. Canberra: ACCC. https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/issues-paper.

AGESIC (Electronic Government and Information and Knowledge Society Agency). 2017. *Digital Agenda 2020*. Montevideo: AEGSIC. https://uruguaydigital.uy/wps/wcm/connect/urudigital/44f1500c-6415-4e21-aa33-1e5210527d94/Download+Digital+Agenda+%28English+Version%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=44f1500c-6415-4e21-aa33-1e5210527d94.

ANATEL (National Agency of Telecommunications). 2013. *Resolution 612/2013*. Brazil: ANATEL. https://www.anatel.gov.br/legislacao/resolucoes/2013/450-resolucao-612.

Angus, Garfield. 2014. "Laws Far Advanced to Modernize ICT Sector". Jamaica Social Investment Fund. June 11. https://jis.gov.jm/laws-far-advanced-modernize-ict-sector/

Bedi, Iqbal. 2018. *Setting the Scene for 5G: Opportunities and Challenges*. Discussion Paper. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2018/documents/DiscussionPaper_Setting%20the%20scene%20for%205G_GSR18.pdf.

BEREC (Body of European Regulatory for Electronic Communications), European Commission. 2020. *Joint Statement from the Commission and the Body of European Regulators for Electronic Communications (BEREC) on coping with the increased demand for network connectivity due to the Covid-19 pandemic*. March 19. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9236-joint-statement-from-the-commission-and-_0.pdf. (Accessed: April 16, 2020)

Botswana Government. 2012. *Communications Regulatory Authority Act 2012*. https://www.bocra.org.bw/sites/default/files/documents/COMMUNICATIONS%20REGULATORY%20ACT%2C%202012.pdf.

Broadband Commission for Sustainable Development. 2019. *State of Broadband Report 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

CEPT (European Conference of Postal and Telecommunications Administrations). 2019. *ERC Recommendation 70-03 Relating to the Use of Short-Range Devices (SRD)*. Copenhagen: CEPT. https://cept.org/DocumentRevisions/srd/mg---short-range-devices/11630/SRDMG(17)153_Rec%2070-03%20October%202017.

DCCAE (Department of Communications, Climate Action and Environment). 2020. *General Scheme Online Safety Media Regulation Bill 2019*. Ireland: DCCAE. https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx.

DCMS (Department for Digital, Culture, Media and Sport). 2019. *Online Harms White Paper: Consultation*. DCMS: London. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

DPA (Authority for Personal Data). 2017. "Toezichthouders ACM en AP treden op tegen StemWijzer.nl". Press Release. February 8. https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-acm-en-ap-treden-op-tegen-stemwijzernl.

Dutta, Sweta. 2020. "Curb your OTT Instincts: Government Gives 100 days to Set Up an Adjudicatory Body and Finalize a Code of Conduct". *Mumbai Mirror* March 3. https://mumbaimirror.indiatimes.com/mumbai/cover-story/curb-your-ott-instincts/articleshow/74449516.cms.

European Commission. 2020. *Commission Work Programme 2020*. Brussels: European Commission. https://eur-lex.europa.eu/resource.html?uri=cellar%3A7ae642ea-4340-11ea-b81b-01aa75ed71a1.0002.02/DOC_1&format=PDF.

European Union. 2016. *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)*. Brussels: EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

European Union. 2018. *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. Brussels: Official Journal of the European Union.

Fanta, Alexander. 2019. "Leaked Document: EU Commission Mulls New Law to Regulate Online Platforms". *Netzpolitik*, July 16. https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/ .

FCC (Federal Communications Commission). 2017. *In the Matter of Section 43.62 Reporting Requirements for U.S. Providers of International Services*. Washington, DC: FCC. https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1024/FCC-17-136A1.pdf.

Headquarters for Japan's Economic Revitalization. 2015. *New Robot Strategy: Japan's Robot Strategy – Vision, Strategy, Action Plan*. https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/robot_honbun_150210EN.pdf.

ICC (International Chamber of Commerce). 2016. *Regulatory Modernization in the Digital Economy: Developing an Enabling Policy Environment for Innovation, Competition, and Growth*. Paris: ICC. https://iccwbo.org/content/uploads/sites/3/2016/05/ICC-Digital-Economy-Commission-Policy-Statement-on-Regulatory-Modernization-in-the-Digital-Economy-1.pdf.

IMDA (Infocomm Media Development Authority). 2020. *Internet of Things (IoT) Cyber Security Guide*. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf.

ITU (International Telecommunication Union). 2018a. *Global ICT Regulatory Outlook 2018*. http://handle.itu.int/11.1002/pub/81234575-en.

ITU (International Telecommunication Union). 2018b. *ITU World Telecommunication/ICT Regulatory Survey 2018*. Geneva: ITU. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/ITU_Telecommunication-Regulatory-Survey-2018_E.pdf.

ITU (International Telecommunication Union). 2019. *Digital Infrastructure Policy and Regulation in Asia-Pacific Region*. Geneva: ITU. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/RRITP2019/ASP/ITU_2019_Digital_Infrastructure_5Sep2019FNL.pdf.

ITU (International Telecommunication Union). 2020. *Global ICT Regulation Outlook 2020*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2020-PDF-E.pdf.

Liu, John. 2019. "Telecom Sector Fuels Myanmar's Economy." *Myanmar Times*, December 18. https://www.mmtimes.com/news/telecom-sector-fuels-myanmars-economy.html.

LVM (Ministry of Transport and Communications). 2020. "More Frequencies for 5G – Consultation Round on the Terms of the Spectrum Auction Launched". Press Release, February 2. https://www.lvm.fi/en/-/more-frequencies-for-5g-consultation-round-on-the-terms-of-the-spectrum-auction-launched-1032878.

Maddens, Sofie. 2016. *Building Blocks for Smart Societies in a Connected World: A Regulatory Perspective on Fifth Generation Collaborative Regulation*. GSR-16 Discussion Paper. Geneva: ITU. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_BuildingBlocksReg_GSR16.pdf (Accessed: April 22, 2020).

Mathew, R., 2020. "Netflix to Slash Traffic Across Europe to Relieve Virus Strain on Internet Providers". *Reuters*, March 22. https://uk.reuters.com/article/us-health-coronavirus-netflix/netflix-to-slash-traffic-across-europe-to-relieve-virus-strain-on-internet-providers-idUKKBN21906P (Accessed April 22, 2020).

MCI (Ministry of Communications and Information). 2016. "MCI Restructures IDA and MDA to Seize New Opportunities". Press Release, January 18. https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2016/1/formation-of-infocomm-media-development-authority-and-government-technology-organisation?page=25.

MIC (Ministry of Internal Affairs and Communications). 2019. *Approval of specific base station opening plan for introduction of 5th generation mobile communication system*. Japan: Mobile Communications Division of MIC. https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000378.html.

MINTIC (Ministry of Information Technology and Communications). 2018. *Plan TIC 2018-2022: El Futuro Digital es de Todos* (ICT Plan 2018-2022: The Digital Future is for Everyone). https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf.

MOSTI (Ministry of Science, Technology and Innovation). 2017. *National Internet of Things (IoT) Strategic Roadmap*. Kuala Lumpur: MOSTI. https://www.mestecc.gov.my/web/wp-content/uploads/2017/02/IoT-Strategic-Roadmap-1.pdf.

MSIT (Ministry of Science and ICT). 2018. *Final Result of 5G Mobile Communication Frequency Auction*. Seoul: MSIT. https://www.msit.go.kr/cms/www/policyCom/report/__icsFiles/afieldfile/2018/06/18/180618%20%EC%A6%89%EC%8B%9C%20(%EB%B3%B4%EB%8F%84)%205%EC%84%B8%EB%8C%80(5G)%20%EC%9D%B4%EB%8F%99%ED%86%B5%EC%8B%A0%EC%9A%A9%20%EC%A3%BC%ED%8C%8C%EC%88%98%20%EA%B2%BD%EB%A7%A4%20%EC%B5%9C%EC%A2%85%20%EA%B2%B0%EA%B3%BC.pdf.

NBTC (National Broadcasting and Telecommunications Commission). 2019. *Compliance Guide regarding the criteria for granting the use of radio frequency for the development and testing of innovations in a specific regulatory area (Regulatory Sandbox)*. Bangkok: NBTC. http://www.nbtc.go.th/getattachment/spectrum_management/38995/02-%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD-%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%95%E0%B8%B2%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8-Sandbox.pdf.aspx.

OECD (Organisation for Economic Co-operation and Development). 2019. *Going Digital: Shaping Policies, Improving Lives*. Paris: OECD Publishing. https://www.oecd-ilibrary.org/docserver/9789264312012-en.pdf?expires=1587947608&id=id&accname=guest&checksum=B0115274823F0FB61E9045106E89E38B.

OECD (Organisation for Economic Co-operation and Development). 2020. *OECD Best Practice Principles for Regulatory Policy: Regulatory Impact Assessment*. Paris: OECD Publishing. https://www.oecd.org/gov/regulatory-policy/regulatory-impact-assessment-7a9638cb-en.htm.

Oka, Abhay. 2019. *Writ Petition No. 6050 of 2019 (C) PIL*. High Court: Karnataka. http://judgmenthck.kar.nic.in/judgmentsdsp/bitstream/123456789/292918/1/WP6050-19-07-08-2019.pdf.

Republic of Kenya. 2019. *Digital Economy Blueprint: Powering Kenya's Transformation*. Nairobi: Republic of Kenya. https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf .

Sayed, Tamer. 2019. "Spectrum Management: Strategic Planning and Policies for Wireless Innovation". Presentation at ITU-D meeting on **Spectrum Management: Strategic Planning and Policies for Wireless Innovation**, Algeria, December 1-5, https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2019/SPP4WI/Session%2013%20Spectrum%20policies%20for%20wireless%20Innovation%20Spectrum%20and%20infrastructure%20sharing.pdf.

Seint Seint Aye. 2015. *Telecommunication Licensing Framework in Myanmar*. Myanmar: Posts and Telecommunications Department of the Ministry of Transport and Communication. https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Myanmar/Session6_2%20SeintSeintAye_Myanmar%20licensing.pdf.

Select Committee on Communications. 2019. *Regulating in a Digital World*. 2nd Report of Session 2017–19, HL Paper 229. London: House of Lords. https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf.

SSEACP (State Secretary for Economic Affairs and Climate Policy). 2019. *2019 Procedure on the Provision of Information by ACM*. The Hague: SSEACP. https://www.acm.nl/sites/default/files/documents/2018-01/procedure-on-the-provision-of-information-by-acm.pdf.

TMG (Telecommunications Management Group). 2020. *Overview of AI Policies and Development in Latin America*. Arlington, VAS: TMG. https://www.tmgtelecom.com/publications/overview-of-ai-policies-and-developments-in-latin-america/.

World Bank. 2019. *Nigeria Digital Economy Diagnostic Report*. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf.

World Bank and ITU. 2021 (forthcoming). *Regulatory Watch Initiative*.

Chapter 2. Competition and economics

2.1 Introduction: Regulatory transformation in the digital economy

Over the past 10 years there has been significant market and regulatory disruption caused by digital transformation. This disruption, which is set to continue, extends to almost all corners of the economy, and is primarily the result of a transition to data-centric business models based on digital platforms (ITU 2020a).

Digital platforms are embedding market power and, in a race for scale and scope, leading to transnational markets. This means that regulation is increasingly beyond the scope of individual national regulatory authorities (NRAs).[1] Elsewhere, NRAs have to work in regional collaboration if they are to be effective. This may be done through supranational organizations and regional organizations (e.g. European Commission) or by individual NRAs building on the work of others that have taken a lead on platform and content regulation. Regulators in microstates face particular challenges[2] as the national market lacks the scale to maintain competitive supply models, and they may lack the resources (mainly in terms of readiness and human capacity) to regulate the dominant supplier.

1 ICT regulators or their counterparts elsewhere in government (e.g. ministries or competition authorities).
2 See *Digital Regulation Platform* thematic section on "The specific competition and regulation challenges of microstates".

Legacy national services still exist, and traditional regulation of services and prices will continue for some time, but the need for such regulation within national borders is in decline. This is because traditional services are constrained by over-the-top (OTT) applications on transnational digital platforms. Traditional approaches to regulation are in any case coming under increased pressure because of digital transformation:

- Market definition and analysis is made more difficult by convergence of fixed/mobile, voice/data and traditional/OTT services. The typical regulatory process also takes too long to be effective in markets that are rapidly developing, and the whole market analysis process strains the resources of many regulatory authorities. A simplification of the market analysis process is urgently needed so that it can be delivered in a timely manner while being robust enough to withstand legal challenge.
- Interconnection remains vital where multiple networks coexist, but termination rates can be simplified – set at or close to zero – often without the need to apply costing methodologies and models.
- Licensing will increasingly be achieved via general authorisation for service provision and symmetrical ex-post regulation, i.e. rules that apply to all service providers not just those with significant market power (SMP). For example, regulators should check for anticompetitive bundling of services practices, and limit mergers and acquisitions that have the potential to lessen competition substantially. New competence and, potentially, new competition agencies are needed if this regulatory transition is to be effective.

Although operating as transnational markets, all digital platforms and services still need access to national infrastructure for delivery and customer engagement. The focus of NRAs should therefore be on ensuring this access is available with sufficient capacity, at acceptable quality of service (QoS) and on fair terms.

The ever-increasing demand for data puts pressure on national network infrastructure, especially access networks. The investment requirements to provide adequate bandwidth may be incompatible with competition (especially in least developed countries, landlocked developing countries, small island developing states and also in rural and isolated areas), and in these circumstances licensing requirements and conditions attached to state funding are critical to success. National regulatory authorities should also explore partnership models in which digital platforms share the cost of national ICT infrastructure (with a need to revisit the use of the concept and principles of network externalities).

Setting access network requirements at the right level requires cost modelling and business plan analysis of network roll-out (ITU 2019a). Regulation is about monitoring progress against pre-determined key performance indicators (KPIs). The ability to impose sanctions and remains essential, although fines are never satisfactory.

More generally, extracting value from digital platforms at a national level requires adaptation of taxation policies – potentially based on subscriber numbers and revenues rather than profits. Money raised should be used to fund network deployment and improvement of access – either directly or via an alternative funding mechanism for digital development – in order that the digital economy can be further developed.

2.2 Regulation in the digital era

Historical approach

Before digital disruption, telecommunication networks, services, and markets were primarily national in scope and for the provision of a limited and standardized set of telecommunication services to end users. Most countries had moved well beyond the limitations of monopoly supply, offering some degree of competition and consumer choice. However, until recently, the supply of telecommunication services was largely a one-way transaction in a single-sided market.

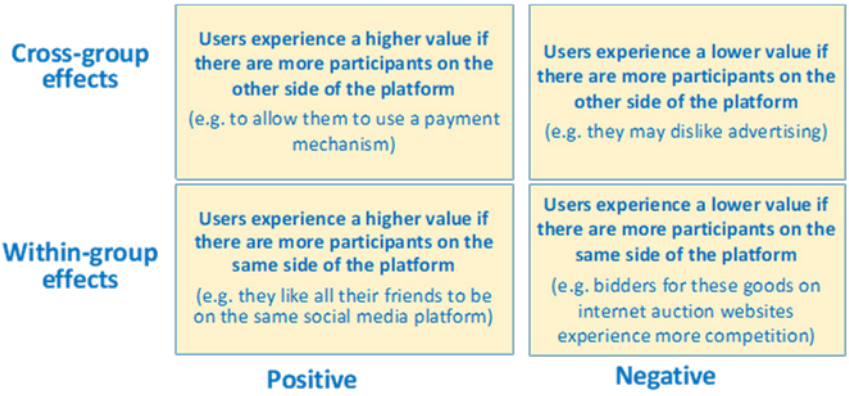
Under the auspices of NRAs, controlling a quasi-competitive market, the supply chain was split into wholesale and retail components. Wholesalers were subject to economic regulation especially where they controlled bottleneck facilities or had SMP. Retailers were generally not regulated or lightly regulated (except for consumer protection[3]), because effective competition could arise based on equal access to wholesale inputs.

Recent developments

Two-sided and multisided digital platforms (e.g. Facebook, Google) have emerged and grown rapidly. Their appeal to customers is based on offering innovative services which appear to cost them nothing (or very little). Purely in terms of price this is true, but the business model of digital platforms relies on customer data (albeit often anonymized and aggregated) to create value that can be monetized on another side of the platform (e.g. to advertisers or content providers). Digital platforms thus act as a marketplace, bringing together and reducing transaction costs between distinct groups of customers.

There are strong network externality effects at play.[4] Network effects describe the impact that an additional user of a service has on the value of that service to others. These externalities can be on one side of the platform or across the platform; they can be positive or negative. If the platform is transactional (i.e. where it enables transactions between customers on either side of the platform) this strengthens externalities.

Figure 2.1. The network effects of digital platforms



Source: ITU 2018a.

[3] See Chapter 4 on "Consumer affairs".
[4] See *Digital Regulation Platform* thematic section on "Explanation of externalities on digital platforms".

Overall, strongly positive cross-group externality effects for digital platforms have led to:

- A race for scale. Scale is critical to enhance service and to lower costs. There are strong first-mover advantages, and established platforms frequently acquire start-up rivals to protect their predominant position.
- A concentration of market power. It is difficult for smaller platforms to compete as they have higher costs and cannot readily match the consumer value of more ubiquitous platforms.
- Transnational and global markets. The more global a platform's reach the greater the network externality effects.
- The fracturing of traditional telecommunication network regulation. Operating outside of the traditional regulated space, and across national boundaries, digital platforms nevertheless compete with and, in some cases, undermine telecommunication network service providers (e.g. OTT service providers have greatly impacted the traditional revenues of telecommunication network providers).

Each of these outcomes could be problematic for economic regulation. They have led to a situation in which:

- Digital platforms are borderless: too large and too wide to regulate;
- Market concentration is excessive: competition is so limited that there are *de facto* monopolies;
- Consumer data funds the system in non-transparent and potentially harmful ways;
- Digital platforms are not making a consistent and proportionate contribution to the national infrastructure that they depend upon.

But consumers do not generally complain. They like the services offered and the low or zero price. Even if consumers have concerns about how their personal data is being used, they are willing to accept (generally without reading) whatever terms and conditions the platform providers impose. This is where regulation must step in: to provide safeguards, monitor operations, and enforce sanctions if needed.[5]

Net neutrality is one area of regulation that has received a lot of publicity. The term "net neutrality" refers to the equal treatment of all data packets, regardless of application, user or price. The key principles have been summarized (FCC 2015) as:

- **No blocking**: network operators may not block access to legal content, applications, services, or non-harmful devices;
- **No throttling**: network operators may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices;
- **No paid prioritization**: network operators may not favour some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind – in other words, no "fast lanes". This rule also bans ISPs from prioritizing content and services of their affiliates.

The ongoing challenge for telecommunication network operators is to provide sufficient bandwidth to support all the applications that the Internet offers and users demand. They are severely constrained in the end-user price that they can set, so they may seek payment from the other side of the market. However, the market power of digital platforms is now so great that the network operator may be unable to extract further revenue. Thus, starved of money on both sides of the market, it may seek instead to block content or throttle demand or prioritize paid traffic simply to cover its costs.

[5] See Chapter 4 on "Consumer affairs" and Chapter 5 on "Data protection and trust".

Although the Federal Communications Commission (FCC) later reversed its decision (FCC 2018), the principles that it espoused in 2015 continue to guide regulators elsewhere. For example, the equivalent European Regulation (EU 2015) requires that , "Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used," although this does not prevent implementation of "reasonable traffic management measures."[6]

In effect, net neutrality principles have been established not as ex-ante regulation, but as a guide for ex-post intervention on a case-by-case basis as required. One article[7] explains that:

> "Broadband access providers and internet content providers are in a symbiotic relationship – each feeds off the other, requiring the other to help it generate revenues and profits. In economic terms, the presence of increasingly powerful internet content providers is providing the necessary countervailing buyer power to curb the dominance of incumbent access providers in national markets, while the demands of a two-sided market mean that the content providers cannot afford to exploit their economic power to the detriment of the organisations that connect them with the very end-users that are the source of that power. The future role of the regulator is going to be much more one of monitoring agreements rather than intervening to set prices or determine quality of service levels. Net neutrality rules are therefore primarily guidelines for ex-post resolution of disputes – which is exactly what the FCC's Open Internet Order suggested."

In Europe, the Body of European Regulators for Electronic Communications issued guidelines to national regulators on the implementation of the net neutrality rules (BEREC 2016) and has subsequently reported each year on the application of the guidelines, with particular emphasis on emerging 5G technologies in relation to net neutrality.

Key findings

- The regulation of traditional networks will continue – although network operators may be small vis-à-vis digital platform providers, they still control access to the customer – but increasingly the focus of regulation needs to be on open and non-discriminatory infrastructure access if it is to continue being relevant and effective.
- Regulators should be wary of authorizing digital platform providers to construct network infrastructure to avoid leverage dominance into the market for network access, but ways should be sought to ensure that digital platforms contribute to the costs of deploying and maintaining access infrastructure.
- Regulation should increasingly be conducted ex post, focused on monitoring agreements and resolving disputes between telecommunication network providers and digital platforms, based on clear principles such as those of net neutrality.
- NRAs must collaborate with one another and with competition authorities to ensure consistent and effective regulation of digital platforms. In these matters the regional/international bodies such as the ITU and Regional Regulatory Associations[8] will play a lead role to ensure coordinated, concurrent regulation. NRAs in developing countries might also build on the work of others that have taken a lead on platform and content regulation, e.g. on the approach to digital platform regulation taken by the Australian

6 See EU 2015, 8 (Article 3).
7 See Rogerson, Holmes, and Seixas 2016, 9.
8 See the ITU website at https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RA_Portal/Home.aspx .

Competition and Consumer Commission (ACCC) in Australia[9] and the work on regulation of OTT services in India.[10]

2.3 The regulation of markets

Historical approach

Economic regulation has traditionally been based on a market analysis procedure that comprises three parts:[11]

- **The definition of markets**. From a regulatory perspective markets are defined on the basis of demand and supply substitutability, with the boundaries of a market based on behavioural responses to a small but significant non-transitory increase in prices (SSNIP) by a hypothetical monopolist providing a single focal product in that market. Markets have by default generally been defined on a national level (occasionally with regional variants).
- **The assessment of dominance or significant market power (SMP)**. Although many economic factors are involved in creating or sustaining a dominant market position, much legislation and most regulatory practice has focused on an assessment of market share (usually revenue-based) as this is the most easily quantified and validated measure. Regulators sometimes assess a range of other relevant factors, such as market concentration, access to finance, economies of scope, technological advantage, and the prospect of countervailing buying power.
- **The imposition of proportionate remedies**. Remedies are imposed ex ante on SMP suppliers in order to prevent them engaging in anticompetitive practices that, absent regulation, they might reasonably be expected to practise. The remedies that are chosen should be the least intrusive remedies that adequately address the specific competition concerns identified. The major categories of commonly imposed remedy are:
    - An obligation to supply
    - Non-discrimination
    - Transparency (e.g. publication of reference offers)
    - Cost-based pricing.

Ex-post remedies are also available if and when specific anticompetitive practices are identified (e.g. predatory pricing, exclusionary behaviour, tying and bundling).[12] The market analysis process to be followed is similar to that for ex-ante regulation: the aim is to impose proportionate remedies on SMP suppliers. However, ex-post regulation requires the regulator to prove that some behaviour has had anticompetitive effect or intention, and then to impose remedies that will remove and recompense for any harm caused.

Moldova provides a good example of market analysis, which shows how the NRA was able to build on the solid foundations laid down in its first round of market analysis so that subsequent updates followed a streamlined but robust process.[13]

9 See *Digital Regulation Platform* thematic section on "ACCC review of digital platform regulation".
10 See *Digital Regulation Platform* thematic section on "OTT regulation in India".
11 For a full description see Blackman and Srivastava 2011, 32ff; and ITU 2016.
12 For a full description see Blackman and Srivastava 2011, 38ff.
13 See *Digital Regulation Platform* thematic section on "Market analysis in Moldova".

Recent developments

The rise of digital platforms and the consequent increase in competition from service providers independent from telecommunication network operators, has radically altered the landscape in which regulators attempt market analysis. In particular:

- Markets can no longer be presumed to be national in scope; and market analysis is harder for NRAs who cannot demand or easily obtain relevant data from global players.
- Market definition is complicated by the presence of two-sided digital platforms[14] – is there a single market covering both sides of the platform or two different markets?
- The SSNIP test is hard to use in markets where services are often zero-rated, bundled, or have usage-independent prices. Which price should be raised? What constitutes a SSNIP when the base price is zero?
- One dominant player in a market may no longer be an undesirable (or avoidable) state of affairs. One platform with high market share may be the welfare-maximizing market structure reflecting high network effects. An explosion in demand for data leading to large-scale network investment may be, in many cases, incompatible with competitive market models.
- SMP designation (and regulatory remedies) therefore needs to be based on a much broader range of indicators (e.g. service differentiation, congestion, access to data, innovation, barriers to entry, and barriers to expansion.)
- Many behaviours previously considered anticompetitive are now part and parcel of legitimate business models, e.g. some pricing below marginal cost and some tying of services are common features of digital platforms. There will still be genuine concerns about predatory pricing and exclusionary behaviour, but they will be much harder to detect and prove.

Key findings

- Traditional ex-ante regulation based on market definition, dominance, and determination of remedies will continue to be important specifically for the regulation of network infrastructure access.
- More generally, there will be refocusing of competition regulation with a transition to ex-post symmetrical regulation (the same rules applied to all suppliers) with regulatory intervention targeted at specific cases of competitive harm, and with high levels of cross-sectoral regulatory cooperation.
- These changes are necessary because:
    - The traditional focus on SMP-based regulation was intended to enable others to compete fairly but digital platforms, access networks, and even entire national broadband networks, may now sometimes be best delivered as virtual monopolies;
    - Even where competition exists it is increasingly hard to define markets, determine thresholds for SMP, and determine and apply appropriate remedies;
    - Under the current regime, some cross-border operators are too big to fail and/or too large to challenge – they can and do act with regulatory impunity.
- Symmetrical regulation will be based on broad regulatory principles such as fair, reasonable and non-discriminatory access to resources.
- For ex-post regulation to be effective, countries need to establish and adequately resource separate competition authorities (or assign equivalent powers to the NRA).

[14] See *Digital Regulation Platform* thematic section on "Approach to market definition in a digital platform environment.

2.4 Interconnection of networks

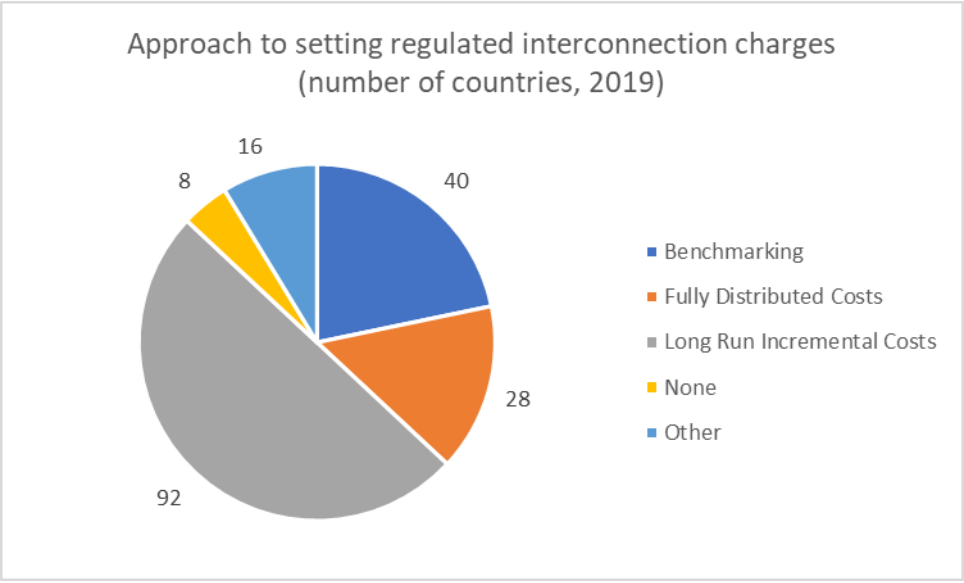
Historical approach

Any-to-any connectivity was a fundamental requirement in newly liberalized telecommunications markets, ensuring that all users could connect with each other regardless of network operator.[15] Interconnection between competing networks was therefore essential and, because of the imbalance of power between incumbents and new entrants, commercial negotiation could not produce fair, reasonable and procompetitive outcomes.

The principle of regulated interconnection was extended to include wholesale access to any technically or commercially feasible component of an incumbent or SMP operator's network. The aim was to create a "level playing field" in which new entrants could choose, without prejudice, between building their own infrastructure and renting from the incumbent, through either access or interconnection. Given this regulated access to necessary wholesale inputs, new entrants could replicate the retail offers of the SMP provider.

For the entrant's build-or-buy decision to be neutral, regulated access and interconnection charges had to be cost based. Much thought and effort went into determining the most efficient cost-standard to be used, gradually settling on the use of long run incremental costs with a mark-up for common overheard costs (LRIC+). Most regulators constructed their own cost models bottom-up (i.e. simulations of actual networks based on efficient economic and engineering practices), giving rise to the acronym BU-LRIC+ as the widely adopted cost-standard. However, in some places (most notably the European Union[16]) even lower rates, based on "pure LRIC" were used for call termination. Pure LRIC represents the difference in total costs with and without the supply of the termination service, divided by the number of call termination minutes.

Figure 2.2. How cost-based interconnection prices are set



Source: ITU.

[15] For a full description see Blackman and Srivastava 2011, 119ff.
[16] The historical development of interconnection rates in the European Union is described in *Digital Regulation Platform* thematic section on "The decline and fall of mobile termination rates in Europe".

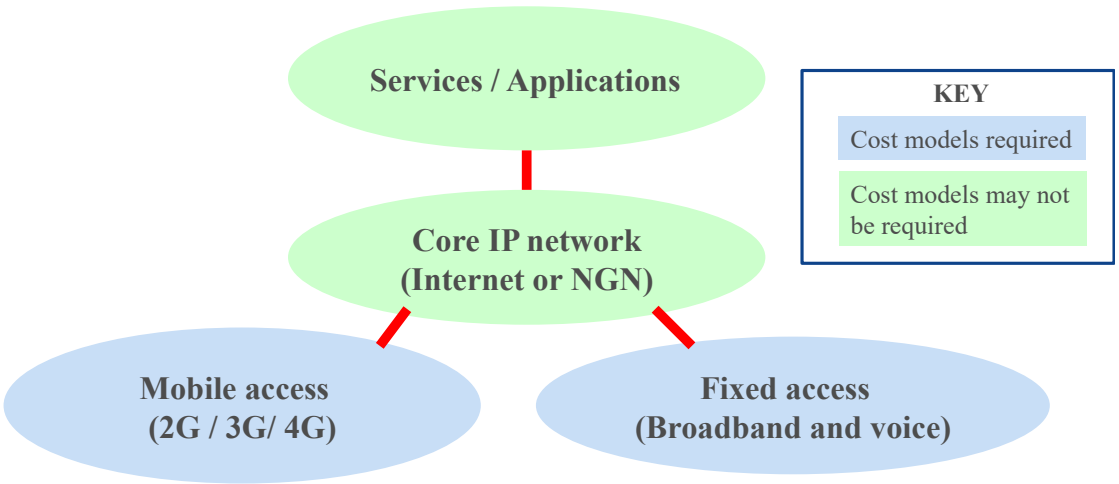
Recent developments

Voice and SMS interconnection continues to be important especially for countries, such as in Africa, where 2G is the most widely used technology either for networks or/and for devices and services. However, data-centric networks, based on the Internet Protocol (IP) have radically changed the service supply chain, affecting costs and prices, and requiring a rethink of traditional regulatory practices. The tendency in IP networks is to have fewer network nodes, centralized service functionality, and multiple transmission paths used for the same communication. All of this results in high-fixed and low-variable costs, thus making usage-based charges somewhat theoretical.

The transition to IP networks affects the fundamental requirement for cost-based regulation, especially for interconnection services. The IP world is dominated by data traffic: voice is a diminishing and insignificant part of the overall network capacity, so cost-based voice termination is of marginal significance.[17] Regulatory cost models for the core IP network may not be needed at all; as competition thrives, there is potentially less SMP and less need for ex-ante regulation.

As the need for regulated cost-based interconnection is reducing, the need for regulated cost-based access is increasing. Application providers require open access to digital infrastructure, as it is only through that infrastructure that they can reach their customers. In many cases, especially for bandwidth-intensive applications such as video, they require access to high-capacity infrastructure. This requires investment on the part of the access provider (e.g. fibre roll-out for fixed networks or 4G/5G mobile technology) that will need to be recovered either directly from the customer or via the application service provider.

Figure 2.3. Regulatory cost models should focus on access prices



Source: ITU, 2019b.

Key findings

- While continuing to support interconnection of traditional circuit-switched networks, effective ICT policy and regulation will need to pave the way for the deployment of very high capacity networks (VHCNs) such as fibre, Data Over Cable Service Interface Specification (DOCSIS) cable, and 5G mobile. The timing of the deployment will vary by country.

[17] See *Digital Regulation Platform* thematic section on "How the growth in data affects interconnection charges".

- There are two basic models for achieving this:
  - A single national broadband network either state-owned or operated under a public-private partnership (e.g. Mexico's *Red Compartida*[18])
  - A regulatory environment that provides incentives for market-driven deployment of high-speed broadband networks (e.g. the European Electronic Communications Code[19]).
- Whichever model is used, access prices must be regulated so as to reward investment in VHCNs but also to encourage reuse and sharing of passive infrastructure wherever possible (see the "Infrastructure sharing" section below and ITU 2018c) and ensure affordability.
- BU-LRIC+ pricing remains valid, but more emphasis should be placed on access to infrastructure and much less on voice call termination. For example, in the European Union, voice termination charges are now being set on the basis of "Eurorates" – standard cost-based rates applicable across all Member States.[20]

2.5 Infrastructure sharing

Historical approach

In the early days of liberalization there was persistent debate about the merits of facilities-based competition and services-based competition. The former prioritized the competitive supply of infrastructure, even if it resulted in less consumer choice in terms of service providers. The cost of duplicating infrastructure was considered to be small relative to the consumer benefits of choice and innovation that would flow from competitive supply models. The United Kingdom and the United States in the 1980s and 1990s were prime examples of countries that gave priority to facilities-based competition.

Even where facilities-based competition was promoted, regulators soon realized that the barrier to market entry was high, and the "ladder of investment" theory was proposed (Cave 2006). The idea was that if various forms of infrastructure access were possible, then investors would be able to choose their entry point and then to increase their investment step-by-step until they became full facilities-based operators. This required access at every technically and commercially feasible point in the network, to provide a full suite of different infrastructure sharing options including passive (civil engineering) assets, active electronics, and radio frequency spectrum.

Recent developments

The need for infrastructure sharing has become greater as the investment required to construct and maintain broadband digital infrastructure has increased. Just as the transformation towards a digital economy was taking shape, the global financial crisis of 2008-2009 curtailed the availability of investment funds; and a similar dynamic is being felt today as the need for 5G mobile and Internet of Things (IoT) investment is juxtaposed with the global recession emerging as a result of the COVID-19 crisis.

---

18 See *Digital Regulation Platform* thematic section on "Red Compartida".
19 See *Digital Regulation Platform* thematic section on "European Electronic Communications Code".
20 See *Digital Regulation Platform* thematic section on "The decline and fall of mobile termination rates in Europe".

Infrastructure sharing is therefore likely to be a permanent feature of the telecommunications landscape. There is a global trend towards permitting infrastructure sharing and, in many cases, mandating the sharing of bottleneck elements in the supply chain: local loops, ducts, towers, and sites. A good example is provided by Brunei Darussalam in which all fixed and mobile networks have been merged into a single new entity, to which all service providers have equal access.[21] More usually, there will not be common ownership of assets, but there remains the need for open and non-discriminatory access to shared infrastructure (e.g., to the submarine cable in the Seychelles).

In most jurisdictions, the terms of infrastructure sharing are set through commercial negotiation, but regulators may publish guidelines and may be required to resolve disputes (see section on "Dispute Resolution" below). Best practice principles for infrastructure sharing regulations include:[22]

- The regulatory framework should apply to all sector participants.
- All types of sharing should be permitted as long as competition is not adversely affected.
- All sector participants should have the right to request to the sharing of infrastructure that has been mandated for sharing.
- All sector participants when requested are obliged to negotiate sharing of their (mandated) infrastructure.
- Operators designated as having SMP in a passive or active infrastructure market are required to publish a reference offer approved by the NRA.

  Commercial terms for infrastructure sharing should be transparent, fair/economic and non- discriminatory.
- The approval process for new infrastructure should be timely and effective and should encourage infrastructure sharing.
- Dispute resolution process should be cross-sector, documented, timely, and effective.
- The infrastructure sharing regulatory framework should take into account the national broadband plan, universal access and service fund (UASF) policy, and future technology development.

Key findings

- The digital economy requires a scale of investment and a geographical reach that precludes the possibility of full facilities-based competition. This makes infrastructure sharing a regulatory prerogative.
- Prices for infrastructure sharing are best set through commercial negotiation so that they embed a commercial rate of return on investment; but regulators need to have oversight of the terms and conditions so as to ensure that infrastructure owners do not abuse their dominant market position.
- All service providers, including the digital platforms that most require high-capacity infrastructure, should contribute proportionately to the cost of that infrastructure through the payment of appropriate regulated access prices.[23]

---

21 See *Digital Regulation Platform* thematic section on "A single integrated wholesale broadband network in Brunei".

22 Adapted from ITU 2018b, 59, based on guidelines prepared by the ITU for the Communications Regulators' Association of Southern Africa (CRASA) in 2016.

23 See, for example, Digicel 2019.

2.6 Price regulation

Historical approach

Before market liberalization, governments set all prices for telecommunications services as part of the annual budget.[24] The range of services was limited, prices varied little from year-to-year and were generally high because telecommunication was a revenue source.

After liberalization governments sought to expand the sector through competition and to collect revenue from the sector primarily through "Licensing and authorization" and "Taxation" (see sections below). Price controls were then focused at the wholesale level (see "Interconnection" section) while retail price regulation was relaxed – just how much depended on the extent of competition, but generally the focus was on SMP providers. The key regulatory discipline was forbearance: intervening only where necessary to prevent excessive prices or anti-competitive prices.

Typically, regulators have deployed two standards of retail price regulation:

- Price approvals – in which formal approval from the regulator is needed before going to market. Price approvals are best applied only to significant tariffs of licensees that have a dominant market position for the service in question. Unless there are reasonable grounds to oppose a tariff, the regulator should approve tariffs expeditiously so as not to undermine the proper functioning of the market.
- Price notification – in which tariffs are submitted to regulator for information purposes only. This approach is appropriate where the service provider does not have SMP, where the service in question is of relatively minor significance and for short-term promotional offers.

The tariff regulations in Iran[25] provide a good example of these procedures.

Recent developments

The aim of traditional retail price regulation has been to limit interventions to those situations where suppliers with SMP might otherwise exploit their market position to the detriment of consumers. However, with increasing direct and indirect competition from unregulated digital platforms, retail tariffs of all telecommunication providers, even those with SMP, are severely constrained.

The role of price regulation is therefore changing – it is now more concerned with ensuring fair competition amongst facilities-based service providers rather than protecting end users directly. The regulatory risk is not in overcharging, but in predatory pricing that leads to underfunding of network development. Broadband service pricing is complex (affected by factors such as the average or minimum download and upload capacity, usage caps, and contract duration) and this gives dominant suppliers more opportunities for anti-competitive pricing (e.g. by tying customers to long-term contracts or failing consistently to deliver the advertised upload/download speeds).

Also, in order to meet the challenge of OTT service providers, telecommunication network operators are increasingly using zero-rating, and bundled tariffs (e.g. for "quad-play" combining broadband Internet access, television, fixed-line telephone, and wireless service) and making greater use of price-promotions to circumvent legacy regulatory price controls. Many of these

[24] For a full description see Blackman and Srivastava 2011, 150ff.
[25] See *Digital Regulation Platform* thematic section on "Price approval and notification procedures in Iran".

developments are positive for consumers and need not result in regulatory interventions. However, regulators need to check for practices that spill over into anti-competitive behaviour.[26]

Key findings

- Regulators should generally take an active monitoring or "watching brief" attitude to retail price regulation: intervention will be principled but ex post.
- Ex-post regulatory intervention in response to complaint or concern may be sufficient for most situations (e.g. of predatory pricing or margin squeeze).
- Service providers should regularly file data on subscription numbers, service tariffs, and volumes so that the regulator can act quickly where necessary.
- A specific focus should be on entry-level products (especially for Internet access) to ensure affordability, including zero-rating where it does not unduly distort service competition.
- As the costs of supplying Internet access are higher in some countries (e.g. those that have low population density, are islands or are landlocked) (A4AI 2018, s4.2), it is important to adopt policies that help to reduce those costs (e.g. through public investment, targeted subsidies, or tax breaks) so as to improve Internet access and affordability.[27]

2.7 Dispute resolution

This section refers to disputes between operators with a specific focus on interconnection and pricing disputes.[28]

Historical approach

The national ICT regulatory authority often has a statutory responsibility for resolving disputes between licensees, as described in Chapter 1 on "Regulatory governance and independence".[29] The World Trade Organization (WTO) Agreement on Basic Telecommunication**s** (WTO 1996) requires member countries to establish an independent body for dispute resolution, and typically those responsibilities are invested in the regulator. Generally, rather than imposing outcomes that might be subject to legal challenge, regulators have sought to mediate in disputes between operators to achieve an outcome acceptable to all parties.

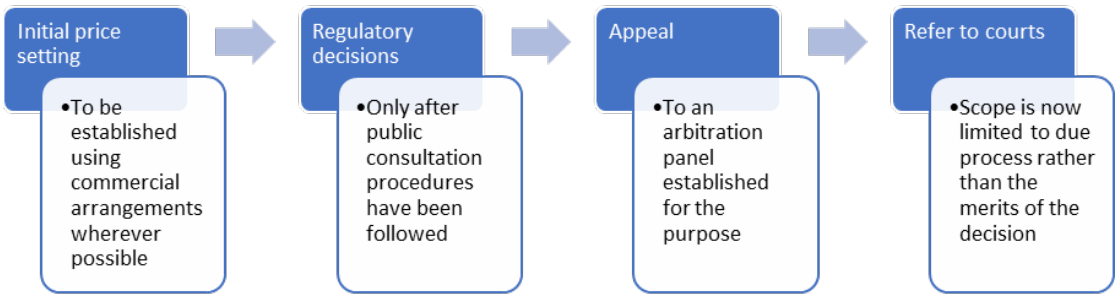
The main reasons for adopting alternative dispute resolution mechanisms are to avoid the high costs, uncertain outcomes, and delays inherent in court proceeding. In some cases where a decision taken by the regulator gives rise to a dispute, the effective final arbiter is an independent body (e.g. the ICT Appeals panel in Papua New Guinea or the Communications and Multimedia Appeals Tribunal in Kenya).[30] However, in some cases the stipulated process is so similar to a formal court that there are few if any savings in terms of cost, time, and regulatory certainty.

While alternative dispute resolution can be preferable to formal legal proceedings, it is far better to avoid disputes altogether. Transparent processes (e.g. public consultations), reasoned statements and the use of external advisors have helped to resolve many disputes.

---

26 See Digital Regulation Platform thematic section on "How to regulate price bundles".
27 The UN Broadband Commission's "1 for 2" target is 1GB at less than 2 per cent of monthly gross national income per capita (see Broadband Commission for Sustainable Development 2019, 34).
28 For disputes between operators (or service providers) and end users, see Chapter 4 on "Consumer affairs".
29 For a full description see Blackman and Srivastava 2011, 147ff, and Bruce and others 2004.
30 There will always be an opportunity to appeal to the courts on matters of law and on whether the tribunal failed to properly determine its own jurisdiction.

Figure 2.4. How to mitigate the risk of interconnection/pricing disputes



Recent developments

The telecommunication sector is highly litigious: there are many high-value disputes, but relatively few of them enter into any form of formal dispute resolution. A recent study by Queen Mary University of London (QMUL 2016) found that disputes within the telecom sector were of higher frequency and greater value than in other sectors, and that telecommunication companies have a tendency to prefer litigation rather than arbitration for resolving disputes. A recent case in the Netherlands demonstrates the tendency to use litigation in cases concerning competition and access pricing. The case saw the highest court in the Netherlands overthrow a decision of the national regulatory authority that had determined joint dominance and required cost-based access to the two main fixed network operators.[31]

Despite the proclivity for litigation, arbitration has several key features that make it particularly suitable for dispute resolution in the telecommunication sector:

- Enforceability – the parties agree from the outset to accept whatever is the outcome of arbitration;
- Avoiding foreign jurisdictions – this is especially useful for disputes involving international businesses, such as digital platforms;
- Access to expert decision-makers – with arbitration the decisions will generally be made by a panel deemed acceptable to the parties and comprising the requisite legal, economic, and technical expertise;
- Confidentiality – in some cases, even the fact that there was a dispute may be deemed confidential; in others, the outcome may be published without all the details being made public.

As a result of these features, 82 per cent of industry respondents in the Queen Mary University survey believe that there will be an increase in the use of international arbitration in the years ahead (QMUL 2016, 25).

Regulators have recognized that they have a key role to play in encouraging greater use of arbitration. For example, in the United Kingdom only disputes involving an SMP operator will normally be heard by the regulator, Ofcom, with all other disputes referred for alternative dispute resolution. Ofcom will formally open a dispute only after its scope has been agreed

[31] The case is detailed in *Digital Regulation Platform* thematic section on "Court overturns Dutch regulator's decision on joint dominance".

and the parties submit statements indicating that best endeavours have already been used to resolve the dispute through commercial negotiation.

Key findings

- A formal process of arbitration should be set up as an alternative to litigation, covering matters related to competition, interconnection, access, and tariffs. In some countries disputes may be referred directly to the arbitrator, although others may prefer that disputes are first submitted to the communications regulator. In both cases the arbitrator should hear appeals against decisions reached by the communications regulator.
- Arbitration procedures are especially important in developing countries where the expertise of the courts (and, indeed, of the regulator itself) may be less than that of the operators or service providers who are party to the dispute.
- In larger and more developed markets it may be preferable to use a national arbitration procedure, which means that the arbitration will itself be subject to national legislation and gives the ability for parties to challenge the decision in local courts if necessary. If national arbitration is pursued, international companies such as digital platform entities should be required to participate in the arbitration process as a condition of having access to national populations.
- In smaller and developing countries, international arbitration is likely to be preferable and will be more easily agreed upon by international companies. In these cases, care should be taken to ensure that the "seat" of the arbitration is in a country that has ratified the New York Convention, an international treaty providing reciprocity of enforcement of arbitration awards.

2.8 Licensing and authorization

Historical approach

Licensing has been widely adopted in the telecommunications industry as a rational means of selecting suppliers for a market with high barriers to entry but which, behind those barriers, was prospectively competitive.[32] Licensing a limited number of suppliers enables governments to attract private-sector investment in infrastructure and services. Licences provided the regulatory certainty needed for investment, while also providing a vehicle to enact public policy goals (e.g. on network coverage, quality of service, or price).

However, in some countries licensing came to be seen more as a means for the government to raise revenue, so the number of licences proliferated and/or the price of licences soared (e.g. one-off fees and royalty payments). A wide variety of licence types (and fees) may appear to work for the government in terms of revenue collection, but it restricts convergence and distorts competition within the industry. In such circumstances industry costs soar and industry structure tends to become overly complicated and fragmented.

[32] For a full description of licensing and authorization, see Blackman and Srivastava 2011, 63ff. For a discussion of licence categories and types of licence, see Chapter 1 on "Regulatory governance and independence".

Recent developments

In recent years, there has been a growing recognition that complex licensing rules and excessive fees have dragged down the sector and threaten the entire digital economy. This is not just a matter of licensing fees diverting potential infrastructure investment; it is the imposition of a suboptimal and static market structure on an industry that is characterized by dynamism and economies of scale and scope. As a recent GSMA report (GSMA 2016, 8) concludes, "effective regulation requires a holistic approach that addresses the diversity of all the relevant platforms" and "should enable, not discourage, the realization of economies of scale and scope that represent real savings for consumers".

Such considerations have resulted in a trend towards open competition (where no licence is required) or general authorization (where a limited set of rules apply equally to all service providers within the class). As Figure 2.5 shows, most countries continue to have some service-specific licences, but they have greatly increased the number of multiservice and unified licences, and in some circumstances removed the need for licensing entirely with the creation of licence-exempt categories.[33] The other parallel trend is the simplification of the process of obtaining such an authorization (sometimes called a class licence) – often it involves little more than a simple registration procedure, without any licence fee. The ITU's Global ICT Regulatory Outlook 2020 report (ITU 2020b, 26)[34] concludes that having a general authorization regime is one of the golden rules for unlocking the power of broadband.

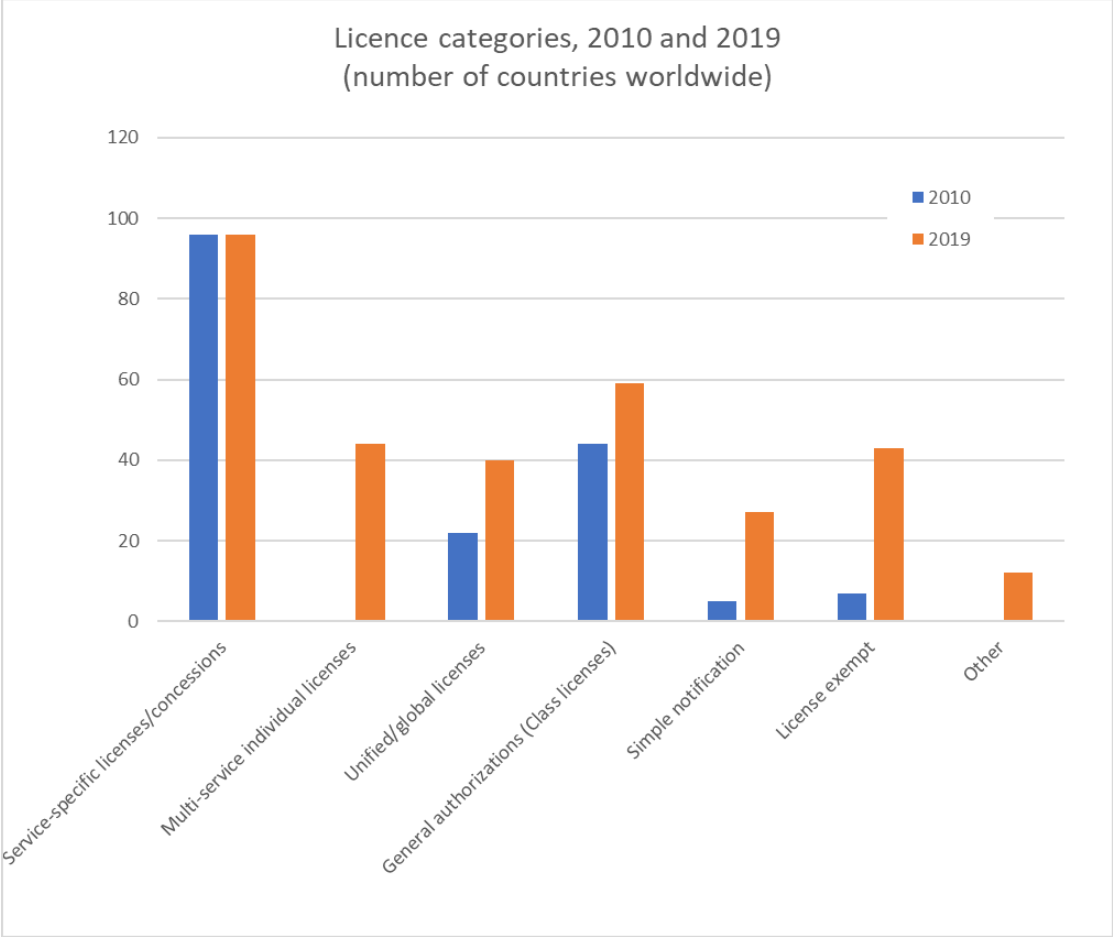
But there are exceptions, especially for facilities-based licences. Convergence has driven the ICT sector towards a small number of network operators, with some countries and territories returning to a network monopoly to maximize economies of scale and scope and ensure national social and economic inclusion.[35]

[33] In 2019, in addition to the figures shown in Figure 2.5, 116 countries report having a licence-exempt regime for wireless broadband devices.

[34] Other golden rules include open competition in services and international gateways, infrastructure sharing, SMP-based regulation and foreign participation/ownership.

[35] For example, see the *Digital Regulation Platform* thematic section on "A single integrated wholesale broadband network in Brunei".

Figure 2.5. The trend towards unified licences/general authorization



Source: ITU.

Key findings

- The objective of licensing is to ensure the effective, efficient delivery of ICT services.
- The optimal licensing structure and the terms and conditions of licences will vary by country; but the objective should never be revenue maximization.
- General authorization is to be preferred and fees should be negligible, set to cover administrative costs only, so as not to deter investment and innovation but also to enhance affordability for consumers.
- Where individual facilities-based licences are issued, the number of licences should be limited to avoid unnecessary duplication of investment, but they should be subject to conditions that provide for open access to key infrastructure on fair and reasonable terms[36] so as to create a healthy, competitive services market.
- Licensees should also be allowed to share infrastructure and to merge, subject only to competition policy considerations.

[36] See, for example, *Digital Regulation Platform* thematic sections on "Red Compartida, Mexico" and "A single integrated wholesale broadband network in Brunei".

2.9 Mergers and acquisitions

Historical approach

Mergers and acquisitions (M&A) are an integral part of a properly functioning competitive market. Routes for existing players to exit the market gracefully are just as important as overcoming barriers to market entry.

M&A activity is only challenged by regulators if it would result in a substantial lessening of competition (SLC): typically, this may occur when an SMP supplier acquires a rival, or two smaller rivals merge to form a putative SMP supplier. However, the SLC test is speculative and difficult to apply because it involves assessing future market competitiveness under two future scenarios – with and without the merger – and then determining whether the difference is significant.

Good practice involves all mergers that pass certain threshold criteria being submitted for approval by the competent authority (e.g. national competition authority if it exists, working in collaboration with the ICT regulator). For example, in the United Kingdom, a merger usually qualifies for investigation by the Competitions and Markets Authority (CMA) if the business being taken over has a turnover in the United Kingdom of over GBP 70 million (about USD 86 million) or the combined business has greater than 25 per cent market share. Such threshold criteria are in place to avoid having to untangle a deal later – which is much more onerous process than simply preventing a merger or acquisition in the first place.

Recent developments

Mergers of licensed network operators have become commonplace as companies seek to achieve scale, provide universal coverage, and enable investment in 4G/5G and fibre networks. This gives rise to concerns about concentration, oligopolistic markets, and joint dominance.

Major digital platforms (such as Google, Facebook, and Amazon) have frequently acquired smaller rivals (such as YouTube, WhatsApp, Instagram) in order to protect their market dominance.[37] The price paid is often excessive compared to market capitalization. Major platforms, Amazon in particular, is vertically integrating both forwards and backwards along the supply (or value) chain, so that it competes with suppliers and customers and exploits central dominance in new markets. Over time these activities have ossified digital markets, creating a "kill zone" around the big firms in which no new entrants can survive.

The SLC no longer functions well in determining whether regulators should intervene in M&A activity.[38] In general, the M&A activities of digital platform providers do easily pass the SLC test (they have only an incremental impact on the acquirer's market share) but they nevertheless ensure that no embryonic company can ever gain the scale necessary to rival the network effects of the acquirer. New approaches are needed. In particular, such approaches need to look at market power not just in terms of revenues and subscribers, but also in terms of access to consumer data and the algorithms necessary to analyse and use that data, including potentially for anti-competitive purposes.

---

[37] See *Digital Regulation Platform* thematic section on "M&A activity of the main digital platform providers".
[38] See *Digital Regulation Platform* thematic section on "Vodafone/TPG operational merger – SLC test no longer works well" for a recent case study.

Key findings

- The legal framework should be modernized to give more scope for preventing and permitting M&A (as, for example, has recently occurred in Germany[39]).
- Resource the regulatory body appropriately, both in the number and the skills of staff, in order to address new types of M&A analysis.
- If M&A approval is subject to conditions, those conditions must be met before the merger or acquisition is undertaken.
- Enhance competition authority powers to move beyond fines (which are easily absorbed as the cost of doing business) and imposing a greater array of conditions (which are not easily ignored).
- Ensure that analysis of M&A involves multiple agencies across all affected economic sectors so that regulatory decision reflect the full impact of M&A on markets and consumers.
- The default outcome of a competition enquiry (triggered by relevant threshold criteria being met) should be to block M&A unless it can be proved to be in long-term consumer interests.

2.10 Taxation

Historical approach

Corporate taxes are designed so that all companies pay a fair contribution for the public services that they rely on (just as residents do through income and consumption taxes). Historically, corporate taxes have tended to be based on profit.

The tax burden on telecommunication companies, especially mobile network operators, is often much higher, especially in developing countries. Sector-specific taxes include excise taxes, higher-than-normal value-added tax (VAT), licence fees, spectrum fees, and universal service obligations. In a study of taxes in the mobile sector in 2017, the GSMA found that mobile taxes on consumers and industry accounted for 22 per cent of market revenue and almost a third of these payments are in sector-specific taxes (GSMA 2019, 5). The full extent of ICT taxation is captured in Figure 2.6.

The rationale for these taxes is often that the mobile network operators are better at collecting revenue which is taxable than the government is at collecting taxes directly. This is probably true in many developing countries; however, it also has the unintended consequence of contributing to Internet access being unaffordable for many users across the world, and hence some of the economic and social benefits of the digital economy being lost. An ITU report (ITU 2015, 5) concluded taxation policy needs to be "based on country-specific policy trade-offs between revenue generation and the potential negative impact on the development of the digital sector as well as the telecommunication/ICT market environment". However, as recently as 2019, the Broadband Commission for Sustainable Development (2019, 63) reported that: "while greater recognition has been paid to the issues of affordability of ICT goods and services, and the role that taxation plays in improving affordability, in some cases, there have been notable increases in sector-specific taxes that have impacted adoption and use of connectivity services".

[39] See *Digital Regulation Platform* thematic section on "Germany adjusts its approach to M&A regulation".

Figure 2.6. Types of taxes applied to the ICT sector, world percentage, 2019

	Range of Taxes										
Type of taxes	Content Services	Incoming int'l voice services	Int'l Data Services	Int'l Mobile Roaming	Internet Services	Nat. Data Services	Nat. Mobile Roaming	Nat. Voice Services	OTT Content Services	Out-going Int'l Voice services (IDD)	Pre-paid mobile top-up cards
VAT	0% - 27%	0% - 27%	0 % - 27%	0% - 27%	0% - 25%	0% - 25%	0% - 27%	0% - 27%	0% - 27%	0% - 27%	0% - 27%
Sector Specific	0.1% - 17%	0.1% - 15%	0.1% - 13%	0.1% - 49.77%	0.1% - 40%	0.1% - 40%	0.1% - 26%	0.1% - 49.77%	1.5% - 13%	0% - 40%	0.1% - 49.77%
Sales	3% - 35%	0% - 27%	1.5% - 27%	4% - 27%	3% - 35%	1.5% - 35%	3% - 27%	1.5% - 35%	5% - 25%	3% - 27%	3.65% -35%
Import Duties	5% - 40.55%	5%- 40.55%	5% - 40.55%	5% - 15%	5% - 40.55%	5% - 15%	5% - 15%	5% - 15%	7.7% - 15%	5% - 15%	5% - 25%

Note: Int'l refers to international and nat. to national.

Source: ITU.

Recent developments

Arguably, a mobile communications or Internet tax premium was justified when these were luxury services enjoyed only by the well-off. Taxes collected this way could be considered redistributive. But it makes little sense now that the emphasis is on achieving ubiquitous, affordable access.

As traffic and revenues move to OTT service providers and applications provided over digital platforms, taxes on traditional, usually mobile, services distort the market while broader ICT taxes and fees limit Internet affordability and deepen digital inequality. End-user surcharges for OTT services, such as have been adopted in several African countries, are self-defeating because taxing users tends to reduce the affordability of Internet access and suppress demand, which results in lower GDP and lower tax revenues overall.

Transnational digital platforms often pay much lower levels of tax than national firms – they use base erosion and profit shifting (BEPS) practices that enable tax to be paid in low-tax jurisdictions rather than where economic activity occurs. Multilateral (e.g. Organization for Economic Co-operation and Development (OECD)) and unilateral (e.g. France, India) efforts are being made to establish fairer tax rules for digital platforms so that taxes are based on revenues generated in-country or based on profits proportional to the platform's revenues in each country.[40] Other important features are simplicity and predictability.

As stated in the *Global ICT Regulatory Outlook* (ITU 2018b), taxation of the digital economy is a challenge faced globally and various approaches are being established. Governments should collaborate closely on digital services taxation matters at regional and international level, and should not compromise long-term, national economic benefits by targeting short-term revenue. In addition, it is relevant to establish effective mechanisms for collaborative regulation, given that taxation decisions fall to finance ministries and tax authorities rather that ICT authorities, for example, working together with all parties before making decisions.

[40] These trends are explored further in *Digital Regulation Platform* thematic section on "Unilateral and bilateral approaches to resolving BEPS".

Key findings

- Taxation of digital platforms and services based on their revenues (rather than profits) makes economic sense because of substantial network externality effects and because revenues are not subject to internal transfer pricing policies.
- Tax levels should not be such as to render universal access to digital services unaffordable: revenue-based taxes should be mitigated where, for instance, the service provider invests in the country (e.g. deploying infrastructure, covering rural and isolated areas, and creating jobs).
- At national level, governments should promote policies that (ITU 2018b):
    - encourage balanced and harmonized taxes;
    - avoid excessive burden to all stakeholders;
    - promote both innovation and effective competition among all sector players in the digital ecosystem; and,
    - consider affordability as a priority.

References

A4AI (Alliance for Affordable Internet). 2018. *2018 Affordability Report*. Washington, DC: A4AI. https://a4ai.org/affordability-report/report/2018/#executive_summary.

BEREC (Body of European Regulators for Electronic Communications). 2016. *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*. Brussels: BEREC. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

Blackman, Colin and Lara Srivastava, eds. 2011. *Telecommunications Regulation Handbook: Tenth Anniversary Edition*. Washington, DC: World Bank and Geneva: International Telecommunication Union. https://www.itu.int/pub/D-PREF-TRH.1-2011.

Broadband Commission for Sustainable Development. 2019. *State of Broadband Report 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

Bruce, Robert R., Rory Macmillan, Timothy St. J. Ellam, Hank Intven, and Theresa Miedema. 2004. *Dispute Resolution in the Telecommunications Sector*. Discussion Paper. Geneva: International Telecommunication Union and Washington, DC: World Bank. https://www.itu.int/ITU-D/treg/publications/ITU_WB_Dispute_Res-E.pdf.

Cave, Martin. 2006. "Encouraging Infrastructure Competition via the Ladder of Investment". *Telecommunications Policy* 30 (3-4). https://doi.org/10.1016/j.telpol.2005.09.001.

Digicel. 2019. "OTTs and Network Infrastructure". A contribution to ITU-D Study Groups, Question 3/1 and Question 4/1 joint session on the Economic Impact of OTTs on National Telecommunication/ICT Markets, October 2019. https://www.itu.int/dms_pub/itu-d/oth/07/1a/D071A0000030001PDFE.pdf.

EU (European Union). 2015. Regulation 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access, 25 November 2015. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en.

FCC (Federal Communications Commission). 2015. Open Internet Order 15-24. https://www.fcc.gov/document/fcc-releases-open-internet-order.

FCC (Federal Communications Commission). 2018. Restoring Internet Freedom Order. https://www.fcc.gov/restoring-internet-freedom .

GSMA. 2016. *A New Regulatory Framework for the Digital Ecosystem*. London: GSMA. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/NERA_Full_Report.pdf.

ITU (International Telecommunication Union). 2015. *The Impact of Taxation on the Digital Economy*. GSR15 Discussion Paper. Geneva: ITU. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR16_Discussion-Paper_Taxation_Latest_web.pdf.

ITU (International Telecommunications Union). 2016. *Principles for Market Definition and Identification of Operators with Significant Market Power*. ITU-T Recommendation D.261, October. https://www.itu.int/rec/T-REC-D.261-201610-I/en.

ITU (International Telecommunication Union). 2018a. "Competition Analysis in Digital Application Environment", Session 11, Regulating Two-sided Markets". ITU Asia-Pacific Centre of Excellence, September 2018.

ITU (International Telecommunication Union). 2018b. *Global ICT Regulatory Outlook 2018*. Geneva: ITU. https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Outlook/2018.aspx.

ITU (International Telecommunication Union). 2018c. *GSR -18 Best Practice Guidelines on New Regulatory Frontiers to Achieve Digital Transformation*. Geneva: ITU. https://www.itu.int/net4/ITU-D/CDS/GSR/2018/documents/Guidelines/GSR-18_BPG_Final-E.PDF.

ITU (International Telecommunication Union). 2019a. ICT Infrastructure Business Planning Toolkit. Geneva: ITU. http://handle.itu.int/11.1002/pub/813e6d7f-en .

ITU (International Telecommunication Union). 2019b. "Costing and Pricing Methodologies in the Digital Economy". ITU, Regional Economic Dialogue on Information and Communications Technologies in Europe and CIS, Odessa, October 2019. ITU, 2020a. Economic Impact of OTTs on National Telecommunication/ICT Markets. ITU-D Study Group 1 report, February. Geneva: ITU.

ITU (International Telecommunication Union). 2020b. Global ICT Regulatory Outlook 2020: Pointing the Way Forward to Collaborative Regulation. Geneva: ITU. https://www.itu.int/pub/D-PREF-BB.REG_OUT01 .

QMUL (Queen Mary University of London). 2016. *Pre-empting and Resolving Technology, Media and Telecoms Disputes. International Dispute Resolution Survey*. London: Queen Mary University of London. http://www.arbitration.qmul.ac.uk/media/arbitration/docs/Fixing_Tech_report_online_singles.pdf.

Rogerson, David, Pedro Seixas and Jim Holmes, *Net Neutrality*, Australian Journal of Telecommunications and the Digital Economy, November 2016. https://telsoc.org/journal/ajtde-v4-n4/a79.

WTO (World Trade Organisation). 1996. *Telecommunications Services: Reference Paper*. Negotiating Group on Basic Telecommunications, World Trade Organization, April 24, 1996, https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

Chapter 3. Access for All

3.1 Introduction

Digital technologies are increasingly a central part of peoples' lives, reshaping the way we live, work, and play and creating new opportunities for social and economic development. Businesses are, in turn, using information and communication technologies (ICTs) to fundamentally transform their processes, increase efficiency, develop new products, and enhance their customers' experience. However, the shift towards an increasingly digital economy can widen the digital divide further between those able to benefit from the digital transformation and those that are not – either because they are in socially and economically disadvantaged sectors of the population or in areas without access to digital technologies, services, and opportunities.

Universal access (UA) to ICTs, including access to broadband networks, devices, and digital services, is a key component for everyone, everywhere to realize the full benefits deriving from digital transformation. It is also a fundamental lifeline during emergency situations, such as the COVID-19 pandemic, providing access to basic commercial and public services, as well as to communicate with friends and family, telework, obtain health care and education. Accordingly, and consistent with the United Nations' Sustainable Development Goal 9c and the Broadband Commission for Sustainable Development's targets (see Box 3.1), effective UA policies must enable access to affordable and good quality broadband services, and facilitate digital inclusion, including developing digital skills, access for women and people with disabilities, and availability of relevant content and applications (United Nations 2015, 9c)

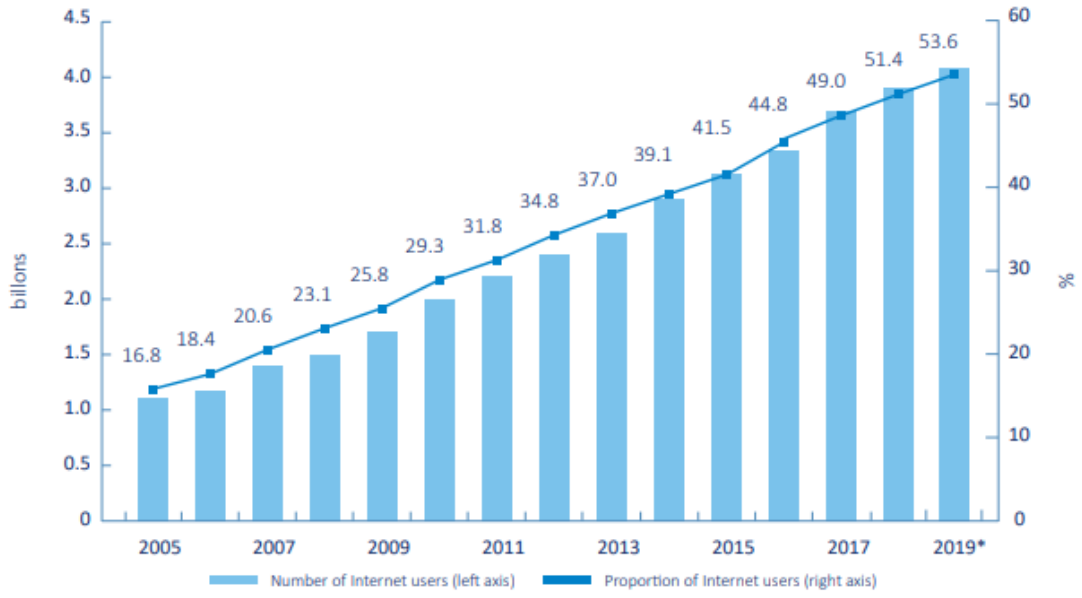
Box 3.1. Broadband Commission for Sustainable Development's 2025 targets

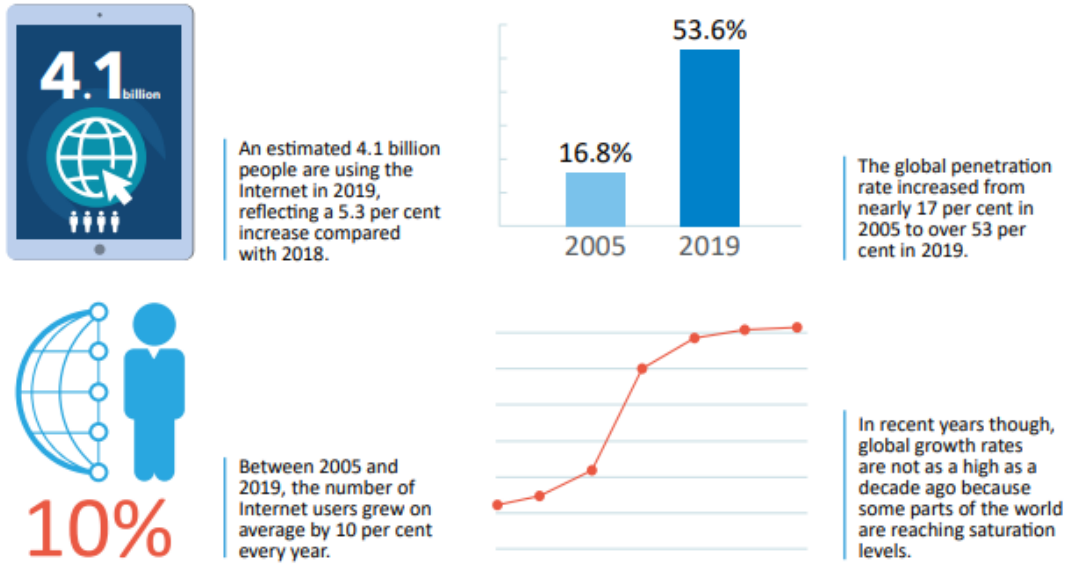
By 2025:

1. All countries should have a funded national broadband plan or strategy or include broadband in their universal access and service (UAS) definition
2. Entry-level broadband services should be made affordable in developing countries at less than 2 per cent of monthly Gross National Income (GNI) per capita
3. Broadband Internet user penetration should reach: a) 75 per cent worldwide b) 65 per cent in developing countries c) 35 per cent in least developed countries
4. 60 per cent of young people and adults should have achieved at least a minimum level of proficiency in sustainable digital skills
5. 40 per cent of the world's population should be using digital financial services
6. Overcome unconnectedness of micro-, small- and medium-sized enterprises (MSMEs) by 50 per cent, by sector
7. Gender equality should be achieved across all targets

Despite continued progress in achieving these goals, with the United Nations noting that about 90 per cent of the world population lives within range of a 3G mobile network (ITU 2019, 8) and the International Telecommunication Union (ITU) estimating that from 2005 to 2019 Internet usage increased on average by 10 per cent per year (ITU 2019), over 3.6 billion people, or about 46 per cent of the world population, still do no use the Internet. Even more concerning, however, Internet usage growth rates have decelerated in recent years as market saturation is being reached (see Figure 3.1) (ITU 2019).

Figure 3.1. Individuals using the Internet and growth rates





Source: ITU 2019.

When examining Internet usage differences between countries grouped by income level, a continuing, but decreasing, digital divide is evident. There were 3.6 times as many Internet users in developed countries as in developing countries in 2009, a figure that decreased to 1.8 in 2019. However, growth rates in developing countries have significantly declined in recent years. At the current rate of decline, developing countries are unlikely to meet the Broadband Commission for Sustainable Development's targets of 65 per cent broadband user penetration by 2025. This supports the need to reassess policies and approaches currently being implemented to ensure UA objectives and meet these targets.

This chapter discusses key challenges and policies to achieve UA objectives within the context of digital transformation. The discussion focuses on three pillars:

- connectivity, which addresses challenges associated with funding broadband infrastructure expansion;
- pricing, which deals with affordability barriers to the take-up of digital services and end-user devices; and
- inclusion, which covers policies to develop digital skills, responds to gender disparities and accessibility of services to people with disabilities (PWDs), and promotes the creation of local digital content.

In addition, this chapter discusses the need to incorporate monitoring and evaluation of UA policies to ensure data-driven decision-making and promptly identify and correct regulatory failures.[1]

3.2 Challenges to achieving universal access to broadband and digital services

Private investment plays a leading role in expanding access to broadband and digital services in developing countries, particularly leveraging mobile and other innovative wireless technologies. Regulators and policy-makers are responsible for implementing policies that promote investment and leverage new technologies and business models (see Box 3.2).

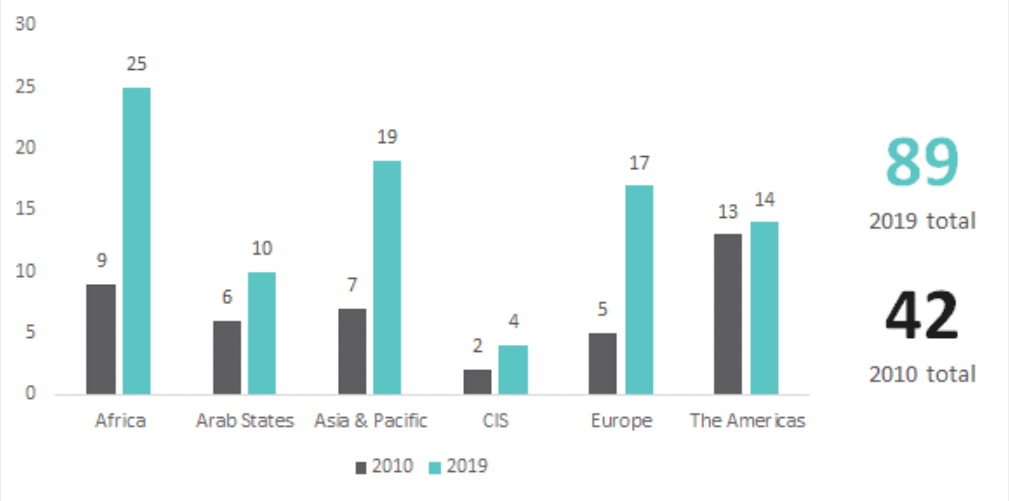
[1] For more detailed examination of the topics covered in this chapter, see relevant thematic sections on the *Digital Regulation Platform*.

However, market forces alone are unable to commercially extend broadband and digital services to certain areas (e.g. remote rural areas) or groups (e.g. those with low income). To resolve this, narrowly tailored and targeted UA policies are required. This section summarizes the key challenges faced by policy-makers to promote UA. In developing countries, which face significant financial, socio-economic and educational constraints, national digital strategies must focus on a multisector, collaborative approach to tackle the UA challenges of access, affordability, skills, and take-up.

Box 3.2. Evolution of universal access and service policies

Universal access and service (UAS) policies traditionally focused on basic voice communications, particularly in more developed markets. But over the past decade, policies and strategies have expanded to include Internet access, and broadband in particular. Between 2010 and 2019, the number of countries that included broadband within their UAS policies more than doubled from 42 to 89. In 2019, this represented around 60 per cent of all countries that reported having adopted a UAS policy. This trend is more pronounced in some developing regions, with about 70 per cent of African and Asia-Pacific countries now including broadband service in their definition of UAS. In addition, access to the Internet has been declared a right in several countries as well as by the United Nations (United Nations 2016).

Figure B3.2.1. Number of countries with broadband as part of their UAS definition



Source: ITU 2020.

Addressing the "digital divide", defined as "the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard to their opportunities to access information and communications technologies (ICTs) and to their use of the Internet for a wide variety of activities" (United Nations 2018, 2), requires tailored policies and strategies that can resolve the challenges shown in Table 3.1.

Table 3.1. Key universal access challenges facing developing countries

	Challenge	Description	Key policies/actions
Connectivity	Availability	Limited sources of financing for broadband infrastructure deployment Limited infrastructure availability throughout the broadband value chain	Update or establish efficient Universal Access and Service Funds (UASFs) to direct funds to uneconomic areas and programmes Utilize public funding, development aid, or government initiatives and regulatory incentives to bring affordable broadband to underserved areas and population groups (e.g. connectivity obligations within spectrum licences; access to spectrum in return for infrastructure deployment or infrastructure sharing). Implement contractual agreements (e.g. public-private partnerships (PPPs)) or mechanisms like "pay or play" to co-fund digital infrastructure deployment Enable the use of innovative business models, alternative technologies (e.g., satellites, drones/ balloons, Wi-Fi) Promote cross-sectoral infrastructure deployment (e.g., transportation, oil and gas, electricity) and infrastructure sharing (passive and active) Ensure fees and taxes on ICT service providers (including spectrum fees) are reasonable, and adequately balance the collection of government revenue and enabling development of digital services
Pricing	Affordability	Low purchasing power, coupled with high prices for services and end-user devices	Targeted policies, subsidies, payment plans and sponsored data to increase affordability of digital service and end user devices for vulnerable populations Promote free public Internet access points, such as digital access centres in schools, libraries, post offices, and public Wi-Fi networks; Reduce import levies and other taxes applicable to end user devices
Inclusion	Accessibility	Ability to use digital services and technologies regardless of education, disability, age, and gender, among other factors	Develop plans to stimulate demand with a focus on women and girls, and PWDs
	Skills	Lack of necessary digital skills and literacy	Implement digital skills training initiatives and life-long learning programmes
	Relevance	Limited awareness of opportunities and benefits of ICTs Limited availability of relevant content and services in local languages	Promote government adoption of ICTs and roll out of e-government services and applications (including e-health, e-education) Develop policies to promote local digital content industries and digital content creation

3.3 Policies to promote universal access to broadband and digital services

UA policies cover not only connectivity, but also measures to ensure affordability and inclusion. The means by which governments, the private sector, non-governmental organizations, and international bodies can effectively and collaboratively achieve these goals directly relate to variables such as population density; income; geographical features; political and economic characteristics; and available resources among others. Depending on features such as these, countries have followed different approaches to close access gaps. Moreover, in some cases such as Kenya, universal access is included in the country's digital strategy (Republic of Kenya 2019). This section reviews UA policies and approaches being adopted around the world.

UA funding and financing policies: tackling accessibility challenges

Funding and financing mechanisms to achieve UA goals are the key challenge to ensure availability of broadband and digital services. Traditionally, government has in many cases used universal access and service funds (UASFs) as the funding mechanism of last resort to achieve UA goals. However, because of funding, operational, and other challenges, over the past several years alternative funding sources and strategies have emerged. Taken together, these approaches can be leveraged to ensure UA policies are better suited to offer connectivity, adequate infrastructure, affordability, digital skills, and inclusion of traditionally marginalized groups.

The main funding options are examined below:

- Universal access and service funds
- Additional funding and financing strategies
- Supplementary direct government funding, or joint public and private funding
- Effective regulatory measures
- "Pay or play" policies.

Universal access and service funds

UASFs are funding mechanisms established by national governments to promote universal access to telecommunication services. They provide financial incentives for telecommunication service operators to provide service in locations that would not be commercially viable otherwise (UN ESCAP 2017, 10). Traditionally, governments allocated service-specific subsidies (e.g. for fixed telephony payphone services). However, more recently there has been a shift to allow service-neutral competition (e.g. fixed or mobile), as well as technology-neutral competition for UASF subsidies. Further, the Economic Commission for Latin America and the Caribbean (ECLAC) notes that UASFs are a valuable resource that can be used to fund programmes to assist PWDs in the Caribbean (Bleeker 2019), a view that is equally valid for other disadvantaged populations and in other regions. Similarly, in emergency situations, such as during the COVID-19 pandemic, UASFs have been noted as a means to, in the short term, finance temporary network capacity relief, and to keep networks running and operational. (Broadband Commission for Sustainable Development 2020).[2]

[2] COVID-19 Crisis: Broadband Commission Agenda for Action for Faster and Better Recovery, https://www.broadbandcommission.org/COVID19/Pages/default.aspx .

The shift in focus from voice services to broadband connectivity, promoting affordability and inclusion, has been crucial for countries. But it has required legal and regulatory changes to give UASFs the flexibility to support initiatives and programmes to implement broadband strategies (Alliance for Affordable Internet 2015, 17).

A review of successful UASFs demonstrates that certain capacity requirements are necessary to attain UA goals. A UASF carries many of the same functions as a financial institution. It manages large capital assets, evaluates and defines projects for investment opportunities, and provides financing to implementing contractors, whose operations must be overseen and evaluated to ensure the UASF's resources are well spent. Some of the necessary capacity requirements include:

- policies and parameters that can be modified quickly and effectively to accommodate the need for a new UASF vision and respond to rapidly changing and evolving priorities;
- well-articulated policy and vision;
- transparency, visibility, and accountability;
- detailed rules on process and eligibility for disbursement;
- capacity building, sustainability, and complementary services;
- availability of resources and knowledge;
- regulators as partners for development and social inclusion;
- autonomous UASFs in administrative budgeting and allocation of resources.

However, UASFs have been subject to well-documented challenges. These include lack of transparency in resource assignment processes, low or non-disbursement of funds collected, fund collection and actual service funding/subsidy needs often are not linked, political interference, and lack of adequately trained staff, among others (GSMA 2013, 261-262). Going forward, effective operation of UASFs require identifying and resolving such problems if they arise (see Box 3.3).

Box 3.3. Examples of effective UASFs

Recent examples of successful UASFs include Costa Rica, Nigeria, and Pakistan. These countries have attained adequate fund management capacity, effectively utilizing UASF contributions and achieving ICT access objectives (Alliance for Affordable Internet 2015, 9).

- Costa Rica launched "CR Digital" in 2015. This national programme intended to connect the whole country to the Internet within two years. Although the goal was not achieved in that period, by 2018, 40 000 more families were online and 400 rural educational institutions had received Internet connection. Also, 95 per cent of households that have participated to date are female-headed (Alliance for Affordable Internet 2020).
- Nigeria's Universal Service Provision Fund (USPF) has funded hundreds of new base stations, School Knowledge Centres and Community Resource Centres, fibre backbone network, inter-university connectivity, and programmes for e-health and e-accessibility (Alliance for Affordable Internet 2015, 15).[a]
- An autonomous Universal Service Fund was established in Pakistan in 2007, which is operated by an independent state company (Alliance for Affordable Internet 2015, 9).[b] This fund focused on basic telecommunications and advanced services, including broadband. By 2013, the fund had financed Internet access to nearly 300 previously unserved towns and cities and about 1 100 high schools, colleges, and libraries.

Note: **a. See Universal Service Provision Fund,** http://www.uspf.gov.ng/**; b. See Universal Service Fund,** http://www.usf.org.pk/**.**

Alternative approaches to funding broadband infrastructure

Additional funding and financing strategies to achieve UA goals are also being implemented around the world. These strategies aim to improve the economics or reduce the cost of projects aimed at deploying infrastructure to meet UA goals that may not be financially viable otherwise. For example, these may include fiscal measures such as enabling tax, tariff, import, and business regulation policies designed to reduce risks and financial burdens and provide incentives to ICT investors and financiers.

Supplementary direct government funding, or joint private and public funding, is also being directed to facilitate investment in broadband infrastructure and digital ecosystems. In the European Union, a series of funding and grant mechanisms have been deployed over the past few years to expand broadband network deployment. For example, the recently adopted Connecting Europe Facility (CEF2) Digital aims to support and catalyse investments in digital connectivity infrastructures of common interest during the 2021-2027 period. CEF2 Digital aims to support projects that address market failure and do not crowd out or overbuild other equivalent investments in the target area. As an EU-level public co-financing instrument, CEF2 Digital can attract private co-financing to address market failures, provided that the infrastructure targets areas in which no equivalent network, in terms of capabilities and/or functionalities, already exists (or is planned in the next 24 months) (European Commission 2019, 5).

Effective regulatory measures can also contribute to reducing network deployment costs. Such policies include promoting access to existing physical infrastructure, including cross-sectoral policies to access ducts, poles, or other passive infrastructure belonging to energy and

other utilities. "Dig once" policies also aim to coordinate civil works between different utility companies to reduce cost of network build-out. Streamlining permitting requirements, such as rights-of-way, can also help reduce infrastructure deployment times and costs.

"Pay or play" policies are also being implemented as an alternative to finance UA goals. Under this approach, in countries such as Vanuatu, service providers may choose to "play" by meeting their cost in rolling out infrastructure to unserved or underserved areas or groups or, alternatively, non-playing providers must "pay" a UASF levy set by the regulatory authority. Accordingly, if a service provider decides to "play" under the UA project, then the regulator will not impose a levy for the relevant year, provided that the service provider meets its commitment. Relief funds are available in case the net costs exceed the UA levy threshold. Between 2015-2018, this pay or play framework has been successfully implemented in Vanuatu to achieve upgrades of mobile networks to offer data services and coverage of over 98 per cent (TRBR 2019, 7-8).

Policies to make broadband and digital services affordable

According to the Broadband Commission for Sustainable Development Target 2, by 2025 entry-level broadband services should be made affordable in developing countries at less than 2 per cent of monthly Gross National Income (GNI) per capita (Broadband Commission for Sustainable Development 2019b, 32). Despite significant advances over the past decade to promote competition market, in many countries prices remain above the Broadband Commission's "1 for 2" affordability target threshold, that is, 1 GB of mobile data priced at or below 2 per cent monthly GNI per capita (Broadband Commission for Sustainable Development 2019a, 34) In some countries, lower per capita income levels combined with low population densities may require public sector or joint public-private support to ensure high network deployment and device costs do not result in continued unaffordable Internet access.

The global average price of a mobile-data basket of at least 1.5 GB dropped from USD 20.4 in 2013 to USD 13.2 in 2019, equivalent to a compound annual growth rate (CAGR) of -7 per cent – driven mostly by the 2013 to 2015 subperiod, followed by relative stability over the past four years. Over the past six years, there has been an explosion in the number of active mobile-data subscriptions, increasing from 27.4 to 83 per 100 inhabitants, or a CAGR of 20.3 per cent (ITU 2019).

In developed countries, the price of a mobile-data basket of 1.5 GB stood at USD 17 in 2019, which was above the global average of USD 14. However, as most people in developed countries will have a data-and-voice bundle, a data-only plan will not be very common. In developing countries, the nominal price remained just under the global average, at USD 13, whereas in the least developed countries the cost was only USD 8 for such a plan. Expressed in USD, the price of a mobile-data basket was the lowest in the Commonwealth of Independent States (CIS) region (USD 7), followed by Africa (USD 10), Asia and the Pacific (USD 11) and the Arab States (USD 14). The two most expensive regions were Europe at USD 16 and the Americas at USD 18 (ITU 2019).

Targeted policies, subsidies, and payment plans are often used to increase affordability of digital services and end-user devices for vulnerable populations. For example, national policies can be leveraged to foster local innovation and research and development for Internet-enabled devices such as handsets, as well as prioritize support through government investment agencies for ventures (between local and foreign firms or PPPs) that seek to offer low-cost devices to the market (Broadband Commission for Sustainable Development 2019a, 19). Similarly,

mobile operators are developing payment plans to facilitate acquisition of smart devices by lower-income consumers. In Kenya, Safaricom's Maisha Ni Digital Campaign, launched in partnership with Google, seeks to provide access to entry-level smartphones (Neon devices) and close gender gaps – Kenyan women are 34 per cent less likely than men to use the mobile Internet. With devices offered at subsidized prices ranging from USD 32 to USD 55, Safaricom sold more than 600,000 Neon smartphones in 2019, making the devices the most popular and affordable smartphone in its retail shops across the country (Safaricom 2019a; Safaricom 2019b; GSMA 2020).

Box 3.4. Different approaches to public Wi-Fi network deployment

Public Wi-Fi allows people to use much more data at little or no extra cost in public spaces, without significant revenue loss for retail operators. This has been implemented using different institutional and funding approaches by governments and cooperative platforms around the world (Alliance for Affordable Internet 2019a, 26).

General budget funding: Governments around the world – from national to local – are supporting free public Wi-Fi deployments. In the EU, the WIFI4EU programme has awarded EUR 15,000 subsidies to 6,000 municipalities to cover the capital expenditure of providing free public Wi-Fi.[a] In the Philippines, the government launched a programme to provide free public Wi-Fi to all citizens in all public places, including parks, plazas, libraries, barangay (village) centres, national and local government offices, public basic education institutions, state universities and colleges, public hospitals, health centres and rural health units, public airports and seaports, and public transport terminals. Legislation passed in 2017 (Republic Act No. 10929) tasks the Department of ICT (DICT) with implementation of the programme and, as of April 2020, 3,735 sites were operational in the Free Public Wi-Fi for All programme.

UASF financing: In some countries UASFs are earmarked to deploy public Wi-Fi networks. In Trinidad and Tobago, public funds are made available via UASF to subsidize deployment of public Wi-Fi networks and service fees (TATT 2016, 12) This initiative had limited success as it faced coordination challenges and limited buy-in from industry. In 2020, the government relaunched the initiative to resolve these challenges.

Sponsored data programmes: Innovative business models to overcome affordability challenges are also being implemented to support deployment of public Wi-Fi networks. In Kenya and Rwanda, a Kenyan start-up, BRCK, successfully launched Moja WiFi, which offers free service to end-users and is funded via sponsorships and advertising. Users "pay" with their time, attention, or engagement rather than with money. Moja WiFi has deployed 1 300 hotspots in rural and urban areas and provides free Internet access to about 2 million users (Loyce Chloe 2020).

Note: WiFi4EU – Free Wi-Fi for Europeans, https://ec.europa.eu/digital-single-market/en/wifi4eu-free-wi-fi-europeans .

Promoting public Internet access points, where Internet access is provided free of charge or at low cost, is also a policy pursued by many countries to offer affordable service for some of the most vulnerable individuals or groups. These include digital access centres in schools, libraries, post offices, and public Wi-Fi networks that ensure privacy and security. Designing policies

for sustainable community telecentres, offering free or low-cost use of computers, broadband connections, e-services, and digital skills training expand broadband and target affordability challenges (see Box 3.4).

Another key incentivizing policy lever to foster UA access to broadband and digital service and devices is decreased taxes and sector-specific fees. Governments must balance the need to raise revenue with the negative impact of higher fees and taxes, that is, decreased broadband adoption and usage, on the economy as a whole and on the process of digital transformation. For instance, in 2017 Colombia opted to remove value-added tax (VAT) on low-cost handsets and laptops and to exempt low-cost plans and lower-income consumers from VAT increases. As a result of these targeted policies, mobile phone sales increased in 2017, even for devices that exceeded the VAT exemption for low-cost devices. Some device manufacturers repriced their devices to move from just-above the VAT threshold to just-below, thereby providing Colombians with a wider range of devices at more affordable prices (Alliance for Affordable Internet 2020b).

Policies to promote inclusion

Cross-sectoral policies: digital skills and literacy

UA policies have evolved to extend beyond the ICT sector itself, more broadly including cross-sectoral approaches that can leverage ICT benefits across multiple economic segments. The Broadband Commission for Sustainable Development highlights the idea of "meaningful universal connectivity", encompassing broadband adoption that is "not just available, accessible, relevant and affordable, but that is also safe, trusted, empowering users and leading to positive impact" (Broadband Commission for Sustainable Development 2019a, ix). The ideas of empowering users leading to positive impact is arguably the ultimate goal of cross-sectoral policies intended to improve and expand the use of ICTs in order to have a broader effect.

Perhaps the most prominent example of this cross-sectoral thinking is the inclusion of digital skills in UA policies and plans. The ITU has identified the benefits of building digital skills and applying them in both work and personal aspects of individuals' lives (ITU 2018, 5):

- Work: qualification for jobs in conventional sectors; enable participation in emerging sectors; leverage advances in digital technologies, platforms, and devices; important to changing nature of work environments.
- Access to information: safe access to news and information; communication with friends and family; access to key services (e-health, e-government, digital finance, agricultural technology, and transportation).

Building on the Broadband Commission for Sustainable Development's view that digital skills exist on a spectrum, the ITU has defined basic, intermediate, and advanced skills (Broadband Commission for Sustainable Development 2017a, 4; ITU 2018, 5-7). These definitions are useful as reference points for policy-makers determining the digital skills and cross-sectoral components of UA plans. In brief:

- **Basic skills** are foundational for performing basic tasks, akin to traditional literacy and numeracy, and include familiarity with use of hardware, software, and basic online operations such as email or form completion.
- **Intermediate skills** enable critical evaluation of technology and content and currently may include work-related functions such as desktop publishing, digital graphic design, and

digital marketing, although ongoing technical change will necessitate changes in what is considered an intermediate skill.

- **Advanced skills** are those required by professional ICT specialists, such as computer programming and network management, as well as broader abilities such as digital entrepreneurship.

The use of a cross-sectoral component such as digital skill-building creates beneficial ripple effects across entire economies, expanding economic opportunities and strengthening communications regardless of the industrial sector, geographic location, or population group. The economy-wide benefits of digital skills development justify a focus on their incorporation into educational settings. These efforts, which sometimes fall under the umbrella of an educational policy or joint education and communications initiative, are crucial to train students at an early age how to leverage the capabilities of broadband and technology. The European Commission has adopted a Digital Education Action Plan, in which school connectivity is only the first of 11 action items (European Commission 2018). The action items are organized in line with three priorities, which include "making better use of technology for teaching and learning," and "developing relevant digital competences and skills for the digital transformation". The digital skills-focused priority includes action items addressing the inclusion of coding in all European school curricula as well as increasing awareness at all levels (parent, teacher, student) of online safety, cybersecurity, and media literacy.

Such education and training is not limited to the primary or secondary school settings. The intermediate and advanced skills identified above are candidates for more specialized vocational and professional development training settings. In the Netherlands, a "Digital Technology Pact" noted a principle of implementing technology education broadly, including not only primary and secondary education, but also vocational education, higher education, and professional development (National Technology Pact 2016). The pact includes an emphasis on cooperation between academia and the business sector in an effort to strengthen the technological skill of Dutch workers. Continued digital skills training is also presented in various countries in the form of boot camps and other focused skills-building environments for professionals.

Beyond access to ICTs, ensuring that their potential benefits can be leveraged across multiple sectors magnifies their impact and should be a key component of a modern UA policy or programme and may be considered in cooperation with ministries or government agencies.

Promoting local content and content industries

Another key consideration of modern UA policies is driving demand for connectivity through the promotion of relevant content. Beyond providing the connection for users to access content, a forward-looking UA policy should also consider the need to bring the newly connected online and make it relevant for them to take advantage of the connection.

While the Internet hosts a tremendous amount of public and private content, connectivity demand is driven by the availability of content that is relevant to users. This includes ensuring that content is available in relevant languages and is tailored to local needs and interests. From its earliest stages, the Broadband Commission has called for the availability of local content. In its October 2011 "Broadband Challenge" (Broadband Commission for Digital Development 2011, 2), the commission called on governments and civil society to "stimulate local content production as well as the development of local language services and applications for an inclusive digital world". In considering demand generation through local content, a 2011 Intel

white paper on the use of USAF resources to broadband programmes notes that software and applications in local languages make education, financial services, health care, e-government, and other services more accessible (Intel 2011, 2).

The role of a UA policy in this context is to support efforts that enable local content creation. In one recent example of such an approach, Nigeria's 2020-2025 National Broadband Plan includes efforts to bring more Nigerian businesses online through free .ng domain name registrations for two years and through multiple digital literacy and awareness approaches intended to spur demand (Government of Nigeria 2020, 61). Both types of efforts foster increased local content availability. The free domain name registration initiative is intended to promote local content development as well as job creation and expanded online business opportunities for Nigerian companies through a reduction in the cost of establishing a new online business or online presence. Notably, the policy does not direct funds to particular businesses or industries, but rather seeks to provide a universal benefit to all Nigerian businesses seeking to register a domain name, allowing them to direct their resources toward other aspects of developing their business. Responsibility for implementation of such initiatives is spread among various government agencies, with Ministry of Communications and Digital Economy participation included in all of the digital literacy activities, while the domain name registration programme is assigned to Nigeria's Internet Registry Association, the National Information Technology Development Agency (NITDA), and the Corporate Affairs Commission. As is seen in this case, approaches to expanding digital literacy and content creation involve a range of stakeholders.

The Philippines includes a similar component in its National Broadband Plan, stating that the government will support the development of local content and applications to drive broadband demand (Department of Information and Communications Technology 2017, 44). Specifically, the plan includes the following measures:

- provision of incentives to local content developers, beginning with the inception, incubation, and marketing of the content or application;
- government policy and regulatory interventions to develop favourable environments for content and application creation; and
- consider development of "rich and useful" content and applications to support the delivery of public services and creation of citizen engagement platforms to drive demand; similarly, such resources should be supported by application programming interfaces that allow websites to be displayed in multiple languages, depending on the user's needs or preferences.

Similarly, Nigeria's digital literacy-related efforts also include development of educational, vocational, and entrepreneurial content in local languages. Nigeria's plan also envisions development and implementation of an enhanced national digital virtual e-library that provides a range of digital resources and includes translation of foreign-language material to local languages.

Additional approaches to local content development can include efforts to increase the online availability of government services and information. As a major producer of information that is both locally relevant and presented in the local language, national, state, and local governments are ideally suited to play a role in the implementation of UA policies that create new or expanded online resources that provide useful information to citizens.

Overall, UA policies should consider the potential benefit of increased availability of local content in terms of increasing Internet usage. In crafting goals or action items intended to

increase the availability of local content, policy-makers should consider the roles of both the private and the public sector in order to maximize the impact of such efforts.

Gender inclusion and accessibility policies

Recognizing that lack of Internet access or usage is not uniform across populations, policy-makers should consider how UA policies and UASFs can be employed to particularly assist those groups with comparatively low levels of access and usage. In particular, research has identified a need to improve connectivity and digital services access for women and for PWDs.

Based on 2019 ITU estimates, there was a 17 per cent difference in Internet penetration between men and women worldwide, although the number varies across regions and income levels (ITU 2019, 3). Notably, developing countries have a difference of 22.8 per cent, while LDCs have a gender gap of nearly 43 per cent. Perhaps of greatest concern is that the gender gap has grown over the past few years. ITU data indicates that the gender gap has increased in the Asia-Pacific, Arab States, and African regions, and also in the developing country and LDC groups between 2013 and 2019.

The OECD notes that the gender gap, sometimes known as the digital gender divide, has multiple root causes, including barriers to access, affordability, education, and lack of technology literacy (OECD 2018, 22). While these aspects are relevant to the digital divide across groups, the OECD also notes the relevance of gender biases and socio-cultural norms leading to gender-based digital exclusion. These can include comparatively higher domestic work and childcare obligations and negative social perceptions of Internet use by women and girls.

Organizations including the Broadband Commission for Sustainable Development and the World Wide Web Foundation have proposed policy approaches to close the gender gap. Among the four recommendations presented by the Broadband Commission's Working Group on the Digital Gender Divide was the integration of a gender perspective in strategies, policies, plans, and budgets (Broadband Commission for Sustainable Development 2017b). This recommendation grows from the recognition that gender-related policies, strategies, and action plans often fail to acknowledge the importance of ICTs and broadband as enabling tools, while broadband strategies, policies, and plans often fail to include a gender dimension. To that end, the working group suggested three primary actions to address this disconnect:

- establishing gender equality targets for Internet and broadband access and use;
- assessing strategies, policies, plans, and budgets for gender equality considerations; and
- consulting and involving women as well as relevant local communities and experts.

Such approaches are particularly salient for the development or revision of UA policies, increasing the likelihood of addressing the gender gap alongside improving overall connectivity and access.

The World Wide Web Foundation has also identified USAFs as an "untapped resource" for addressing the gender digital divide (Thakur and Potter 2018). To that end, the organization has proposed four key recommendations to improve the efficiency and efficacy of USAFs specifically to address the gender gap:

1). Invest at least 50 per cent of funds in projects targeting women's Internet access and use.
2). Make project design and implementation more gender-responsive.
3). Increase transparency of fund financing, disbursements, and operations.

4). Improve diversity in USAF governance and increase awareness of gender issues within the USAF.

A recent example of this approach is Colombia's 2018-2022 ICT plan, which includes a section on using ICTs as a tool for closing the gender gap (MinTIC 2018, 72). The plan underscores the importance of improving both women's access to and adoption of ICTs, and also notes the need to address the socio-cultural norms and beliefs that discourage women from using ICTs or pursuing ICT-related careers. Colombia's plan continues by highlighting two programmes intended to increase women's use of ICTs and related tools.

In addition to the gender gap, there are also access disparities that affect PWDs. While ICTs can play a significant role in overcoming barriers faced by PWDs in terms of participating actively in society, technological progress does not guarantee equal access to new and improved technologies.

Among various action items that more broadly suggest operational improvements to UASFs, ECLAC proposes several action items to close access gaps for PWDs. These include:

- enable funding to be disbursed to civil society and non-governmental organizations working with PWDs and other marginalized groups;
- include a stronger mandate for PWDs, including an obligation to have annual targets to meet fund objectives;
- increase engagement with PWDs at each stage of a project's lifespan, including the identification, appraisal, and allocation process;
- increase representation of PWDs in UASFs; and
- invest a fixed percentage of funds in projects to increase access to technology for PWDs.

It is perhaps noteworthy that there is significant overlap between the World Wide Web Foundation's recommendations for addressing the gender gap and ECLAC's recommendations to improve access for PWDs. These may point to common approaches to addressing access gaps among other marginalized populations.

3.4 Monitoring and evaluation of impact of universal access policies

In addition to considering how UA policies have evolved and the key areas of focus for modern plans, it is also important to be able to evaluate whether a policy or individual project has met its intended goals. This consideration of accountability should be a foundational component of UA approaches, and relies both on clear, measurable objectives and on the ability to measure progress against them. In a sense, this equates UA policies and plans with many other government policies or programmes, for which policy-makers need to design and implement mechanisms for monitoring effects. In addition to transparently disbursing funds in support of UASF targeted projects, it is also particularly important to evaluate whether such spending is an effective and efficient use of collected funds.

As such, two approaches to monitoring and evaluating the impact of UA policies should be considered: (i) evaluation of the overall policy, and (ii) evaluation of individual UASF-supported projects. In both cases, the establishment of clear goals and/or milestones will lay the groundwork for later impact evaluation.

For UA policies, governments should set specific, attainable goals for the key aspects of the policy. This could include, for example, ensuring Internet connectivity in a minimum number of

locations or to a minimum percentage of the population, ensuring access to a certain level of connectivity without exceeding a certain proportion of per capita national income, and ensuring a minimum level of service quality. The inclusion of specific goals or milestones allows a review of the efforts undertaken as a result of the policy. For example, if a UA policy includes a goal of increasing the percentage of the population with access to a 10 Mbit/s Internet connection to at least 98 per cent within five years, a subsequent review should be able to evaluate whether that goal was met. If resources permit, an interim or mid-term assessment of the policy's impact is a particularly useful tool, allowing for course corrections before the target date is reached.

Similarly, UASF-funded projects should be designed to have specific implementation milestones and goals that must be met, and clear criteria against which success can be measured. Traditional voice service-focused UASF-supported projects have often been structured such that payment is disbursed upon successful, timely completion of project milestones, providing recipients with an incentive to meet the stated implementation timeline and goals. This approach is equally applicable to UASF-supported projects for expanding access to the Internet and digital services more broadly. Funding recipients should be able to substantiate that they have met goals that may include not only connectivity, but adoption, price levels, variety of services available, or services available to disadvantaged populations.

In line with meeting specific milestones and timelines, UASF-funded projects should include reporting requirements that may incorporate a progress assessment, analysis of any unexpected circumstances, financial statements, and any other relevant analysis, particularly in cases of deviation from initial project plans. As above, such requirements may not markedly differ from reporting requirements for a telephony-focused project but should be tailored to the particular project and its goals. Thus, additional reporting requirements could include, for example, average available broadband speeds, access to particular digital services, or measures to ensure access for PWDs. The goals of reporting requirements should be to enable all stakeholders to assess project progress or success, and also to serve as a motivation for the funding recipient to commit appropriate resources to meet the project goals.

UA policy and project monitoring is a key policy element for increasing the likelihood of success. While the concept dates back to the earliest UA policy approaches, it can and should be adapted to fit modern UA and digital service needs.

3.5 Key findings

Considering the issues reviewed in the preceding sections, the following key findings may be informative for policy-makers and other stakeholders.

Focus on reliable, affordable broadband and devices. As policy-makers develop or revise UA policies, the availability of reliable, affordable broadband is increasingly taking a central role. This connectivity is comprised of, and enabled by, international and backbone connections, backhaul connectivity, and last mile connections. This foundation enables connectivity that, in turn, promotes broader socio-economic development. Affordability is a core issue, necessitating innovative approaches and business models, particularly for access to devices.

Improve UASF effectiveness. The past and current challenges faced by UASFs and the populations intended to benefit from their projects indicate a need to review and, if necessary, reform the scope, processes, and effectiveness of such funds. These challenges need to be

resolved to make UASFs more efficient and better positioned to be able to deliver universal connectivity.

Diversified funding sources and alternative approaches. Policy-makers and stakeholders are considering a wide range of traditional and alternative approaches to funding projects to better reach UA goals. As discussed, this can include fiscal measures and regulations intended to reduce risk, UASFs and new funding approaches that leverage private funding or expertise, or which combine public and private sources, as well as regulatory streamlining.

Skills development enables and drives broadband adoption. Connectivity alone is not enough to drive wider broadband adoption. Rather, UA plans are expanding to include components intended to develop the digital skills that enable users to take advantage of connectivity and to effectively work in an increasingly digital economy.

Inclusion and accessibility are increasingly built into UA plans. Beyond connectivity and broad socio-economic goals, UA plans are increasingly incorporating measures to ensure that connectivity and its benefits reach populations that have traditionally been excluded, such as women and PWDs.

Monitoring and evaluation continue to play important roles. UA policy impacts are dependent on effective and efficient implementation. Thus, UA policies continue to require structured monitoring and evaluation mechanisms intended to ensure that policy, programme, and investment goals are met.

Consideration of these key findings may help policy-makers and stakeholders consider the questions and issues that will inform their UA policy evaluation and development.

References

Alliance for Affordable Internet. 2015. *Universal Access and Service Funds in the Broadband Era: The Collective Investment Imperative*. Washington, DC: A4AI. http://a4ai.org/wp-content/uploads/2015/03/A4AI-USAFs-2015_Final-v.2.pdf.

Alliance for Affordable Internet. 2019. *2019 Affordability Report*. Washington, DC: A4AI. https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/A4AI_2019_AR_Screen_AW.pdf.

Alliance for Affordable Internet. 2020. *Good Practices Database*. Washington, DC: A4AI https://a4ai.org/good-practices-database/.

Article 19. 2020. *Coronavirus: Access to the Internet Can Be a Matter of Life and Death During a Pandemic*, London. https://www.article19.org/resources/access-to-the-internet-can-be-a-matter-of-life-and-death-during-the-coronavirus-pandemic/.

Broadband Commission for Digital Development. 2011. *The Broadband Challenge*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/publications/Broadband_Challenge.pdf.

Broadband Commission for Sustainable Development. 2015. *2025 Targets: "Connecting the Other Half"*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/publications/wef2018.pdf.

Broadband Commission for Sustainable Development. 2017a. *Working Group on Education: Digital skills for Life and Work*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://broadbandcommission.org/Documents/publications/WG-Education-Report2017.pdf.

Broadband Commission for Sustainable Development. 2017b. *Working Group on the Digital Gender Divide: Recommendations for Action: Bridging the Gender Gap in Internet and Broadband Access and Use*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/publications/WG-Gender-Digital-Divide-Report2017.pdf.

Broadband Commission for Sustainable Development. 2019a. *Connecting Africa Through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf.

Broadband Commission for Sustainable Development. 2019b. *The State of Broadband 2019*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

Bleeker, Amelia. 2019. "Using Universal Service Funds to Increase Access to Technology for Persons with Disabilities in the Caribbean", Studies and Perspectives series-ECLAC

Subregional Headquarters for the Caribbean, No. 79(LC/TS.2019/59-LC/CAR/TS.2019/2). Santiago: Economic Commission for Latin America and the Caribbean. https://www.cepal.org/sites/default/files/events/files/series_79_lcarts2019_2.pdf.

Department of Information and Communication Technology. 2017. *National Broadband Plan*. Quezon City: Department of Information and Communications Technology (DICT). https://dict.gov.ph/wp-content/uploads/2017/09/2017.08.09-National-Broadband-Plan.pdf.

ECTEL. 2008. *Telecommunications Universal Service Guidelines*. Saint Lucia: Eastern Caribbean Telecommunications Authority (ECTEL). https://www.ectel.int/wp-content/uploads/2015/12/ECTEL-universal-service-guidelines.pdf.

European Commission. 2018. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan*. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:22:FIN.

European Commission. 2019. *Draft Orientations Towards an Implementation Roadmap: Connecting Europe Facility (CEF2) Digital*. Brussels: European Commission https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital.

Government of Nigeria. 2020. *Nigerian National Broadband Plan 2020-2025*. Abuja: Federal Ministry of Communications and Digital Economy. https://www.ncc.gov.ng/docman-main/legal-regulatory/legal-other/880-nigerian-national-broadband-plan-2020-2025/file.

GSMA. 2013. *Universal Service Fund Study*. London: GSMA. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_Report_SurveyOfUniversalServiceFunds.pdf.

GSMA. 2016. *Are Universal Service Funds an Effective Way to Achieve Universal Access?* London: GSMA. https://www.gsma.com/mobilefordevelopment/country/global/universal-service-funds-effective-way-achieve-universal-access/.

GSMA. 2020. Safaricom *Maisha Ni Digital: Driving Digital Inclusion for Women*. London: GSMA. https://www.gsma.com/mobilefordevelopment/resources/safaricom-maisha-ni-digital/.

IEEE. 2017. *Options and Challenges in Providing Universal Access*. New Jersey: Institute of Electrical and Electronics Engineers (IEEE). https://internetinitiative.ieee.org/images/files/resources/white_papers/universal_access_feb2017.pdf.

Intel. 2011. *The Benefits of Applying Universal Service Funds to Support ICT/Broadband Programs*. Santa Clara: Intel Corporation. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/usf-support-ict-broadband-programs-paper.pdf.

ITU. 2017. *Connecting the Unconnected: Working Together to Achieve Connect 2020 Agenda Targets*. Geneva: International Telecommunication Union. https://broadbandcommission.org/Documents/ITU_discussion-paper_Davos2017.pdf.

ITU. 2018. *Digital Skills Toolkit*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf.

ITU. 2019. *Measuring Digital Development: Facts and Figures 2019*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

ITU. 2020. *2019 Statistics*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Loyce Chloe. 2020. "The Affordability Barrier: Moja in Numbers". *BRCK Blog*, April 3, 2020. https://www.brck.com/2020/04/the-affordability-barrier-moja-in-numbers/.

MinTIC. 2018. *Plan TIC 2018-2022*. Bogota: Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf.

National Technology Pact. National Technology Pact 2020: Targets for 2016-2020. https://www.techniekpact.nl/cdi/files/e3bd421f98a0f362b6a13091de60d08978df34e9.pdf.

OECD. 2018. *Bridging the Digital Gender Divide: Include, Upskill, Innovate*. Paris: Organisation for Economic Co-operation and Development. http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf.

OECD. 2019a. *Going Digital: Shaping Policies, Improving Lives*. Paris: Organisation for Economic Co-operation and Development. https://www.oecd-ilibrary.org/docserver/9789264312012-en.pdf?expires=1588087194&id=id&accname=guest&checksum=01C4C2080AC6C52A3024A2989151250D

OECD. 2019b. "OECD Urges More Action on Bridging Digital Divides, Boosting Skills and Enhancing Access to Data at Going Digital Summit". Press Release, March 12, 2019. https://www.oecd.org/newsroom/oecd-urges-more-action-on-bridging-digital-divides-boosting-skills-and-enhancing-access-to-data-at-going-digital-summit.htm.

Republic of Kenya. 2019. *Digital Economy Blueprint: Powering Kenya's Transformation*. https://ca.go.ke/wp-content/uploads/2019/05/Kenyas-Digital-Economy-Blueprint.pdf.

Safaricom. 2019a. "Safaricom Launches Third Edition of Maisha Ni Digital Campaign". Press Release, April 18, 2019. https://www.safaricom.co.ke/about/media-center/publications/press-releases/release/546.

Safaricom. 2019b. "Safaricom Sells More Than 0.6 Million Neon Smartphones". Press Release. September 24, 2019. https://www.safaricom.co.ke/about/media-center/publications/press-releases/release/801.

TATT. 2016. *Framework for the Implementation of Free Public WiFi Hotspots Throughout Trinidad and Tobago*. Port of Spain: TATT. https://tatt.org.tt/UniversalService/UniversalServiceFundInitiatives.aspx.

Thakur, D., and Potter, L. 2018. *Universal Service and Access Funds: An Untapped Resource to Close the Gender Digital Divide*. Washington DC: Web Foundation. http://webfoundation.org/docs/2018/03/Using-USAFs-to-Close-the-Gender-Digital-Divide-in-Africa.pdf.

TRBR (Office of the Telecommunications, Radiocommunications and Broadcasting Regulator). 2019. *Universal Access Policy (UAP) Stakeholders Tenth and Final Report on the Status of Implementation of the Government's Universal Access Policy*. Port Vila, Vanuatu: TRBR. https://www.trbr.vu/attachments/article/756/uap_stakeholder_10th_and_final_report.pdf

United Nations. 2015. *Transforming our world: the 2030 Agenda for Sustainable Development*, A/RES/70/1. Resolution adopted by the General Assembly on 25 September 2015. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E

United Nations. 2016. *The Promotion, Protection and Enjoyment of Human Rights on the Internet,* A/HRC/32/L.20. Resolution adopted by the General Assembly on June 27, 2016. https://digitallibrary.un.org/record/845728?ln=en.

United Nations. 2017. *Promotion, Protection and Enjoyment of Human Rights on the Internet: Ways to Bridge the Gender Digital Divide from a Human Rights Perspective*. Report of the United Nations High Commissioner for Human Rights. New York: United Nations. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/111/81/PDF/G1711181.pdf?OpenElement.

United Nations. 2018. *Progress Made in the Implementation of and Follow-Up to the Outcomes of the World Summit on the Information Society at the Regional and International levels*. Report of the Secretary-General. New York: United Nations. https://unctad.org/en/PublicationsLibrary/a73d66_en.pdf.

United Nations. 2019. *Report of the Secretary-General on SDG Progress 2019: Special Edition.* E/2019/68. New York: United Nations https://sustainabledevelopment.un.org/content/documents/24978Report_of_the_SG_on_SDG_Progress_2019.pdf.

UN ESCAP (United Nations Economic and Social Commission for Asia and the Pacific). 2017. *The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific*. Thailand: UN ESCAP. https://www.unescap.org/sites/default/files/Universal%20Access%20and%20Service%20Funds%20final.pdf.

Chapter 4. Consumer affairs

4.1 Introduction to digital consumer rights

Why care about consumers?

Digital transformation of the economy has many facets, including digitization of products themselves, of production processes, of the means of advertising and distributing products, of transacting to acquire them, and of course of communications.

Consumers have important interests in each facet, but perhaps especially in communications and the content and other facilities accessed via communications networks and tools. This chapter covers regulatory issues related to consumer interests in connectivity, and outlines consumer issues related to digital content, transactions, advertising, and distribution.

Empowering and protecting consumers has become a more important part of regulators' jobs for several reasons, including:

- The widespread take-up of digital communications means that people have come to depend on them as essential services, and ICT regulators are usually responsible for ensuring their universal availability and affordability.[1]

[1] See Chapter 3 on "Access for all".

- Another reason for the rise in interest in consumers in digital regulation is the shift towards outcomes-based regulation (Hogg 2020), in which regulators consider actual consumer experiences rather than simply whether firms are obeying the rules.[2]
- The past few decades have also seen great progress in the behavioural sciences, leading to a better understanding of consumer behaviour and how policies should take account of it. Real people do not always behave like the "rational consumer" assumed by classical economists.[3]
- The huge variety of digital services means that consumer choice is a vital factor in maintaining healthy competition in many linked markets.[4]
- Widespread use of the Internet and apps enables *prosumption*, in which consumers are both producers and consumers of user-generated content, and can interact directly on person-to-person platforms like eBay or Taobao.

All this shows the new benefits available to consumers, and consumers' shared power in shaping markets, in the digital era. At the same time, the new range of services brings new challenges and new risks, with corresponding needs for consumer empowerment and consumer protection. The statement from the Body of European Regulators for Electronic Communications (BEREC) in Box 4.1 strongly indicates that empowering end-users is likely to become a priority for regulators around the world in the coming decade.

The ITU also stresses consumer affairs in its concept of 5th generation (collaborative) regulation:[5]

Collaborative regulation puts a new emphasis on consumer benefits and protection, and leverages the resources of government institutions and industry to deliver them, through organic consultation, collaboration and conciliation.

2 This stress on fairness is reflected at least across Europe. See, for example, Ofcom (2020) and BEREC (2020), which stresses consumer empowerment as part of its work programme.
3 See for example Evans (2003), Dutta-Powell and others (2019), Lunn (2014), Lunn and Lyons (2018), and https://www.esri.ie/news/experiments-show-when-consumers-are-vulnerable-to-mistakes.
4 See Chapter 2 on "Competition and economics".
5 At https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Policy-%26-Regulatory-Frameworks.aspx.

Box 4.1. BEREC strategic statement on consumer empowerment

BEREC's draft strategy for 2021 to 2025 has three high-level strategic priorities: promoting full connectivity, supporting sustainable and open digital markets, and empowering end users. On the last of these, BEREC states:

Engaging consumers in the fast-evolving digital ecosystem is becoming more complex. While digital innovation and competition among digital service providers has improved consumer empowerment, there is still an important role for regulators to play in ensuring a certain level of consumer transparency and digital skills.

The promotion of full connectivity will enable the demand for high-quality services on the part of consumers, provided by the very high capacity networks whose development is a key priority in creating positive interactions.

BEREC will continue its work in promoting choice and empowerment for end-users by prioritising work to build trust in ICT and digital services, and to enable and result in better informed choices by consumers.

BEREC's approach to empowering end-users is based on two pillars: monitoring of the sector and the appropriate level of transparency. As part of monitoring the functioning of the EECC, BEREC will also monitor new end-user provisions such as the information provision requirements, including the contract summary template, and will provide input to the EC regarding the review of end-user rights. In terms of transparency, BEREC will also continue its work towards greater involvement of stakeholders, including consumer representatives, and publish its work in compliance with the BEREC regulation.

As part of its work on transparency, BEREC will build its knowledge base on AI and explore ways to safeguard consumers against potential risks.

Source: BEREC 2020.

This chapter covers the following topics:

- **Consumer support framework** discusses the framework within which ICT regulators will work. Within this, **Roles of ICT regulators** identifies consumer-oriented actions likely to fall to ICT regulators.
- **Specific consumer issues** identifies key consumer issues already arising, and outlines changing consumer horizons and needs.
- Finally, **Key findings** summarizes the most important lessons from the chapter.

Consumer rights and responsibilities in the digital world

In ICT regulatory contexts, the term *consumer* usually means a person who buys services for their own or household use. Often it extends to people who buy services for both business and personal use, or for study purposes.[6]

This means that most people in the world are consumers of ICT services.[7] This fact is helpful for regulators who have difficulties in finding consumer representatives to consult on policy issues, or who wonder what actions would best serve consumers. Although these questions are best explored using consumer consultation and research, a good start can be made by considering the consumer needs of one's own family, friends, and acquaintances – especially where these include people living in rural areas, on low incomes, or in otherwise disadvantaged circumstances.

Basic consumer rights across all sectors were identified in the 1960s as: access, choice, information/education, safety, redress, sustainability, and representation.[8] The 2014 ITU Global Regulatory Symposium incorporated these into their Best Practice Guidelines on consumer protection in a digital world, which are summarized in Box 4.2. These are evolving, for example, into the fuller set shown in Table 4.1, based on consumer research in 23 mainly developing countries, which shows how ideas of consumer and citizen rights are becoming more varied and converging to what are now called digital rights, which accrue to people without role distinction.[9]

6 A more detailed discussion of this and related terms (including (end) user, (business or residential) customer, potential consumer and citizen) is given in Digital Regulation Platform thematic section on "Consumer protection in general".

7 In the *Digital Regulation Handbook and Platform*, the term information and communications technology (ICTs) generally refers to telecommunications and related equipment and networks, while "digital" refers to Internet and online-related concepts.

8 See UNCTAD (2016) for the latest set of basic consumer rights.

9 *Digital Regulation Platform* thematic section on "Consumer rights in the digital context" provides a more detailed discussion. The Consumers International report from which Table 4.1 is adapted contains more information on the situation in 2017 and how it may change.

Box 4.2. Areas covered in the GSR-14 Best Practice Guidelines for Consumer Protection in a Digital World

1. **Charting a strategic direction** giving consumer affairs a higher and better defined profile within a forward-looking overall policy framework covering both national and international contexts.
2. **Enhancing market competitiveness** at all levels, treating both ICT providers and OTT service providers equally in regard to consumer protection.
3. **Partnering with industry**, taking advantage of providers' desire to protect consumers from potential harm.
4. **Providing a sound framework for contractual services** ensuring transparency, and balance between rights and obligations.
5. **Multiple channels for redress** so that consumers can defend their rights rapidly and at no or minimal cost.
6. **Quality of service and consumer experience,** introducing measures to assure easy and reliable access to ICTs and web content for all, including consumers with disabilities.
7. **Protecting consumer privacy and data,** requiring consumer opt-in for online data collection, paying special attention to protecting children and young people, and setting up computer emergency response teams (CERTs).
8. **Empowering consumers** through education, awareness-raising, and participation in policy dialogues, using new media as well as traditional channels like schools.
9. **The consumer right to information,** ensuring clear, up-to-date, comparable information in a form that supports consumers' decisions.
10. **Redefining the role of regulators,** possibly including consumer advocacy, bringing evidence, technical expertise, and strong enforcement to bear on matters that concern consumers.

Source: ITU 2014.

Of course, the existence of rights in law varies from country to country, as does their implementation. Rights entail corresponding responsibilities. Consumer responsibilities include:

- Paying agreed charges for service.
- Observing applicable laws online as much as offline, and in particular not engaging in fraudulent or otherwise criminal activity.
- Behaving online in accordance with applicable rules and norms, such as observing copyright and privacy restrictions, using acceptable language, and not deliberately misleading others.
- Looking after passwords and keeping up-to-date with security updates to apps and software.
- Taking care of usage by their children and others around them who may need help.

Table 4.1. Mapping digital rights for consumers and citizens

DIGITAL RIGHTS FOR PEOPLE AS...	
CONSUMERS	**CITIZENS**
1. Access and inclusion	
• Affordable access and devices • Quality, reliable connection • Relevant content • Right to cap-free Internet • Infrastructure for remote areas	• Freedom from online harassment • Equality and inclusion • Freedom of association • Open networks
2. Disclosure and transparency	
• Meaningful information, easy to access and understand • Fair contracts • Informed choices • Transparent business models and terms of use	• Free press, freedom of information • Right to communication • Freedom of expression, end to censorship • Filtering/content controls
3. Security and safety	
• Data protection/security from fraud/loss • Redress for breaches • Right to safe and private digital products and services, including for vulnerable consumers • Transparency on data breaches • People are who they say they are (digital ID)	• Secure public services particularly for sensitive data such as health • Safe space for all online: women, minority groups, children, free from hate speech • Cybersecurity
4. Data protection and privacy online	
• Privacy – end to corporate surveillance • Freedom from invasive marketing • End to price/quality/service discrimination • Special provisions for sensitive data and vulnerable consumers	• Right to be forgotten • Freedom from state surveillance • End to data-led bias in decisions about jobs, education, justice, public service, etc.
5. Competition and choice	
• Choice of provider and ability to switch easily • Enforcement of competition law • Recognition of data holder's advantage • Fair choice regardless of location • Fair, inclusive markets	• Rights to access justice with a fair hearing
6. Fair use and clear ownership	
• Rights to repair • Right to reply/due process for automated sanctions • Reasonable lifespan and support	• Fair copyright regimes • Digital rights management • Fair use • Access to knowledge
7. Redress and complaint handling	
• Right to easy, simple, and cost-effective access to redress	• Rights to access justice and be compensated for harms

DIGITAL RIGHTS FOR PEOPLE AS...	
CONSUMERS	**CITIZENS**
8. Digital education and awareness	
• Right to consumer education • Systems and products that are easy to use • Access to content • Reliable and verifiable sources	• Rights to education to manage risks and maximize opportunities online • Rights to digital literacy provision • Local language provision
9. Regulatory framework	
• Rights to be heard in digital policy making • Processes for companies to respond to consumers • Transparent processes	• Diversity of voices in Internet governance • E-voting • Civic and political participation, online protests • Freedom of information
10. Responsible business practice	
• End to price/quality/service discrimination • Accountable information/content • End to lower standards for lower income countries • Companies meet human rights obligations	• Ethical data supply chains • Duty of care • Employee conditions: fair treatment, free from surveillance

Source: Adapted from Consumers International 2017a.

General and special consumer protection law

General consumer protection law has a long history [10] and, over time, its underlying principles have been elaborated in laws that balance the rights of consumers against those of producers. Adjustments are needed as underlying power structures change; typically, the growing relative strength of producers has led (after some delay) to more legal protections for consumers.

Because of its monopoly past and its nature as an essential service and an *experience good* (which can only be known by trying it out), various special consumer protection regulations[11] for electronic communications have been put in place in different jurisdictions. For example, providers may be required to make both network services and customer services accessible to people with disabilities, and maximum contract lengths may be laid down.[12]

Similarly, special protections are often required for e-commerce transactions. These are justified because consumers usually cannot inspect their potential purchase before making it, and can be subjected to pressured sales techniques, such as "one time" offers and sign-up bonuses. General consumer protection authorities are more likely than ICT regulators to be responsible for enforcing these, but ICT regulators should be aware of their existence. The

[10] The UN Consumer Protection Guidelines, based on principles articulated by U.S. President Kennedy in the early 1960s, were first adopted by the General Assembly in resolution 39/248 of April 16, 1985, later expanded by the Economic and Social Council in resolution E/1999/INF/2/Add.2 of July 26, 1999, and revised by the General Assembly in resolution 70/186 of December 22, 2015.

[11] Throughout this chapter, the term "regulations" includes relevant licence conditions.

[12] These are explored in *Digital Regulation Platform* thematic section on "Consumer rights in the digital context".

broader regulation of digital platforms like Google, Amazon, and Facebook is a topic of current debate because of their transnational nature, often coupled with market dominance.

Table 4.2 shows the worldwide variation in existence of a suite of laws deemed essential for developing the digital economy in ways that are safe for consumers, and who is responsible for telecommunication/ICT consumer protection issues. Key points to note include:

- There are still large gaps to be filled in essential legislation, most markedly in general consumer protection laws and data protection laws[13] in the African, Arab, Asia-Pacific and CIS (Commonwealth of Independent States) regions.
- In all regions except the Americas, significantly more countries have specific telecommunications consumer protection legislation/regulation than have a general equivalent. In other words, ICT regulators are ahead of the game.
- In all regions, a large majority of ICT regulators are responsible for handling consumer complaints. Where a separate consumer protection authority exists, it rarely has jurisdiction on its own for consumer protection issues related to the telecommunication/ICT sector – rather, this jurisdiction either belongs solely to the ICT regulator or (more commonly) is shared between the two. In other words, ICT regulators are tending to collaborate with consumer protection authorities.

Figure 4.1 shows the percentage of regulators reporting involvement in certain activities relevant to consumer affairs in ITU surveys carried out in 2007 and 2019. There is an increase in all activities between the two years. Overall, it seems that most ICT regulators are already active in consumer affairs, and those that are not have plenty of examples to follow.

The ITU's 2018 report on regulatory collaboration (ITU 2018a)[14] contains a more detailed exposition of these and related trends.

Table 4.2 Responsibility for ICT consumer issues and relevant legislation worldwide

		Africa + Arab States	Asia & Pacific + CIS	The Americas	Europe
Total countries in region		65	49	35	46
Data from ITU Consumer Measures Survey 2019					
Jurisdiction over consumer protection issues related to the telecommunication/ICT sector (%)	Telecom/ICT regulator	62	29	34	26
	Consumer protection authority	5	6	20	9
	Both authorities	17	24	31	48
Separate consumer protection authority exists (%)		31	41	57	72
Regulator responsible for consumer complaints (%)		91	76	83	85

[13] Law firm DLA Piper provides a useful facility for comparing data protection laws worldwide, at https://www.dlapiperdataprotection.com/#handbook/world-map-section.

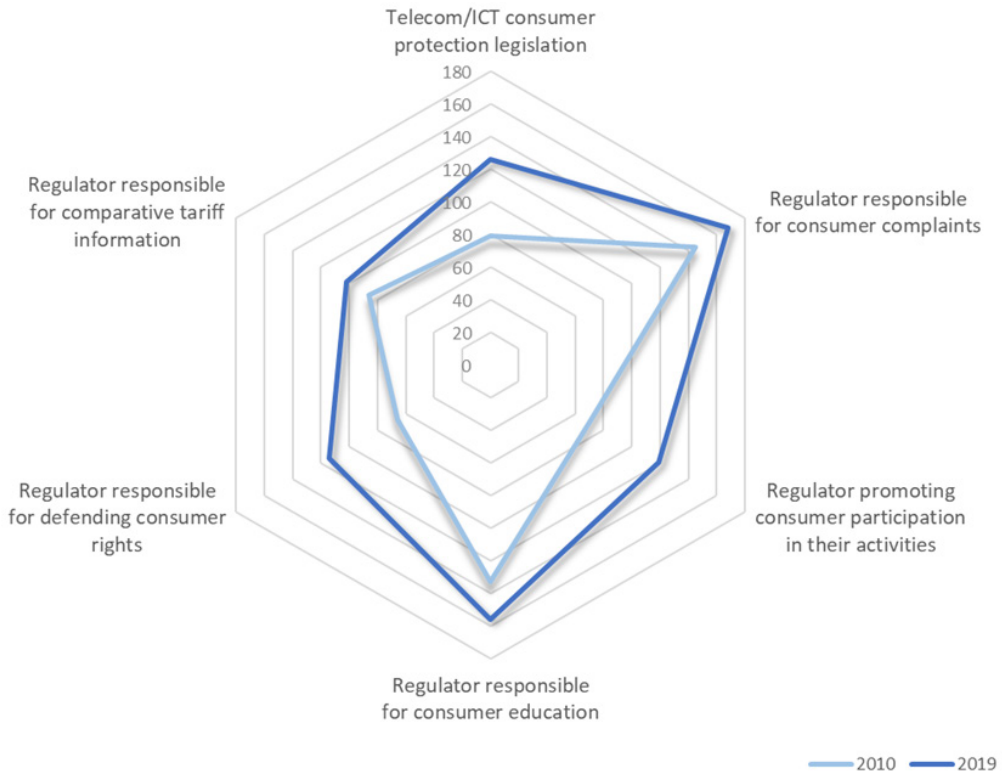
[14] See especially chapters 4 and 5, and within chapter 4, the section on "Developments in the field of consumer protection (pp. 53-55) and within chapter 5, section 5.3 on "Power coupling: the ICT regulator and the consumer protection authority" (pp. 133-134).

	Africa + Arab States	Asia & Pacific + CIS	The Americas	Europe
Specific telecommunication consumer protection legislation/regulation exists (%)	65	55	46	83
Data from UNCTAD Summary of Adoption of E-Commerce Legislation Worldwide				
General consumer protection law exists (%)	42	31	80	74
Data protection/privacy law exists (%)	51	45	77	91
E-transaction law exists (%)	71	69	94	91
Cybercrime law exists (%)	69	67	86	91

Source: Based on data from ITU and UNCTAD.

Note: **UNCTAD data were taken on May 21, 2020 from** https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx **(data subject to continuous update). "Law exists" means positive response received. ITU data are from responses to its 2019 survey.**

Figure 4.1 ICT regulators reporting activities relevant to consumer affairs, 2010 and 2019



Source: ITU.

Average consumers and vulnerable consumers

Consumer protection law is often framed in terms of imaginary *average consumers*, who are supposed to be "reasonably circumspect" and able to look after themselves. Increasingly,

however, regulatory concern has been refocused towards *vulnerable consumers*, who are more likely than average to experience detriment in a specific context. Who is regarded as vulnerable will vary. For example, people with impaired hearing are more likely than average to have difficulty with a voice conversation, and people with low incomes are more likely than average to be unable to maintain service when prices rise. Anybody can become vulnerable for a while, for example, through job loss or bereavement.

How regulators should balance the attention paid to the interests of vulnerable consumers compared with average (or privileged) consumers is often a political matter. Equality legislation often requires reasonable adjustment to the needs of people with disabilities, and governments may provide social policy guidance. Economic analysis requires assumptions about aggregate utility or welfare, which may not match intuition.[15] Whatever economic approach is adopted, regulators must clearly recognize that consumers vary greatly in their general and digital behaviour, desires, and resources, and assess the effects of policy decisions on different segments, including the most vulnerable.[16]

The shift to online data

The past decade has seen major change in consumers' take-up and use of digital services.[17] A market that was dominated by voice telephony is now dominated by data. Voice is still a very popular communications medium, but now is often carried over Internet Protocol (IP) and paid for as part of an Internet or data package. Protecting consumers' interests in data is only one of a suite of policies needed to foster safe and beneficial data-driven economies.[18]

Electronic communications have always raised privacy issues, related both to their content and to their circumstances (that is, metadata, which would typically include the calling and called numbers and the time, date, duration and location of a call).

Now, Internet use (often via apps) has vastly multiplied both the amount and the type of data that providers can collect from users. Often, this includes their location, interests, browsing history, and transactions – and who is in their social network. Going further, smart objects, like voice assistants in homes, and CCTV cameras and connected vehicles in streets, may capture and transmit information about people who are unaware that such data is being collected. Put together, this so-called big data reaches ever more powerful data processing units, which through artificial intelligence (AI) techniques can now detect patterns in the data and reach probabilistic conclusions about groups and individuals.

These major developments can both benefit and harm consumers.[19] A topical example in 2020 is the use of data in response to the global COVID-19 pandemic – it can help in tracing potential infection, while at the same time raising concerns about unwarranted surveillance. In many countries, data protection legislation is being introduced or strengthened, and specialized

15 The welfare weights approach, based on the principle that a USD1 price rise matters more to a person with USD10 than to a person with USD100, is explained in Cowell and Gardiner (1999).
16 See for example Ofcom (2019) and UKRN (2020). The latter is a good example of regulatory collaboration and data use as well as attention to consumer vulnerability.
17 See, for example, Chapter 3, Figure 3.1 "Individuals using the Internet and growth rates".
18 See Chapter 5 on "Data protection and trust".
19 See World Bank (2019a).

data protection regulators are being set up or expanded.[20] In parallel, debates are in progress around the world on the ethical use of data.

4.2 Consumer support framework

Roles in protection and empowerment of digital consumers

The ITU (2018a) has shown clearly how different countries have different institutional arrangements for handling consumer affairs, both generally and in specific sectors, digital being just one (cross-cutting) sector. Whatever the institutional set-up, certain roles should be fulfilled. Table 4.3 identifies essential roles and suggests typical organizations that may be charged with fulfilling them. Community groups and social networks add great value in sharing concerns and information, but also bring risks of misinformation and disinformation – with the COVID-19 pandemic again providing examples.

Table 4.3 Roles in digital consumer affairs

Role in relation to digital consumers	Typical organizations involved in fulfilling the role
Consumer and sectoral policies	Ministries (with wide public input), competition authority
Understanding consumer needs	Consumer organizations, **regulators**, service providers
Consumer protection legislation	Executive branch of government, parliament, courts
Consumer protection regulations and codes of practice	**Regulators**, service provider associations, standards bodies
Provision of consumer information	Service providers, comparison and review websites, online forums, consumer organizations, **regulators**
Consumer education	Schools and colleges, broadcasters, press, **regulators**
Monitoring market functioning	Service providers, **regulators**, competition authority
Complaints handling	Service providers, **regulators**, ADR bodies, courts
Enforcement	**Regulators**, local authorities, police, courts

In Table 4.3, the term "regulators" refers to all regulators who are involved in protecting the interests of consumers when they interact with providers digitally. This will include consumer protection authorities, data protection regulators, and financial services regulators, and often also others – for example, energy regulators, if consumers deal with energy providers online. A typical ICT regulator will have all the "regulator" roles above in relation to connectivity and some online content issues, and will need to work closely with the other types of organization mentioned in the table, including other regulators.

[20] See ITU (2018a), chapters 4 and 5, which deal with the remit and powers of ICT regulators and their relationships with other regulators.

Consumer-provider relationships

Companies often say that they understand their customers and potential customers better than regulators ever can, so there is no need for regulators to carry out consumer research or consult consumers. The first part is true: companies have both incentives and resources to understand what satisfies their customers. However, the second part does not follow from the first. Companies are likely to understand only their own customers (or, possibly, their direct competitors' customers), and to focus resources on the most profitable market segments. To fulfil their duties, regulators need an overview of the needs of all consumers and would-be consumers, including those "at the bottom of the pyramid" who do not much interest some service providers.

Regulators should not come between companies and their customers, unless direct relations have reached an impasse (or, exceptionally, serious misconduct is alleged). Satisfied consumers are companies' best marketing channel: welcoming complaints, acting on them at the individual level, and using them as a source of market intelligence, can improve customer service and boost competitive advantage. Regulators should help this constructive relationship to flourish through dialogues with both consumers and service providers. Digital media, such as online surveys, can contribute to dialogues with consumers, but it is important to be aware which consumers are taking part and which are excluded.

Roles of ICT regulators

Specific roles of ICT regulators are shown below. As discussed above, these have become more important and now often extend into aspects of content and data as well as connectivity. What is more, digital media can now help in carrying them out well, for example, through crowdsourcing of consumer views of service levels.

- Regulating companies' handling of customer complaints about their services, and monitoring compliance with regulations.
- Providing or facilitating complaints channels of last resort, to resolve difficult cases.
- Monitoring complaints received in all relevant channels, to assess efficacy of processes, track trends, and spot new issues as they emerge.
- Providing a consumer-oriented part of their website, or a separate consumer website, complete with interactive options to enable consumers to get advice tailored to their own situations. This might include, for example, lists of providers offering service in specific locations, or offering particular features possibly of niche interest (e.g. catering for a disability), or "best buys" for certain usage patterns.
- Supporting grass roots and regional or national consumer groups to get organized, to support individuals with problems and gather consumers' views on digital issues.
- Engaging with those groups, both to help with their consumer education, and to learn from them how well current policies are working.
- Carrying out targeted consumer research to throw light on consumers' priorities and preferences; and following relevant research done elsewhere, including behavioural studies.
- In close collaboration with consumer groups and (where they exist) consumer protection authorities, developing regulations and codes of practice for consumer empowerment and consumer protection
- Making policy consultations accessible to consumer groups and welcoming their inputs, especially where the policy in question directly affects consumers.
- Collaborating with others to help consumers find the right place to go for the support they need.

Relevant international bodies

International bodies can help national regulators to handle consumer affairs in various ways, including:[21]

- Ensuring that frameworks for international trade and cooperation take account of consumer interests – for example, the United Nations Conference on Trade and Development (UNCTAD) and the TransAtlantic Consumer Dialogue (TACD).
- Supporting each other's enforcement efforts related to cross-border e-commerce and illegal activities – for example, the International Consumer Protection and Enforcement Network (ICPEN) and Unsolicited Communications Enforcement Network (UCENET).
- Devising international standards, among others for ICT and digital related products and services – for example, ITU, the International Organization for Standardization (ISO), and ANEC (the European consumer voice in standardization).
- Providing training and examples of good practice in ICT and digital consumer affairs, primarily for regulators and other officials – for example, ITU.
- Setting legal and policy frameworks for consumer affairs that command widespread acceptance and influence – for example, EU and OECD.
- Articulating consumer perspectives on ICT and digital issues – for example, Consumers International and BEUC (The European Consumer Organisation).

Many other international bodies, in particular regional associations, also play useful roles.

4.3 Specific consumer issues

Price and quality of service

Service pricing generally remains the single most crucial aspect for consumers, when both choosing and using services. Low-priced packages attract many consumers, even when low price entails lower quality. New market entrants typically price a few percentage points below incumbents in order to attract their early customers, and competition is nearly always on price as well as on service features.

Regulators' roles in controlling and monitoring pricing are explored elsewhere in this handbook.[22] Regulators should further help consumers by ensuring that providers' pricing information is easily accessible, understandable, and accurate. Comparison websites can help consumers choose the best provider and package for themselves, usually only comparing prices; some regulators provide this information, while others encourage consumer or commercial organizations to do so. [23] Another handbook chapter discusses how regulators can help consumers to assess the quality of service they should expect.[24]

---

21 *Digital Regulation Platform* thematic section on "International organizations relevant to consumer affairs" provides more detail and links.

22 See Chapter 2 on "Competition and economics".

23 See, for example: https://www.comreg.ie/compare/#/services ,provided by the Commission for Communications Regulation in Ireland; http://www.anacom.pt/tarifarios/Paginalnicial.do ,from Anacom in Portugal; or https://www.meilleurtarif.be/ ,from BIPT in Belgium. As markets attract more service providers and more varied packages are offered, the comparison task becomes more challenging, and some regulators have left it to external providers – see for example the Czech regulator at https://www.ctu.eu/price-calculators . The formerly exemplary LetsCompare facility at www.consumerinfo.my , may be in course of revision.

24 See Chapter 8 on "Technical regulation", which covers quality of service.

The topic of zero-rated content, provided free of charge to consumers by certain service providers, for example Facebook in its Free Basics offering, has proved controversial.[25] On the one hand, many users, especially in lower-income groups with limited data allowances, have welcomed the offering, and, in some countries, it appears to have supported higher take-up of the Internet as well as higher usage of Facebook. On the other hand, some regulators regard such offerings as discriminatory and counter to the principle of net neutrality; India is the prime example of a developing country that has outlawed zero-rated content on these grounds. An OECD study (OECD 2019a) concluded: "The effects of zero rating can be very diverse and depend heavily on the circumstances of individual countries…case by case analysis is almost indispensable". An earlier study by the Alliance for Affordable Internet (A4AI 2016) came to a similar conclusion, but also provided guidelines to regulators for how to use zero rating to extend access while preserving competition.

Contracts and prepayment

Originally, relationships between service providers and their customers required explicit written agreements, known as contracts. These are still widespread, and often preferred by connectivity providers (CPs) as they provide a predictable revenue stream. Typically, they allow customers to pay usage charges at the end of each month for the service they have already received, an arrangement known as credit or postpayment.

Once entered into, postpayment contracts may last indefinitely (until terminated by either party, usually after a given notice period), or they may have a set duration, typically of a year or more. Regulators may limit contract durations, because contracts that are too long can weaken competition and tie consumers in to deals that no longer suit them.

Since mobile prepayment arrived in the 1990s, it has become extremely popular around the world, because by ensuring that consumers never owe money it sidesteps the formality of traditional contracts and gives consumers much more flexibility over their spending.[26] Although it is especially appreciated by lower-income consumers, consumer protection in prepayment relationships is much less well developed than its postpayment contractual equivalent. Some regulators have taken steps in this area; for example, TRAI [27] in India requires operators to adopt a standard colour code for prepaid vouchers to make their tariffs easier for consumers to understand, and also to provide consumers with both current and retrospective records of how usage reduces their credit balance.

Particularly in e-commerce, contractual terms and conditions (often presented online) are a frequent source of annoyance and complaint. They are often unreasonably long and complex, consumers rarely read them and often feel they have no choice but to accept them.[28] The U.K. government has published materials (Behavioural Insights Team 2019) providing practical guidance for improving this situation, and an international standard is in preparation building on this foundation.

25 As has the larger topic of net neutrality, which encompasses zero rating and is discussed in Chapter 2.
26 See Digital Regulation Platform thematic section on "Mobile prepayment".
27 See TRAI (2018), chapter 1.
28 See, for example, Which? (2018).

Billing and payment procedures

Digital payments can often be made via CPs for digital content and services received. In-app purchases may be paid for using specialized virtual currencies, but ultimately a consumer's account may need external funding with "real money", first converted into electronic credit, for example via a mobile payment account like M-Pesa in Kenya and elsewhere. Established payment mechanisms include calls and messages which are charged at a premium rate, some of which is passed on to a content provider. These and alternatives [29] which enable payment via a CP have led to many dissatisfied consumers, often because the content provider can "hide" behind the CP and even disappear. Different consumer protection systems exist, [30] often involving coregulation, but overall there is a trend away from these indirect payment mechanisms and towards mobile payment apps, like the Malaysian mPay Walet, which are typically regulated as financial entities.

Consumers' options for paying amounts due to their service providers can also make a big difference to the attractiveness of the service. Ideally both cash and electronic payment should be accepted, without significant payment charges. Time limits for settling postpaid bills must be reasonable, taking account of possible delivery delays (particularly for paper bills).

In case of undisputed non-payment of amounts due, or lasting non-use of a service, service providers may embark on procedures to restrict and ultimately disconnect service. ICT regulators should make sure that these procedures are fair and clear to consumers who experience them, giving the consumers reasonable opportunities to recover full service.

Of course, the amounts that customers are charged must correspond accurately to their chosen package and services accessed through it, with any additional usage charges demonstrably matching actual usage. A high proportion of consumer complaints is usually related to incorrect billing.

Customer service, complaints, and redress

Consumers need to be able to contact their service providers and receive timely responses from them. Ideally, service providers will enable their customers to choose among a range of contact channels, for example, shops, telephone, email, text, or online messaging. Such options are especially important when the consumer has a problem which means they cannot use their own service, for example, to report a fault or restore a disconnected service. The quality of customer service is an important dimension of overall quality of service, and as with other aspects of quality of service, regulators may intervene in markets to varying extents.

However, complaints handling often requires regulatory intervention, because the market incentives on service providers to deal appropriately with unhappy customers are too weak. Typically, regulators require service providers to acknowledge and respond to complaints within specified periods; and provide or organize back-up adjudication for complaints which

[29] For example, the U.K. mobile payment mechanism Payforit, explained here: https://www.resolver.co.uk/consumer-rights/three_pay_monthly-payforit-complaints .

[30] An established example is the U.K. premium rate service regulator, PhonePaid Services Authority. A 2011 overview of regulatory arrangements in 20 countries is available at https://psauthority.org.uk/-/media/Files/PhonepayPlus/Research/Mason-International-Markets.pdf?la=en&hash=3AAF54A57288481AE77FA4727BF4226020033F47 .

are not resolved to customers' satisfaction by service providers. Redress can take various forms, including apologies, righting errors, and paying compensation. [31]

As mentioned above, billing and payments often cause the most complaints to regulators, with quality of network service and customer service following behind. However, particularly in some English-speaking jurisdictions, unwanted commercial calls and messages have become a major problem over the past decade – and these are now spreading to more countries. These often are, or look like, telemarketing attempts, but a proportion have outright fraudulent intent (for example, "wangiri" calls which ring off before they can be answered, encouraging a costly return call from which the fraudster benefits).

Early control measures often take the form of "do not call" lists,[32] where consumers who do not want to receive unsolicited commercial calls or messages can register their telephone number and genuine telemarketers are not allowed to call them. Automated calls (also known as "robocalls" are also illegal in many jurisdictions. However, it is all too easy for wrongdoers to flout these rules, and available enforcement effort has to be focused where it is most effective. Increasingly, technical measures are being introduced in networks, apps, and terminal equipment to stop unwanted calls reaching their targets. [33]

Helping consumers navigate the digital economy

A single digital consumer transaction (for example, a payment to access a music track) can involve a long chain of service providers (in this example, the original performer, recording studios, agencies, content aggregators, online merchants, online money account managers, and Internet service providers). If the consumer seeks prepurchase advice, or if something goes wrong, for example a duplicate payment takes place, who should a consumer approach and how are they to be found? A "one-stop shop" which can point consumers to the right place will help.

The ITU has highlighted [34] the importance of regulators of different sectors and at different levels working together, and this is particularly the case when helping consumers to help themselves. Even for experts the picture is complex, and most people cannot find their way around unaided.

At least, all bodies that offer to help consumers, whether commercial, governmental, or NGOs, should have access to a shared up-to-date database on which of them is responsible for what topic. Usually this can most conveniently be shared online, and a version of it can be made directly accessible to consumers. [35] It should also form a valuable source for organizations and telephone helplines that provide advice and support to consumers, helping to ensure consistency of approach.

Web search will help skilled Internet users to find what they need, but many people still prefer (or can only use) voice services. Ideally, a well-publicized telephone helpline with an easily

---

31 *A Digital Regulation Platform* thematic section on "Redress" examines this in more detail, and also collective complaints and collective redress.

32 Also known as "Robinson lists", after Daniel Defoe's fictional character Robinson Crusoe who lived alone on an island for many years.

33 The topic was addressed in ITU (2017b), reporting on activities from 2014 to 2017, and will be addressed more thoroughly in its successor volume. See Milne (2016) for a presentation on the international situation in 2016.

34 For example, in ITU (2018a).

35 An example from the United Kingdom can be found at https://www.iwf.org.uk/resources/useful-links .

remembered number that is free to call would be provided for consumer support. Enquiries may be routed via interactive voice response and use chatbots. Ideally, it should also be possible for callers to speak to well-informed, sympathetic live operators who speak their language, but this is likely to raise costs. To limit demand for live operators, special numbers may be provided for people who most need their help, such as those with certain disabilities.

Good businesses will benefit from well-informed, confident consumers and may make voluntary contributions, in cash or kind, to the provision of consumer support. Regulators could also require such contributions – for example, the Indian regulator, TRAI, requires service providers to pay into a Consumer Protection and Education Fund any amounts that are due to customers but which cannot be paid to them.[36] Consumer protection and education could be another application of universal access and service funding.[37]

Provision for consumers with disabilities

The ageing of the world's population inevitably brings with it a higher proportion of people having some impairment – physical (such as loss of a limb), sensory (such as being blind or deaf) or cognitive (such as dyslexia). The United Nations Convention on the Rights of Persons with Disabilities demands equal treatment for people with disabilities,[38] and specific laws and regulations often interpret what that should mean in practice.

The first concrete recognition by ICT regulators of the special needs of people with disabilities has often been through universal access policies.[39] Increasingly, regulators are also implementing ICT accessibility policies, which may deal, for example, with specialist equipment and the usability of online resources. An ITU survey in 2019 showed that only 29 per cent of 195 regulators responding worldwide had no ICT accessibility framework, with separate attention being paid to mobile, TV/video programming, web and public ICT accessibility, as well as other aspects. However, the percentage with no accessibility framework rose to 48 per cent in Africa.

The South African regulator, ICASA, has a Consumer Advisory Panel [40] which includes representatives of people with disabilities. It also has a comprehensive Code for People with Disabilities,[41] listing many requirements on operators to cater for special needs.

Australia has long had an active disability movement and a responsive regime. A special "accessible telecoms" website [42] demonstrates both a wide range of equipment and services and clear, accessible presentation. The regulator has approved a series of industry Codes of Practice on Accessibility.[43] Compliance with information requirements (to enable people to choose the equipment best suited to specific needs) is compulsory.

---

36 See TRAI press release at https://trai.gov.in/sites/default/files/PR_No.08of2020.pdf ,about an amendment in January 2020.

37 See Chapter 3 on "Access for all".

38 https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html .

39 See Chapter 3 on "Access for all".

40 https://www.icasa.org.za/pages/consumer-advisory-panel .

41 https://www.icasa.org.za/uploads/files/Code-for-People-Disabilities-2014.pdf .

42 Supported by both the regulator, ACMA, and the consumer organization ACCAN:https://www.accessibletelecoms.ideas.org.au/telecom-home.html .

43 Hosted and managed by the industry Communications Alliance: https://www.commsalliance.com.au/Documents/Publications-by-Topic/accessibilty .

Going beyond equitable access, digital technologies can offset disabilities and enhance lives, with broad social and economic benefits. As an example, recent research into ensuring that people with hearing loss can benefit from smart home technology has highlighted the importance of developing mainstream technologies with flexible user interfaces.[44] For example, audible user signals should be capable of being expressed visually.

Smart consumer devices

Telecommunication regulation has focused on networks rather than equipment. Regulatory duties related to devices have usually been limited to ensuring their compliance with standards designed to safeguard users and networks and combat counterfeiting. The important consideration of electromagnetic field (EMF) radiation safety is discussed in Chapter 6 on "Spectrum management". Consumers deserve reliable, independent advice on the safe use of wireless devices, particularly with the advent of 5G.

The arrival of smart devices raises the question of extending regulators' remit to other aspects of devices that are significant for competition and consumers. The French regulator, ARCEP, has studied how devices limit Internet openness (for example, because of the need for apps to be compatible with proprietary operating systems), and recommended actions to control this harm (ARCEP 2018).[45]

But multifunctional smart mobile phones are already pervasive. They act not only as telephones but also as cameras, clocks, calculators, TVs, radios, and wayfinding devices – and provide Internet access, often via apps. Smart phones are now being joined by smart watches, smart speakers and other connected devices used at home or on the move, which are being widely taken up by consumers in developed countries and spreading across the world.

These capabilities open new ways for consumers to stay in touch with family, friends, and associates; to learn, earn, spend, save, and play. But they also open new risks, for example, of wasting time and money, and of being misled, deceived, or let down. In extreme cases, they can even lead to addiction, typically through gaming or gambling, or simply excessive social media use.

These sophisticated functions span the different aspects shown in Chapter 7, Figure 7.7, and apps can take consumers into areas as diverse as healthcare and agriculture.[46] ICT regulators cannot, and are not expected to, protect and support consumers everywhere that a smartphone may lead them. They must exercise the essential functions that they are given in their own country, in relation to their applicable jurisdiction, and collaborate with other bodies to achieve broader coverage.

Regulators also need to remember that smart device access and use is still far from universal. Even in developed countries with effectively universal and affordable fixed and mobile broadband, a proportion of consumers do not take up the Internet, whether through choice or through encountering barriers such as disability or lack of confidence. In less developed countries, availability and affordability are often lower and barriers higher, leading to larger offline populations. Proxy use (for example with a younger person helping an older one) is a common way for people to gain some benefits from the digital world while remaining offline.

---

44 https://petras-iot.org/update/people-with-hearing-loss-and-connected-home-technologies/ .

45 A comic strip introduction to the issues can be found at https://en.arcep.fr/uploads/tx_gspublication/comic-strip-devices-feb2018-ENG.pdf .

46 See ITU (2017a) for a discussion of the economic potential of apps and the challenge of regulating them.

Intermediary services accessible via ordinary phones are another, for example, enabling farmers to access current crop prices by voice interaction. Such services may be seen as digital even if access to them is not.

Trust requires trustworthiness

Just as in the physical economy, a flourishing digital economy depends on consumers' trust – that is, their belief that others will act in honest and ethical ways. Trust in turn depends on assessment of others' trustworthiness. In the physical world people rely on personal knowledge or recommendations of which individuals or organizations are trustworthy.

In the digital economy, personal knowledge and recommendations also play a part, but they are nowhere near enough, because the others are so many, can be anywhere in the world, and may not be what they appear. Consumer review websites like Trustpilot and Tripadvisor can be valuable but also risky (OECD 2019b): because it is so easy to fake reviews, industry codes of conduct can make them more reliable, but are not the whole answer. Building consumer trust in the digital economy is a major challenge, not least because of continual setbacks when bad experiences undermine trust. Bad experiences may include interference with connectivity (such as the nuisances of spam and phishing, and security failures like malware and hacking), as well as difficulties with online activity and transactions (such as duplicate payments, disappointing content, or non-existent products). Security and especially privacy have proved to be significant new concerns for consumers – even though their behaviour may suggest otherwise.[47]

ICT regulators can help to promote consumer trust by requiring or incentivizing good business practice that demonstrates trustworthiness. They can also help to educate consumers to be on their guard against bad practice, such as sale of their data leading to unwanted targeted advertising. Where practical, they may take enforcement action against wrongdoers, collaborating across borders with their counterparts elsewhere. Major disputes may reach the courts, if there is one with appropriate jurisdiction.

Online safety for children

Children (defined as people aged under 18) are often more skilled than their parents or teachers at operating smartphones and other connected gadgets, and all over the world have adopted new technologies with enthusiasm as "digital natives". They readily learn, communicate, and play using these technologies. However, they still lack life experience, and may fall prey to harms. Risks are commonly divided into the "4C" categories below:

- Content risks: where children are exposed to harmful material (e.g. pornography, hate speech, violence);
- Contact risks: where children are involved in usually adult-initiated online activity (e.g. grooming, stalking, sexual exploitation);
- Conduct risks: where children are victims or perpetrators in peer-to-peer exchanges (e.g. bullying, sexting, revenge porn);
- Commercial risks: where children are exposed to inappropriate advertising, marketing schemes or hidden costs (e.g. targeted advertising, fraud, scams).

[47] See findings of Which? research on consumer attitudes and behaviour in 2019 and 2018 at https://consumerinsight.which.co.uk/articles/consumer-data-summary . The findings of behavioural economics are also relevant here.

Some of these can be addressed in legislation, for example, on data protection and obscenity, but these and other rules are only useful to the extent they are enforced. Ensuring rapid removal of even clearly illegal material from the Internet has proved to be a major challenge, best addressed by collaboration between Internet service providers in a child protection context. The European hotline network, INHOPE, has 46 national members operating collaboratively to take down illegal materials.[48]

Naturally, the adults around them are anxious to protect children from harm, and this may lead to strict controls or even banning of "screen time". However, extensive research in many different countries shows the importance of helping children to benefit from the many advantages of online activity,[49] and of a measured and age-appropriate approach to controlling their Internet use. The aim is for them to reach young adulthood as fully competent Internet users who understand both the benefits they can get from it (for example in job search or further education) and how to avoid being misled, deceived, or exploited. As part of the work carried out in 2019 by the Broadband Commission for Sustainable Development's Working group on child online safety,[50] a universal declaration [51] was adopted that outlines the steps that public and private entities must take in order to safeguard children online that complements the ITU's work on child online protection.[52]

Online safety for adults

Adults can also be vulnerable to harms similar to those that affect children online, especially if they lack experience or belong to a disadvantaged group. Challenges that women have faced in an online environment are already extending to abuse via connected objects.[53]

In addition, as consumers, adults may suffer financial loss through e-commerce or other online transactions, using virtual and electronic money (which deserve, but as yet often do not have, the same legal protection as "real" money). And, as citizens, their voting and other political behaviour may be influenced by online messaging, particularly via social media.

As in the case of children, there are no easy answers. Now that the Internet has become such an integral part of life, barring access to it is rarely justifiable. A balanced, effective approach would include a mix of the following types of government action:

- Improving Internet skills and media literacy, so that people learn both to find what they want online and to assess its likely safety and reliability.
- Assuring for everybody unrestricted online access to content which is legal according to national laws, with due respect for social norms.[54]

48 https://www.inhope.org/EN .
49 See for example http://globalkidsonline.net/ . Many other valuable resources are available via ITU's special Child Online Protection website at http://www.itu.int/cop .
50 https://www.broadbandcommission.org/workinggroups/Pages/WG1-2018.aspx .
51 http://www.childonlinesafety.org/ .
52 https://www.itu.int/en/cop/Pages/guidelines.aspx .
53 See summary of Ugandan women's experiences at https://cipesa.org/?wpfb_dl=329 , and U.K. research project "Gender and IoT" at https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot .
54 The Freedom Online Coalition, https://freedomonlinecoalition.com/ , is a partnership of 31 governments, working to advance Internet freedom.

- Promoting ethical business practice,[55] in which online businesses behave well and pursue social goals, because they understand that this will be in in the best interests of their shareholders, employees, and customers, and will lead to less intrusive regulatory oversight.
- Giving powers to a regulatory body to incentivize and police responsible behaviour by platforms and social media companies. This is just starting to happen in some advanced economies; because the companies concerned are often global, improvements in one part of the world should more easily be applied elsewhere, adjusted to local circumstances.

Developments of these kinds, especially the last, are new, and doubtless more of them will emerge in coming years.[56]

Digital identity and automated decision-making

Any person may have several valid identities, linked with different aspects of their lives (ITU 2018b). For example, a woman called Meron Kabede may be "mum" to her children, "Meron" to her friends, and "Ms Kabede" to her boss – and with these names go different identities, as perceived by the person and those around her. The same holds in the digital sphere, where it is easy to have as many identities as desired, and harder for a stranger to associate disparate identities with the same person.

The first digital identity acquired by many people, especially in developing countries, is a mobile phone number. In the past, with prepayment a phone number did not identify an individual, but increasingly, anti-crime measures have been leading to registration requirements for prepayment accounts under know-your-customer (KYC) regulations commonly used in the banking sector, so that the phone number links to at least a name, and probably also a date of birth and often an address, which together uniquely identify the registrant. Mobile phone numbers are also used for personal identification by many applications.

Other forms of digital identity include email addresses, social media account IDs, and, increasingly, official documents like driving licences, health care cards, and passports.[57] Official documents naturally include other personal data – such as, for a driving licence, certification of passing a driving test, and records of any driving offences – and being digital makes it easy to link together different pieces of data about a person. Ultimately, these may all be available to government officials through a central digital identity system like the Indian Aadhaar.[58] To date Aadhaar remains a voluntary system, but as it is used for important official purposes (like claiming benefits) the ability to opt out is likely to become theoretical.

Such all-embracing digital identity systems can offer considerable efficiency benefits, but also raise concerns about over-reaching state power leading, for example, to restrictions on the travel or health care of people whose views are unwelcome to the government. Digital identity systems are being developed which are controlled by the individual, and which reveal only such facts about them as are necessary for the purpose in hand. For example, to buy alcoholic drink a

[55] See, for example, Hodges and Steinholtz (2018) for U.K. developments and proposals, and https://bcorporation.net/ for information on an international movement for ethical business.

[56] See Chapter 2 on "Competition and economics", which includes discussion of the regulation of digital platforms.

[57] For more information on the transformational potential of digital identification systems, see the World Bank's ID4D initiative, https://id4d.worldbank.org .

[58] https://uidai.gov.in/my-aadhaar/get-aadhaar.html .

person may have to show their age, to borrow they may have to demonstrate creditworthiness, and to get work, they may need to show residence status.[59]

Automated decision-making is also causing much public interest and concern at present. Systems that inspect applications (for example, for jobs, college places, or loans) use AI techniques to infer the likely performance of applicants, based on comparing their digital identities with those of previous successful applicants.[60] Algorithms trained on historical data are likely to reproduce previous patterns of success, continuing embedded discrimination, unless specific efforts are made to avoid this. In the consumer sphere, personalized recommendations may be appreciated while loss of agency is regretted.[61]

4.4 Key findings

Introduction to digital consumer rights

- Serving the interests of consumers and other users is the primary purpose of markets, and competitive markets are usually the best way to improve services for consumers. However, market forces alone do not always lead to best possible outcomes for all consumers, and regulators have a vital role in recognizing where this happens and intervening as appropriate.
- Research in developing countries shows a convergence between rights expected for consumers and rights expected for citizens, leading to new ideas of digital rights for all people.
- Consumer groups who are least likely to be well served by market forces alone include those with high costs of service – often through remote location or need for specialized equipment to counter a disability – and those whose budgets do not permit desired amounts of use. They, and others who are or become vulnerable, require special attention from regulators.

Consumer support framework

- Regulatory responsibility for digital consumer affairs may be split among different agencies, such as a dedicated consumer affairs regulator, a competition authority, a data protection regulator as well as an ICT regulator. Given its stage and rate of digital transformation, policy-makers should review what regulatory structure for consumer affairs will be best suited to their own country's circumstances.
- ICT regulators need to be familiar with all other agencies that are concerned with digital consumer affairs, and jointly devise ways of working together to ensure that all aspects are properly covered.
- Basic digital consumer protection is often laid down in general consumer protection law. Legislators need to review this law from time to time, and ICT regulators need to ensure that it is complemented by appropriate sector-specific protections, for example, in regulations that service providers must abide by.
- ICT regulators have an important role to play in enforcing such regulations, and may also have similar duties in relation to breaches of general consumer protection law by communications service providers and any other regulated entities.
- Ensuring that consumer complaints are handled fairly, promptly, and effectively is an important part of most ICT regulators' duties. Usually consumers must complain first to

[59] The Identities Project, https://www.identitiesproject.com/ , based on the experience of people in India, is associated with World Bank (2019b). See also Consumers International (2017). The refugee story at https://readymag.com/u82923304/refugee-id-journey/8/ is easy to read and informative.
[60] Discussed more fully in Chapter 7 on "Regulatory response to evolving technologies".
[61] See Consumers International (2019).

their service providers, who are required to respond in accordance with detailed rules. Consumers who remain dissatisfied can then take their complaint further, either to the regulator itself or to an independent alternative dispute resolution agency.

- Whether or not regulators have prime responsibility for handling consumer complaints that are not resolved by companies, these complaints are a valuable source of information for regulators on what is troubling consumers.
- Consumers themselves, and their representatives, are the best people to express consumers' varying needs. Service providers recognize this and will research their markets, but regulators also have a responsibility to facilitate the expression of consumer needs, especially those of vulnerable groups which may not be met by markets.
- ICT regulators can facilitate the expression of digital consumer needs by a variety of actions, including:
    - Supporting the formation and operation of consumer organizations, with well-qualified staff, whose expertise includes digital consumer issues. Organizations may represent consumers generally or just certain groups, such as those with a disability.
    - Initiating and maintaining dialogue with consumer representatives, through both lasting structures (such as consumer panels and forums) and ad hoc informal discussions of specific issues.
    - Encouraging service providers also to engage directly with consumer representatives.
    - Carrying out their own consumer research.

Specific consumer issues

- In these fast-changing markets, periodic reviews are advisable of the protections offered to both prepayment and postpayment customers of communications providers, covering the correctness and transparency of amounts paid, procedures for compensation when errors occur, and consumers' ability to switch operator. Reviews may show up needs for better enforcement of existing regulations, or for new or amended regulations.
- Consumer-friendly price comparisons by regulators are a valuable aid for consumers when choosing their service provider, but keeping them wide-ranging, accurate and up-to-date gets harder as a market expands. Rather than meeting this challenge themselves, some regulators choose to commission or accredit comparisons by external providers.
- ICT regulators and other bodies with responsibilities to support consumers can jointly help consumers to find the advice or support that they need in this increasingly complex arena, perhaps through an online "one stop shop" or telephone helpline.
- Consumers with disabilities may require adapted equipment or services in order to enjoy equitable digital access, and digital options for these people have potential for wider social and economic benefit. Regulators can influence positive developments for people with disabilities through both regulation and encouragement of voluntary initiatives.
- ICT regulators can help to promote consumer trust, by requiring or incentivizing good business practice that demonstrates trustworthiness. They can also help to educate consumers to be on their guard against bad practice, such as sale of their data leading to unwanted targeted advertising.
- ICT regulators should be aware of consumer concerns relating to online safety and use of their personal data, some of which are outlined in this chapter. If, as if often the case, direct responsibility for data protection and privacy regulation is with a different regulator, ICT regulators should work closely with that other regulator to ensure full coverage of all consumer issues.

References

A4AI (Alliance for Affordable Internet). 2016. *Policy Guidelines for Affordable Mobile Data Services*. Research Brief No. 3. https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2016/11/MeasuringImpactsOfMobileDataServices_ResearchBrief3.pdf.

ARCEP (L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2018. *Devices, the Weak Link in Achieving an Open Internet*. Paris: ARCEP. https://en.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf .

Behavioural Insights Team. 2019. *Contractual Terms and Privacy Policies: How to Improve Consumer Understanding*. London: Department for Business, Energy and Industrial Strategy. https://www.gov.uk/government/publications/contractual-terms-and-privacy-policies-how-to-improve-consumer-understanding.

BEREC (Body of European Regulators for Electronic Communications). 2020. *BEREC Strategy 2021-2025*. BoR (20) 43. https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/9039-draft-berec-strategy-2021-2025.

Consumers International. 2017a. *Connecting Voices: A Role for Consumer Rights in Developing Digital Society*. London: Consumers International. https://www.consumersinternational.org/media/154869/ci_connecting-voices_2017_v2.pdf.

Consumers International. 2017b. *Digital ID in Peer to Peer Markets*. London: Consumers International. https://www.consumersinternational.org/media/154884/digital-id-report.pdf.

Consumers International. 2019. *Artificial Intelligence: consumer experiences in new technology*. London: Consumers International. https://www.consumersinternational.org/media/261949/ai-consumerexperiencesinnewtech.pdf.

Cowell, Frank, and Karen Gardiner. 1999. *Welfare Weights*. London: London School of Economics. http://darp.lse.ac.uk/papersDB/Cowell-Gardiner_(OFT).pdf.

Dutta-Powell, Ravi, Zoe Powell, and Nathan Chappell. 2019. *Behavioural Biases in Telecommunications: A Review for the Commerce Commission*. Wellington, New Zealand: Behavioural Insights Team. https://comcom.govt.nz/__data/assets/pdf_file/0026/146681/BIT-Behavioural-biases-in-telecommunications-13-May-2019.PDF.

Evans, Phil. 2003. *The Consumer Guide to Competition: A Practical Handbook*. London: Consumers International. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/34850/126821.pdf.

Hodges, Christopher and Ruth Steinholtz. 2018. *Ethical Business Practice and Regulation*. London: Bloomsbury. https://www.bloomsbury.com/au/ethical-business-practice-and-regulation-9781509916375/.

Hogg, Tim. 2020. "Framing Fairness". *InterMEDIA* 48 (1): 29-31. https://www.iicom.org/wp-content/uploads/IM-April-2020-Vol-48-Issue-1_Hogg.pdf.

ITU. 2014. *Best Practice Guidelines on Consumer Protection in a Digital World*. Geneva: ITU. https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/BestPractices/GSR14_BPG_en.pdf.

ITU. 2016. *Digital Financial Services: Regulating for Financial Inclusion: An ICT Perspective*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT02-2016-PDF-E.pdf.

ITU. 2017a. *The App Economy in Africa: Economic Benefits and Regulatory Directions*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.APP_ECO_AFRICA-2017-PDF-E.pdf.

ITU. 2017b. *Final Report on ITU-D SG1 Question 6/1: Consumer Information, Protection and Rights: Laws, Regulation, Economic Bases, Consumer Networks*. Geneva: ITU. https://www.itu.int/pub/publications.aspx?lang=en&parent=D-STG-SG01.06.3-2017.

ITU. 2018a. *Global ICT Regulatory Outlook: Regulatory Collaboration: "Power Coupling"*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2018-PDF-E.pdf.

ITU. 2018b. *Digital Identity in the ICT Ecosystem: An Overview*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.ID01-2018-PDF-E.pdf.

ITU. 2018c. *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.

Lunn, Peter. 2014. Regulatory Policy and Behavioural Economics. Paris: OECD. https://www.oecd-ilibrary.org/governance/regulatory-policy-and-behavioural-economics_9789264207851-en.

Lunn, Peter, and Sean Lyons. 2018. "Consumer Switching Intentions for Telecoms Services: Evidence from Ireland". Heliyon 4(5). https://doi.org/10.1016/j.heliyon.2018.e00618.

Milne, Claire. 2016. "Nuisance Calls and Texts: What Can Be Done?". Presentation for MIIT/ITU meeting in Chongqing, China. http://public.antelopeweb.fmail.co.uk/publications/what%20can%20be%20done%20about%20nuisance%20calls%20and%20texts.pdf.

OECD.2019a. The Effects of Zero Rating. Paris: OECD. https://www.oecd-ilibrary.org/docserver/6eefc666-en.pdf.

OECD. 2019b. *Understanding Online Consumer Ratings and Reviews*. Paris: OECD. https://www.oecd-ilibrary.org/docserver/eb018587-en.pdf.

Ofcom. 2019. *Access and Inclusion in 2018: Consumers' Experiences in Communications Markets*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/132912/Access-and-Inclusion-report-2018.pdf.

Ofcom. 2020. *Making Communications Markets Work Well for Customers: A Framework for Assessing Fairness in Broadband, Mobile, Home Phone and Pay TV*. Policy Statement, January 23. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0033/189960/statement-fairness-framework.pdf.

Russell, Graham, and Christopher Hodges. 2020. *Regulatory Delivery*. London: Bloomsbury https://www.bloomsburyprofessional.com/uk/regulatory-delivery-9781509918584/.

TRAI. 2018. *Consumer Handbook on Telecommunications*. New Delhi. https://trai.gov.in/sites/default/files/TRAI_Handbook_2018_Eng.pdf.

UKRN (U.K. Regulators Network). 2020. *Driving Fair Outcomes for Vulnerable Consumers across UK Markets.* Event Report. London: UKRN. https://www.ukrn.org.uk/wp-content/uploads/2020/03/Driving-Fair-Outcomes-for-Vulnerable-Consumers-Report.pdf.

UNCTAD (United Nations Conference on Trade and Development). 2016. *United Nations Guidelines for Consumer Protection*. Geneva: UNCTAD. https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf.

Which? 2018. *Control, Alt or Delete: Consumer Research on Attitudes to Data Collection and Use*. London: Consumers' Association. https://www.which.co.uk/policy/digitisation/2707/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use.

World Bank. 2019a. *Information and Communications for Development 2018: Data-Driven Development*. Washington, DC: World Bank. https://elibrary.worldbank.org/doi/book/10.1596/978-1-4648-1325-2?chapterTab=true.

World Bank. 2019b. *Principles on Identification for Sustainable Development: Toward the Digital Age.* Washington, DC: World Bank. http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

Chapter 5. Data protection and trust

5.1 Introduction

Data are sometimes described as the "oil of the digital economy"[1] while their use in the digital economy is sometimes referred to as "surveillance capitalism."[2] While the former has relatively benign connotations, the latter directly provokes concerns about the use of personal data.[3] This chapter focuses on regulatory aspects of data with an emphasis on personal data.

The digital transformation process has necessarily focused attention on the adequacy of, and need for, legal and regulatory frameworks that govern information products, services, and platforms. Intellectual property laws, especially copyright, have had to be revised to reflect the increasing value of intangible assets. Criminal laws and procedures have needed to be amended to address cybercrime; deterring new forms of harmful conduct and enabling effective investigations. Likewise, as personal data has become an increasingly valuable strategic commercial asset, so there has been a demand for rules that protect such data and give individuals the ability to control the collection, processing, use and abuse of their data. Having a data protection regime in place is widely recognized as a key factor in facilitating digital transformation (African Union 2020). Control is seen as critical in terms of engendering trust in data subjects about operating in an online environment, whether as citizens, consumers, or friends, which itself encourages take-up, participation, and consumption (ITU 2018).

1 The comparison of data (an infinite and non-rivalrous thing) to oil (a finite and rivalrous resource) is probably erroneous.

2 "Surveillance capitalism" was coined by Shoshana Zuboff (Zuboff 2019).

3 This chapter refers to data protection, not privacy. While these concepts are linked, they are not synonymous. See, for example, World Bank 2021 (forthcoming). Sometimes used interchangeably, and sometimes referred to in mixed fashion ("privacy and data protection," or "data privacy") a distinction is drawn here to firmly place data protection in regulatory context.

This chapter examines the nature of data protection regimes, focusing particularly on its regulatory aspects – a feature that results in interesting similarities with the telecommunication sector. It examines the extent to which emerging technology and services should, and could, be impacted, as well as the controls over the cross-border flow of personal data and the resultant trade implications. Data protection and privacy concerns particularly overlap when considering the need for special rules to govern our communication activities. The complex intersection between data protection and information security is also examined. Finally, some key considerations for regulators are offered.

5.2 Data protection regimes

While data protection is clearly related to and overlaps with the right to privacy, it also contains some unique characteristics that distinguish it from traditional notions of privacy law. First, data protection is firmly embedded in the digital economy, the processing of data in its many forms by information and communications technologies (ICTs), hence its relevance to this handbook. Privacy laws, meanwhile, extend into areas of our lives that may be far removed from technology. Second, data protection regimes are generally applicable to all data relating to a person, referred to as "personal data," whether that data can be said to be of a private or public nature. So, what a person posts on their Facebook page is as deserving of protection under the regime as that which is held in a password-protected file, even if not to the same level. Third, personal data can generally only be processed on some legitimate ground, such as consent, which places the onus on the person possessing the personal data to justify having control over it; whereas traditional privacy law has focused on controlling instances where a person's private life is interfered with, resulting in a harm, whether pecuniary or non-pecuniary. Fourth, there is generally a need for a supervisory authority to "control" compliance with data protection rules. It is this feature that establishes data protection as a regulatory regime, a regime that goes way beyond our traditional notion of a privacy right.

Data protection as a regulatory concept first appeared in the Council of Europe's 1981 Convention on data protection (commonly known as Convention 108).[4] While based in the right to privacy in Article 8 of the European Convention on Human Rights (ECHR), it was exclusively concerned with the "automatic processing of personal data." The focus shifted to the European Union (EU) in 1995 with the adoption of the Data Protection Directive.[5] This quickly became the leading instrument against which most other laws and initiatives were measured. In May 2018, the Directive was replaced by the General Data Protection Regulation (GDPR) and is generally recognized as being the leading measure in the field.

While data protection emerged in Europe, data protection regimes have since been adopted widely around the world, with nearly 140 countries having some form of legal regime (Greenleaf 2020), as well as numerous other regional instruments, including the Asia-Pacific Economic Cooperation Privacy Framework[6] and the African Union Convention on Cyber Security and

[4] The Council of Europe is a 47 Member State intergovernmental body responsible for the *European Convention on Human Rights* (ECHR) and the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Strasbourg, January 28, 1981 (Convention 108). Convention 108 has been recently updated to align it with the GDPR, and is available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

[5] Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data," OJ L 281/31, 23.11.1995.

[6] First adopted in 2005, it was revised in 2015.

Personal Data Protection (2014).[7] However, despite such a multitude of instruments and laws, as noted by the International Telecommunication Union (ITU), there is "a trend towards adoption of laws along the 'European' lines."[8] China is perhaps the most recent country to introduce draft legislation regarding data protection.[9]

While these various legal instruments differ considerably in scope and detail, the majority of data protection regimes are based around a common set of "data protection principles" to which regulatees are expected to comply when processing personal data. Broadly, these principles can be further subdivided in two categories:

- Principles focusing on the quality of personal information and information systems, such as the need to ensure accurate data and secure systems,
- Principles applicable to those whose data is being processed, such as fairness and transparency. (Bygrave 2002)

Similar to telecommunications, the regulatory nature of data protection arises both from the nature of the obligations imposed upon regulatees and the role of the supervisory authority in exercising powers of oversight and enforcement against non-compliant regulatees. Each national authority (and some at a regional level) will be issuing various forms of opinion, guidance, and recommendations that, although not generally mandatory, comprises part of the regulatory framework for regulatees. In addition, there are numerous industry self-regulatory initiatives, such as codes of conduct, often at a sectoral level, which elaborate and supplement the legal rules.

Finally, data protection issues have been incorporated into standards, such as those of the International Organization for Standardization (ISO),[10] which can also come to form part of the regulatory regime, whether through express incorporation or becoming *de facto* best practice. Related to data protection codes of conduct and standards has been the emergence of certification regimes that enable organizations to obtain external review and verification that their practices and procedures meet the requisite standards, and publicize such compliance through the use of seals, marks, or labels.[11]

Together this spectrum of measures, from "hard" and "soft" law, comprises a data protection regulatory regime. In terms of regulatees, attention is focused on the "controller," either acting alone or jointly with others, as the person that determines the purpose and the means of the processing. In most laws, there is a second category of regulatee, the "processor," who processes the personal data on behalf of the controller. The direct statutory obligations placed upon on a processor are generally less onerous than those imposed on the controller, such as compliance with the principles, although there is often a requirement for a contract governing the relationship between the controller and processor, which may redistribute the responsibilities of the respective parties. Determining the role of a person, as controller and/or processor, and therefore their respective regulatory obligations, can itself be a difficult and

7 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

8 Fn. 1, at p. 35.

9 China published for consultation a draft law on Personal Data Protection that in many respects mirrors provisions of the GDPR. See, e.g., https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.

10 ISO, 27018: 2014 "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors."

11 For example, Truste Privacy Program Standards, see https://trustarc.com/consumer-info/privacy-certification-standards/.

contentious issue. This is especially pertinent given the increasing complexity of digital supply chains and markets, such as in the Internet of Things (IoT), which blends products, services, and software.

5.3 Regulatory authorities

As noted already, one pillar that distinguishes data protection as a regulatory regime rather than simply a statutory framework is the establishment of an authority or appointment of a commissioner to oversee compliance and enforce against infringers. Indeed, under the Charter of Fundamental Rights of the European Union, the need for an authority is enshrined within the right itself: "Compliance with these rules shall be subject to control by an independent authority" (Art. 8(3). While some international instruments did not initially acknowledge the need for an authority, such a requirement has been inserted into subsequent revisions.[12]

Data protection regimes must therefore be distinguished into their substantive and procedural components. The former comprises the obligations imposed on regulatees and rights granted to individual data subjects, while the latter concerns the nature and powers of the authority. When comparing national regimes, both components should be considered of equal importance and, indeed, may have regulatory consequences. Under EU law, for example, when the European Commission assesses whether a third country ensures "an adequate level of protection" to enable the transfer of personal data, the suitability of the procedural elements is a critical part of the analysis.[13]

In terms of nature and powers, there are clear parallels between national telecommunication and data protection authorities. The authority should be independent from regulatees, which will generally include the government and public bodies. While an incumbent operator may or may not be owned, in whole or part, by the government, the government will certainly be a major collector and processor of personal data. However, in many countries, data protection laws are either limited in application to the private sector or, where public bodies are included, the public sector is subject to exceptions not available to private sector controllers. Achieving effective independence for regulatory authorities can be problematic, with the need for adequate financial resources, capacity, and expertise to be ensured. In terms of powers, data protection authorities will generally be granted both *ex-ante* powers to intervene, such as authorizing certain activities, as well as *ex-post* investigative powers, such a right to request the disclosure of information. As a public body itself, the appropriate exercise of these powers by the authority enters the realm of administrative law, with concerns that decision-making and other types of conduct are carried out properly.

The role and importance of a data protection authority can create issues for countries, especially where the notion and experience of independent regulation is less well established. However, a lack of an effective and independent regulator may be viewed by data protection regulators in other countries as a reason to prohibit or restrict the transfer of personal data into that country, to protect data subjects. To address this issue, there may be an argument for considering expanding the mandate of an existing national regulator, such as the telecommunications or ICT authority or consumer authority, to cover data protection issues rather than establishing

[12] For example, Council of Europe Additional Protocol to the Convention (2001), OECD (2013), and APEC (2015).
[13] Article 29 Working Party, *Adequacy Referential (updated)*, WP 254, November 2017.

a completely new body with the attendant issues of resourcing and building a culture of independence.

Box 5.1. The Global Privacy Assembly

The Global Privacy Assembly (GPA) is an international entity which brings together more than 130 data protection and privacy authorities, as well as observers from various international organizations and NGOs. It first met as an international conference in 1979. The GPA adopts ad hoc resolutions and communiques, including a recent call for increased co-operation between data protection, consumer protection and competition authorities. The GPA also operates a number of working groups, including one on International Enforcement Cooperation, which includes a consideration of legal solutions. As a forum for collaboration, co-operation and the sharing experiences and know-how, the GPA can provide support to national data protection authorities in less developed countries.

Source: https://globalprivacyassembly.org.

5.4 Technologies and services

As noted earlier, one distinction between data protection and privacy is that the former is solely concerned with personal data processed by IT systems. To that extent, it cannot be said that data protection law is technology neutral, since it was computerization that gave rise to the concern for personal data in the 1960s and 1970s, and current regulatory frameworks are primarily focused on such processing activities. Processing is generally given a broad legislative definition to encompass the whole processing lifecycle from data collection to its eventual deletion or, in the alternative, anonymization, which would prevent it from any longer identifying individual data subjects. Such a broad scope does extend the application of data protection regimes into the physical sphere; for example, governing the manual collection of data intended for subsequent processing.

At the same time, however, the data protection principles that form the core of national and international data protection regimes have been developed precisely to avoid being too prescriptive with respect to particular types of technologies and services, which are evolving rapidly. Principles-based regulation is designed to help avoid rules and regulations becoming technologically redundant, or worse, inhibiting innovation.

Although "technology neutral," compliance with the data protection principles can directly impact the development of particular technologies and services by controllers, as well as indirectly those upstream in the supply chain, producing components and applications that form part of the deployed technologies and services. The data minimization principle, in particular, should be reflected in the design of applications and systems.

Box 5.2. Case study: COVID-19 tracing apps

Since the start of the COVID-19 pandemic, one of the biggest challenges has been to track people who develop symptoms and anyone who they have been in close contact with during the virus' incubation period to prevent them infecting other people. To help achieve this, various "contact tracing" applications have been developed for people to use on their mobile phones. Such applications can differ between the collection of data on a decentralized or centralized basis, as well as the types of data collected, such as location or proximity data. Such design decisions result in trade-offs between the rights users may have over their data and countervailing public health considerations:

- A system developed by Apple and Google is based on the DP-3T Bluetooth decentralized protocol, meaning that all processing and storing of data takes place on a user's device. The data stored is stored on the device only for 14 days and the system does not allow for location data to be collected.
- Some governments have developed systems using a centralized model, which enables medical professionals to obtain access to more data, which could help them better trace people, as well as providing data for ongoing research into the virus and its public health implications.

International and national laws recognize that in extraordinary circumstances, certain fundamental rights, including the right to data protection, may be restricted, on the condition that basic democratic principles and safeguards are ensured, and the restriction is legitimate, time limited, and not arbitrary.[1]

[1] See, World Bank 2021 (forthcoming), Spotlight 6.1.

While the data protection principles are applicable to all technologies and services, that does not preclude jurisdictions from determining that particular technological or market developments deserve additional rules to address manifest public concerns and public interest objectives.[14] Two key examples are the emergence of artificial intelligence (AI) and social media.

AI enables machines to identify patterns in big data sets and to build representative models that can be used in automated decision-making – from purchasing recommendations for consumers and diagnosing medical conditions, to sentencing decisions in respect of criminals. Such automated decision-making can obviously have real world impacts on individuals that may not always be welcome or deserving. Data protection laws have addressed two aspects of such automated decision-making: fair and transparent processing, and the ability to demand a review of the decision. In terms of the former, a data subject is seen as needing to be informed of three things: (a) the existence of the automated decision-making process; (b) how was the

[14] For example, Mexico, Article 52 "Processing of Personal Data in Cloud Computing," in Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (2011).

decision reached, i.e. meaningful information about the logic embodied in the algorithm that determines the result; and (c) what consequences flow from the processing for the data subject. Such transparency is designed to enable a data subject to exercise effective control over the use of their data. With regard to review, data subjects may be given the right, in certain circumstances, to have a person intervene in the decision-making process, often referred to as a "human in the loop" (Wang 2019). This reflects a widely held concern that we should be able to appeal against a decision made by a machine to a human, although whether this makes for better decision-making is debateable.

Social media companies, such as Facebook and Weibo, are prime examples of the phenomenon that has been termed "surveillance capitalism." Data subjects obtain a service for free in exchange for enabling the providers to exploit their personal data by selling it to advertisers, a two-sided market. One concern with social media is the possibility that consumers may get "locked-in" to the provider they use, because of difficulties with moving the content they have posted to an alternative provider. To address this concern, some data protection regimes have given individuals a right of data portability, which can include the right to demand that their data be transmitted directly from their incumbent provider to their chosen alternative.[15] This can be seen as analogous to number portability obligations in the telecommunications sector, which enables customers to change providers rapidly, cheaply, and easily without having to change their numbers.[16] By reducing the switching costs involved in moving providers, dependency becomes less likely. Although achieved through data protection law, such user empowerment can also be seen as a demand-side competition measure, as well as a component of consumer protection regimes.[17]

Other innovative and disruptive technologies can generate data protection concerns that, while not addressed through specific regulatory measures, may require regulators to give specific attention to how they can be used in a data protection compliant manner. Blockchain, for example, when deployed using a distributed architecture, creates concerns about the roles of the respective parties and the ability of data subjects to exercise their rights.[18]

It is often noted that law tends to lag behind technologies, which is an inevitable result of the different environments under which each operates. Data protection authorities can try to reduce this gap through soft law guidance and recommendations, based on applying the data protection principles to novel processing situations. Such regulatory intervention can ensure that the rights and interests of data subjects are given appropriate consideration, while innovation is not unduly constrained by inflexible rules.

5.5 Transfers and trade implications

The digital economy is inherently transnational in nature, with the possibility of data being transmitted across borders in accordance with efficient network design and resource allocation parameters that are often opaque to users. The global nature of networks also provides economic opportunities for those capable of processing data in one country to get access to

15 GDPR, Art. 20.

16 In the EU, see Directive 2002/22/EC "on universal service and users' rights relating to electronic communications networks and services' (OJ L108/51, 24.2.2002), at Art. 30. From December 2020, Art. 106 of the European Electronic Communications Code (Directive (EU) 2018/1972, OJ L 17.12.2018) will be the applicable provision.

17 For more details, see Chapter 4 on "Consumer affairs."

18 For example, see CNIL 2018.

markets in other countries. From a data protection perspective, however, such transborder data flows represent an avenue for potential erosion of the protections granted to data subjects under national law. As such, data protection regimes will generally include rules governing the flow of personal data out of the jurisdiction.

Cross-border data transfer controls can take a variety of forms, but are generally based on establishing or achieving some threshold standard of protection between the two jurisdictions, which provides a gateway through which the data transfers are governed. The standard to be met to facilitate cross-border data flows may be expressed in differing terms, such as "equivalent," "adequate," "appropriate," "comparable," "sufficient," and may achieved through different mechanisms:

- **International agreement**: Countries may enter into bilateral or multilateral agreements to govern data flows in general,[19] specific categories of personal data or for specific purposes (e.g. law enforcement).
- **Jurisdictional determination**: a country may reach a determination that a foreign country's legal framework is adequate, whether in general or at a sectoral level, and therefore no further restrictions are required.[20]
- **National licensing/authorization regime**: The national regulatory authority may licence or authorize transfers on either an individual or class basis.
- **Private law mechanisms**: Private entities may be able to enter into binding and enforceable legal agreements, such as contracts, that govern the handling of data when transferred between jurisdictions.

Most regimes also provide for derogations or exceptions from these control mechanisms under certain circumstances, such as when the transfer is infrequent or involves only a limited number of data subjects.

Achieving interoperability between differing data protection laws remains an ongoing challenge in our global economy, with different cultures and regimes assigning differing priorities to competing public interests, of which data protection is but one. Indeed, the ability to send and receive information across borders engages the rights of individuals as much as that of data protection and privacy.

The nature of such controls over the cross-border flows of personal data can obviously have trade implications. Under the World Trade Organization's (WTO) General Agreement on Trade in Services (GATS), member states that commit to liberalizing a service sector, such as telecommunications or "information supply services,"[21] may continue to rely on an exception where it concerns the "[p]rotection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individuals."[22] This provision can legitimize countries imposing data localization rules under the auspices of data protection on the processing of all or certain categories of personal data, such as health or financial data. Such controls may either prohibit the processing of personal data outside the territory or restricting such flows and impose conditions, such as data residency that require copies of the personal data to be maintained within the originating jurisdiction. However, in terms of scope and application, data protection laws should operate in a manner that restricts

19 For example, the APEC Cross-Border Privacy Rules (CBPR) system, whereby companies can be certified.
20 For example, the EU's GDPR, Art. 45; e.g. Commission Implementing Decision (EU) 2019/419, January 2019 with respect to Japan.
21 CPC Ver.2.1 (2015), Sec. 8, Div. 84: "information supply services."
22 GATS, Art. XIV(c)(ii).

international trade only to the extent necessary and proportionate to safeguard the interests of individuals, rather than be used as a tool for disguising non-tariff trade barriers.

Data protection laws have become an increasingly important part of international trade policy and negotiations. Given the multistakeholder and societal interests involved, greater compatibility and interoperability between national data protection regimes will not only serve to protect the interests of data subjects, but reduce the compliance costs for business, especially SMEs, and facilitate international trade and investment (UNCTAD 2016).

5.6 Communications privacy

Telecommunications law comprises sectoral rules, while data protection rules tend to be horizontally applicable across industry sectors. As such, these rules may overlap in certain areas, such as security. Indeed, in some countries, telecommunications law may be the only source of data protection rules or may contain additional specific data protection rules for industry players.

In the EU, when the Data Protection Directive was first proposed it was supplemented by a sectoral measure applicable to privacy and electronic communication.[23] The measure refers to privacy rather than data protection in recognition that our communication activities are traditional viewed as part of the fundamental right to privacy.[24] The provisions can be further divided into four distinct privacy relationships that exist within a communications environment.

First, that between the service provider and the subscriber or user. In providing communication services, an operator is obviously in a potentially privileged position concerning the handling of user data, both in terms of communications content and associated communications data, the "who," "when," "where" and "how" of a communication. Telecommunications law often expressly makes it unlawful for employees within operators to exploit this position, whether for commercial purposes or otherwise.[25] With digital transformation, communications-generated data has grown in value and volume exponentially. As a consequence, some jurisdictions have adopted sectoral rules restricting the ability of operators to process users' personal data except for limited purposes, such as end-user billing and interconnection payments, or subject to restrictive conditions, such as consent-based only. One area of ongoing controversy in the telecommunication sector is that the current regulatory playing field is not level, since in some jurisdictions traditional telecommunication operators are subject to strict controls over their use of personal data, while providers of over-the-top (OTT) communication services, such as Skype and Gmail, are not subject to such controls and are therefore free to monetize their customers' data. There have been calls to harmonize the approach and remove this regulatory asymmetry, with the EU proposing to move in the direction of imposing restrictions on all providers of communications services.[26]

---

23 The initial measure was adopted in 1997, but subsequently amended and replaced by Directive 02/58/EC of the European Parliament and of the Council concerning "the processing of personal data and the protection of privacy in the electronic communications sector." OJ L 201/37, 31.7.2002 (ePrivacy Directive).

24 For example, the Universal Declaration of Human Rights (1948), Article 12, states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

25 For example, The Kenya Information and Communications Act, Chapter 411A, s. 30, "Modification etc., of messages," and s. 31, "Interception and disclosure."

26 Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications, COM(2017) 10 final, 10.1.2017.

A second privacy relationship is that between a subscriber to a communication service and the user of that service. An example where this scenario may give rise to concerns is that between an employer and employees, since the former may want to monitor and record the communications of employees or other system users, such as customers contacting a call centre, while those users may have a legitimate expectation that they can make private calls or be notified when such monitoring occurs. To protect the privacy of users, therefore, the law may require that itemized bills sent to subscribers will not record calls that do not incur a charge, such as a toll-free number.

A third privacy relationship is that between the two parties to a communication, traditionally referred to as the calling party and called party. Rules governing the use of calling line identification (CLI) and prohibiting unsolicited messaging are examples of measures designed to protect the privacy of the recipient from the communications of the sender, although the latter may also be designed to safeguard the network from harmful practices.[27] It is the desire to regulate this privacy relationship that has resulted in the proliferation of so-called "cookie" banners, so prevalent in our online environment, which are designed to ensure that users are informed (and give their consent) when a website with whom the user interacts tries to place a "cookie" on the user's device, whether for their own or a third-party purposes.

The final privacy relationship is that between the user and the state. Controls are imposed over the circumstances and conditions under which the state can engage in communications surveillance for law enforcement purposes; primarily the interception of communications and the acquisition of communications data, although also extending to data retention requirements imposed on operators.[28] The user-state relationship is a fundamental privacy concern and the reason that "correspondence" has always been an element of the standard constitutional right to privacy.[29]

Whether and how each of these privacy relationships are governed will vary between states, sometimes being addressed as part of the general data protection regime, sectorally within the telecommunications framework, under employment law, as an element of consumer protection law[30] and/or criminal procedure.

5.7 Data protection and information security

If viewed as a Venn diagram, data protection, privacy and information security would be drawn as three distinct but overlapping sets. One widely recognized fundamental data protection principle is the need to implement "appropriate" technical and organizational security measures when processing personal data, to protect against both accidental and deliberate conduct resulting in the loss, alteration, disclosure, or destruction of the data. What constitutes "appropriate" security will vary depending on the nature of the personal data being processed, with "sensitive" personal data requiring greater protection. What constitutes "sensitive" personal data may be specified in the legislation, e.g. health and financial data, but should also reflect the nature of the processing activity, as the harmful consequences of, for example, an unintended loss or disclosure of personal data will vary according to the specific context. The nature of

[27] See ITU, International Telecommunications Regulations (Dubai, 2012), at Article 7, "Unsolicited bulk electronic communications."
[28] For example, Russia, Federal Law 374-FZ, 2016, requires providers to store content and communications data for six months.
[29] United Nations Resolution 68/167: "The right to privacy in the digital age," December 18, 2018.
[30] For more details, see Chapter 4 on "Consumer affairs."

the security measures taken will also need to be reviewed and evolve over time to reflect both technological developments and the attendant risks and threats posed. It should also be noted that security obligations should not be viewed as binary in the sense that any breach results in infringement and potential liability, since a regulator may find that all the "appropriate" measures were taken by the controller as regulatee, but a breach still occurred.

The relationship between data protection and information security is primarily viewed as complementary in nature. Information security laws and requirements tend to impose both safeguarding and transparency obligations on systems operators:

- Safeguarding obligations, which require the implementation of appropriate security measures, especially by those entities operating or supplying services to critical national infrastructure; and,
- Transparency obligations, which generally take the form of security breach notification requirements, whether to the relevant authority and/or the individual data subject, where they are likely to suffer harm and can take steps to mitigate.

Data protection laws will often impose similar obligations on controllers and processors. While such complementarity is positive, it is important that the standards the respective regimes impose, such as time limits for breach reporting, are harmonized in a manner that does not generate legal uncertainties and additional compliance burdens for regulatees.

Box 5.3. The cost of data breaches

In January 2019, the Marriott hotel group reported that hackers had accessed the accounts of some 339 million guests from the reservation database system of its Starwood division, which it had acquired in 2016. The stolen data included names, addresses, phone numbers, email addresses, credit card details, passport numbers, and travel details. However, of the 25 million passport details, 20 million were encrypted, so the Marriott expected them to remain protected. In terms of costs, Marriott is expected to have to pay out some $500 million to its affected customers, especially those who subsequently became victims of fraud. The breach was investigated by the United Kingdom's data protection authority, the Information Commissioner's Office, who imposed a fine of £99 million in relation to the seven million guests that were U.K. residents.

Security and safety concerns may also come into conflict with data protection laws. Access to, or the sharing of, information may be seen as a necessary measure to protect the security of a community from harm, which may run counter to data protection practices that focus on the rights of the individual. Two key areas that are generating policy debates in many countries are online safety and the current COVID-19 pandemic.

Online safety: The dark side of the Internet as an environment is that it can facilitate illegal and harmful conduct; from hacking systems to exposing children to obscene material and "fake" news. Enforcement against *illegal* conduct in cyberspace is fraught with difficulties, because of the ephemeral nature of online activities, the technological complexities, and its cross-border nature (see, generally, Walden 2016). Acting against *harmful* (but legal) conduct generates even greater problems for policy-makers, legislators, and regulators. While it is broadly recognized that effective action requires input by both public- and private-sector actors, including service providers, determining what the respective roles and responsibilities should be is highly and fiercely debated in many countries. One element of that debate concerns the extent to which personal data should be used to investigate, prevent, and detect illegal and harmful conduct. Online anonymity, provided by virtual private networks (VPN)s and end-to-end encryption, will equally protect the political dissident or public interest whistle-blower, as shield the child sexual abuse predator or terrorist.

COVID-19: As noted in Box 5.2, the pandemic has generated tensions between the need to safeguard the health of the community and limit the use and abuse of personal data. The data collected from individuals may not only stem the current spread of the disease, but its aggregation and analysis over time may further understanding of the virus that can enable public authorities to better handle future such public health emergencies. Countries are having to make determinations on a range of things that have direct implications for data subjects and their personal data: the types of data that can be collected from the individual (e.g. location data); whether disclosure is mandatory or voluntary; whether the collected data can be aggregated with other data held on the individual (e.g. national ID); the range of purposes for which the data can be used (e.g. care and management or research) and the length of time the data is retained.

A key area of debate in the data protection field is the use of techniques to pseudonymize or anonymize personal data using techniques such as encryption. With regard to the former, while pseudonymization can safeguard personal data, it remains subject to data protection regulation, since the process can be reversed and the data reidentified. Conversely, effective anonymization should take the data outside of the data protection regime, since it is no longer personal data. The debate revolves around whether certain anonymization techniques are truly effective in preventing a person from reidentifying individuals, given sufficient motivation, technical capability, and being able to correlate the data against other data sets (Ohm 2010). Both pseudonymization and anonymization techniques are tools of effective information security, but may also be seen as potential "weapons," having both a civilian and military application, as well as rendering the Internet "dark" and inhibiting legitimate law enforcement investigations. Balancing these multiple and conflicting interests presents challenging policy choices for governments and legislators.

References

African Union. 2020. *The Digital Transformation Strategy for Africa (2020-2030)*. Addis Ababa: African Union. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

CNIL (Commission Nationale Informatique & Libertés). 2018. *Blockchain: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*. Paris: CNIL> https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

Greenleaf, G., and B. Cottier. 2020. "2020 Ends a Decade of 62 New Data Privacy Laws." *Privacy Laws and Business International Report* 163 (February): 24-26.

ITU (International Telecommunication Union). 2018. *Regulatory Challenges and Opportunities in the New ICT Ecosystem*. Geneva: ITU. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT03-2018-PDF-E.pdf.

Ohm, P. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* (57) 6: 1701-1777. https://www.uclalawreview.org/pdf/57-6-3.pdf.

UNCTAD (United Nations Conference on Trade and Development). 2016. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. New York and Geneva: UNCTAD. https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

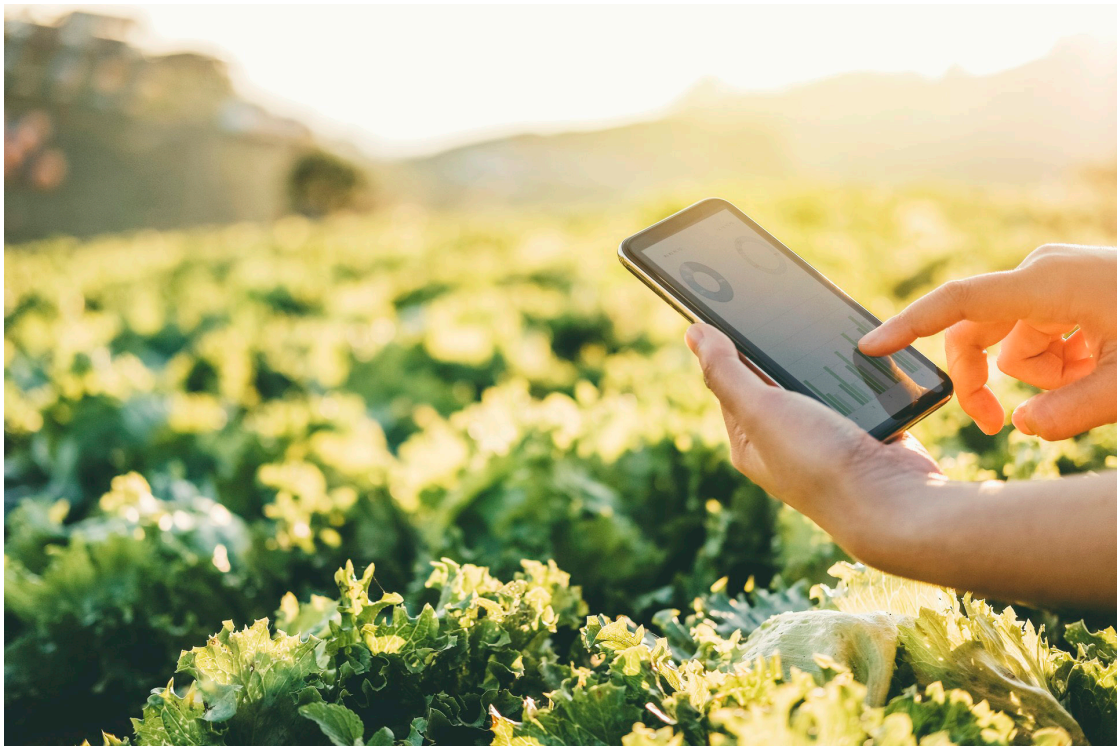
Walden, I. 2016. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press.

Wang, G.E. 2019. "Humans in the Loop: The Design of Interactive AI Systems." *Human-centred Artificial Intelligence Blog*, October 20, 2019. https://hai.stanford.edu/blog/humans-loop-design-interactive-ai-systems.

World Bank. 2021 (forthcoming). *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. New York: Public Affairs.

Chapter 6. Spectrum management



6.1 Introduction

In today's increasingly digital society, access to spectrum and adequate spectrum management processes are key to expanding the deployment, coverage, and reach of telecommunication networks providing great opportunities for socioeconomic development. Increased demand for these networks to support a variety of online applications across sectors of the economy, such as health, transportation, education, agriculture, employment, government, and financial services, requires that spectrum be used efficiently and that effective spectrum management processes be implemented.

Prepared by the Radiocommunication Bureau of the International Telecommunication Union, Part 1 of this chapter provides overall guidance on the regulatory framework for national spectrum management starting by setting the international context and processes. It is excerpted from Report ITU-R SM.2093-3, *Guidance on the Regulatory Framework for National Spectrum Management*, and is reprinted here with the permission of the ITU.

Part 2 discusses key applications and regulatory considerations driving the future use of spectrum, highlighting some of the main points that regulators are invited to consider at the national level, based on the relevant experience of different country examples. It presents some of the mechanisms for spectrum allocation and licensing of new spectrum, with due consideration to the evolution of technology. It also looks at promoting the use of spectrum for these key applications, as well as business models that can strengthen existing and new approaches for the deployment of wireless broadband.

6.2 Part 1. Guidance on the regulatory framework for national spectrum management

Society's increasing use of radio-based technologies, and the tremendous opportunities for socio-economic development that these technologies provide, highlight the importance of radio-frequency spectrum and national spectrum management processes. Technological progress has continually opened doors to a variety of new spectrum applications that have spurred greater interest in, and demand for, the limited spectrum resource. Increased demand requires that spectrum be used efficiently and that effective spectrum management processes be implemented.

Spectrum management is the combination of administrative and technical procedures necessary to ensure the efficient utilization of the radio-frequency spectrum by all radiocommunication services defined in the ITU Radio Regulations and the operation of radio systems, without causing harmful interference.

The role of the International Telecommunication Union Radiocommunication Sector (ITU-R) in international spectrum management is to ensure the rational, equitable, efficient, and economical use of the radio-frequency spectrum by all radiocommunication services, including satellite services, and carry out studies without limit of frequency range on the basis of which ITU-R Recommendations and Reports are adopted.

The regulatory and policy functions of the ITU-R are performed by World and Regional Radiocommunication Conferences and Radiocommunication Assemblies supported by Study Groups.

This chapter provides guidance on the regulatory framework for national spectrum management.[1]

The international context

The telecommunication sector, including radiocommunications, is organized internationally within the framework of the International Telecommunication Union (ITU), which provides the basic framework for the global coordination and management of the radio-frequency spectrum. In between ITU and the national administrations, two other kinds of organizations, regional organizations and specialized international organizations, are also involved in spectrum management, at either regional or global level.

At the regional level, organizations have been founded that bring together administrations, in some cases associating industry or radiocommunication operators. Their aim is to establish common positions in preparation for ITU decisions, to harmonize national frequency allocations within the relatively flexible framework set by ITU so as to facilitate the coordinated introduction of new services, and to harmonize the standards and procedures for certification of equipment with a view to its free circulation and use in the countries concerned.

At the global and regional levels, specialized international organizations also exist in sectors of activity that use radiocommunications and are therefore dependent on spectrum availability:

[1] Part 1 of this chapter is excerpted from ITU (2018b). This report is one of a series of publications on spectrum management developed in the ITU-R. The list of references at the end of this chapter comprises a sample of other relevant ITU publications on spectrum management.

civil aviation, the maritime sector, meteorology, broadcasting, radio amateurs, radio astronomy and research.

The World Trade Organization, within the framework of the General Agreement on Trade in Services (GATS), while recognizing the sovereign right of States to manage the frequency spectrum in terms of their own objectives, works to develop the instruments required so that exercise of that right does not in fact result in barriers to trade in services between its members.

International principles governing spectrum use

ITU international agreements recognize that utilization of the radio-frequency spectrum is a matter of State sovereignty, but that to be efficient it must be regulated. They are the basic global instruments with which, States, in ratifying such a work, undertake to respect common rules for sharing and using the spectrum, the goal being efficient utilization and equitable access.

The ITU instruments relevant to spectrum management are the Constitution (CS), the Convention (CV) and, mainly, the Radio Regulations (RR). These instruments are only binding on the Member States among themselves.

The radio-frequency spectrum is a non-depletable but limited natural resource available in all countries and in outer space. Since any transmitting radio station may cause harmful interference to spectrum uses on Earth or in space, the spectrum is a common resource of mankind that requires rational management by a treaty level agreement among all countries. In that spirit, ITU has been drawing up legal instruments for over a century, so that spectrum use is based on the fundamental principles set forth in the ITU Constitution.

The ITU Radio Regulations (RR) constitute the principle regulatory framework within which States undertake to operate radio services and the basic tool for international spectrum use. They have international treaty status and are periodically reviewed (about every three years) by World Radiocommunication Conferences (WRC), which are attended by most ITU Member States.

The RR specify, amongst other things, the frequency bands allocated to radio services and the regulatory conditions and procedures that administrations must follow for implementing radio stations providing those services. The guiding principle underlying all RR provisions is that new uses must avoid causing harmful interference to the services provided by stations using frequencies assigned to them in accordance with the RR and recorded favourably in the Master International Frequency Register (MIFR).

The RRs, as drawn up by successive WRCs in past years, aims to allow each country the greatest possible flexibility with regard to spectrum use. In particular, the Table of Frequency Allocations (RR Article 5) authorizes several radiocommunication services in each band; those services are not necessarily compatible locally, but each country can select those it wishes to implement on its territory. The RR's regulatory provisions and procedures then enable each country to coordinate, as required, the stations providing the services selected with those of other countries that may be affected, thus maximizing the efficient utilization of the spectrum.

This relatively flexible framework has the advantage of respecting the wide range of countries' spectrum needs and their sovereign right to meet those needs as long as it does not place undue constraints on other countries. It has the disadvantage of limiting economies of scale and the capacity for interoperability required to develop radiocommunications, in particular within the framework of worldwide services or those intended for the general public (e.g.

mobile telephony, satellite broadcasting). For this reason, a major effort has been made to harmonize spectrum use at regional, or even global level, in particular with regard to mobile telephony. The activity towards harmonization has been to identify specific frequency bands for applications, corresponding to specific standards. The purpose of this harmonization is to increase economies of scale and decrease interference and incompatibilities.

Principles of national spectrum use

The radio-frequency spectrum is in the State's public domain. As such, it is subject to State authority and must be managed efficiently so as to be of the greatest benefit to the entire population. This spectrum management usually takes place within a regulatory framework comprised of legislation, regulation, procedures, and policies.

As the result of the State's right to manage the spectrum, authorized spectrum users derive the benefits of the right and associated obligations to access and use the spectrum.

It is up to the State, or a delegated regulatory authority, to allocate frequency bands for government or administrative uses, broadcasting, and telecommunications in the private industrial and commercial sector, taking into account the ITU Table of Frequency Allocations (RR Article 5) with due regard to the State's international commitments.

The managing authority draws up the national frequency allocation table and the national frequency register listing frequency assignments and keeps them up to date.

It is responsible for coordinating the establishment, on national territory, of radio stations so as to ensure optimal use of available sites with a view to obtaining the best possible overall electromagnetic compatibility.

The State can include provisions in its regulatory framework aimed at protecting transmitting and receiving radio centres from obstructions, and at protecting receiving radio centres from electromagnetic interference. The State, or the managing authority, can impose effective and appropriate spectrum utilization, taking account of the available technology and the development of society.

In order to ensure optimum use of the frequency spectrum, the managing authority may proceed to reaffirming that this objective can be achieved either through the direct exercise of authority or through a negotiated process involving a financial consideration or by a procedure combining the two approaches. For example, the managing authority can use spectrum redeployment.

As regards the public domain, the managing authority may make arrangements, including through a unilateral procedure (for example, licence revocation for non-utilization of assigned frequencies), in order to ensure the proper execution of missions of general interest or public service.

Spectrum utilization for broadcasting and for telecommunications purposes in the private commercial and industrial sector

The utilization of frequencies in the national territory either to transmit or to transmit and receive signals is subject to administrative authorization (i.e. a licence). The State, or a delegated managing authority (which in some countries is not necessarily the same as the regulatory

authority mentioned in the section above), grants individual authorizations to use the spectrum on national territory by assigning specific frequencies.

In the case of radio stations situated in an extraterritorial area (i.e. sea, space), the States or delegated authorities can also grant authorizations, in compliance with the RR and any relevant international agreements.

In exceptional cases, and in the conditions set forth in the national regulations, low-power, short-range radio telecommunication facilities and facilities not using frequencies specifically assigned to their user can be freely established. The State may require authorized operators to pay a compensation for the right to use the spectrum. This compensation should be in proportion to the estimated value of the resource.

The State, or the delegated managing authority, can impose terms and conditions of general interest on authorized operators.

The competent authority must define the technical standards and essential requirements with regard to:

- public health;
- electromagnetic compatibility;
- efficient utilization of the spectrum allocated to terrestrial or space stations and of orbital resources in order to avoid harmful interference.

The radio equipment whose use is authorized in the national territory must comply with these standards and essential requirements.

Prevention and elimination of interference

The State, or its delegated authorities, must ensure that the spectrum is utilized in conformity with the conditions stipulated in national and international regulations, in particular Article 15 of the RR. They must ensure that equipment is not sold unless it conforms to the essential standards and requirements set forth in national regulations. They must also take steps to prevent unauthorized utilization of the spectrum by employing methods such as:

- monitoring the spectrum and seeking out unauthorized radio stations;
- managing licences giving access to the spectrum and monitoring the technical and operating conditions of radio stations;
- identifying the sources of interferences in response to complaints.

The State, or its managing authorities, must put a stop to any recognized harmful interference observed.

Depending on national law, the State's liability may be incurred when an interest has been infringed. A claim may be made by any person, foreign or not, having suffered damages. The State may be charged with a variety of faults: failure to act, insufficient means, inefficiency, delayed action, seriousness of the infringement of a general interest, and so on, such infringement shall conform to the legislation of such country.

Rights and obligations of the authorized users

The authorization (or licence) does not confer ownership of part of the spectrum but only the right to use it for a period of time specified in the authorization and in accordance with the rules contained in the terms and conditions attached.

The State, or the delegated managing authority, may limit the number of authorizations giving access to the spectrum because of the technical constraints inherent in frequency availability. The authorization may not be transferred unless so provided in the national regulatory framework.

The State or delegated authority endeavours to provide a level of protection to the users from harmful interference. The authorized users must respect the general rules and those laid down in the terms and conditions, and may only utilize those frequencies it has been assigned.

The terms and conditions for telecommunication operators authorized to set up a public network may also contain obligations of a general nature, such as:

- minimum coverage of the population or the territory;
- a minimum number of services offered to consumers and a minimum quality threshold;
- guaranteed protection of personal data and the private lives of users and secure electronic exchanges.

The authorized user is in breach of its authorization should it fail to comply with its obligations. Depending on the seriousness of the non-compliance, the penalty may be:

- total or partial suspension, reduction in the duration, or withdrawal of the authorization;
- a financial penalty if the non-compliance did not constitute a criminal offence.

Penal sanctions (imprisonment and/or fines) may be instituted by the national laws for the most serious offences, such as:

- unauthorized establishment or maintenance in violation of a decision to suspend or withdraw the authorization;
- interference with an authorized service by making unauthorized use of a frequency or by using a radio facility that does not meet the applicable essential requirements;
- for broadcasting, violation of the provisions on the power or location of the transmitter.

Transparency in national spectrum management

In the field of spectrum management, one of the pivotal tasks of each administration is to define the categories of users subject to specific management, and to draw up a national frequency allocation table dividing utilization of the spectrum among the categories of users, with their related rights and obligations.

The requirement of transparency varies depending on the type of user concerned. As mentioned above, transparency is a highly desirable management method in competitive markets; in other areas, however, where confidentiality and secrecy are crucial, transparency is neither required nor desired. Indeed, even in the regulation of markets open to competition, transparency is partly limited by the right to protect public needs and trade secrets.

For example, a significant part of the spectrum is usually allocated to the government's inherent functions, such as defence, policing, and security. Those activities require special protection, and transparency in their management is not the rule. Qualified transparency may be applied

to other activities in which security is important, such as maritime or aeronautical utilizations. However, utilization of the spectrum should benefit from transparent management, except for those previously cases mentioned.

Transparency may apply in particular to the following areas:

- allocation to services, frequency planning (participation in the establishment of the relevant parts of the national frequency allocation table);
- issuing of licences, assignment to stations, notification to ITU;
- conditions for frequency sharing;
- installations/grouping of stations;
- preparation of negotiations on international treaties relating to spectrum management (in particular WRCs, which amend the RR). Indeed, although it is governments that negotiate treaties, those treaties can modify the national regulations applying to other players, who should therefore be able to take part, whenever necessary, in national preparations.

The linkage between international and national regulations

As in any other field, national legislation is drawn up with due regard for the State's undertakings in the framework of its international activities. When it comes to radio frequencies and associated orbits, the States' rights and obligations are governed mainly by the RR, which stipulate that those orbits and frequencies must be used rationally, efficiently, and economically so that countries may have equitable access to them.

The RR complements the ITU's Constitution and Convention. The RR has international treaty status and national legislation must therefore conform to its provisions. This is obviously an essential rule for drafting national legislation. It must nevertheless be borne in mind that the RR are reviewed at WRCs held on the average every three years. Provision must therefore be made to adapt national regulations at the same pace.

The State may be bound by other obligations in the framework of its commitments to a regional organization or under bilateral or multilateral agreements.

Monitoring the spectrum

In order to guarantee that spectrum use conforms to existing regulations and the authorizations granted, there must be a spectrum monitoring system comprising fixed and mobile equipment.

That equipment is employed to check that frequencies are used in accordance with the authorizations granted. It can also be used to detect sources of interference.

The means involved are substantial and should be used in alliance whenever possible. They can be employed to conduct the international enquiries requested by ITU-R or by a foreign administration in the event of interference.[2]

Best practices for national spectrum management

With due regard to the ITU Constitution and Convention, this section addresses best practices for national spectrum management activities.[3] International practices are not included.

[2] Further information may be found in ITU (2011).
[3] The contents of this section are an excerpt from ITU (2015b), Annex 2.

However, some of the best practices outlined below are intended to interface with, or transition to, international practices, e.g. those relating either to collaboration with colleagues in other countries, or to coordination, such as that which would occur at a bilateral or multilateral consultation preceding a WRC, or at an international satellite coordination meeting. These practices are further intended to harmonize global spectrum management policies, to the extent practicable, by harmonizing practices among national administrations.

Best practices:

- Establishing and maintaining a national spectrum management organization, either independent or part of the telecommunication regulatory authority responsible for managing the radio spectrum in the public interest.
- Promoting transparent, fair, economically efficient, and effective spectrum management policies, i.e. regulating the efficient and adequate use of the spectrum, taking into account the need to avoid harmful interference and the possibility of imposing technical restrictions in order to safeguard the public interest.
- Making public, wherever practicable, national frequency allocation plans and frequency assignment data to encourage openness, and to facilitate development of new radio systems, i.e. carrying out public consultations on proposed changes to national frequency allocation plans and on spectrum management decisions likely to affect service providers, to allow interested parties to participate in the decision-making process.
- Maintaining a stable decision-making process that permits consideration of the public interest in managing the radio frequency spectrum, i.e. providing legal certainty by having fair and transparent processes for granting licences for the use of spectrum, using competitive mechanisms, when necessary.
- Providing in the national process, in special cases where adequately justified, for exceptions or waivers to spectrum management decisions.
- Having a process for reconsideration of spectrum management decisions.
- Minimizing unnecessary regulations.
- Encouraging radiocommunication policies that lead to flexible spectrum use, to the extent practicable, so as to allow for the evolution of services[4] and technologies using clearly-defined methods, i.e.:
    - eliminating regulatory barriers and allocating frequencies in a manner to facilitate entry into the market of new competitors;
    - encouraging efficiency in the use of spectrum by reducing or removing unnecessary restrictions on spectrum use, thereby encouraging competition and bringing benefits to consumers; and
    - promoting innovation and the introduction of new radio applications and technologies.
- Assuring open and fair competition in the marketplaces for equipment and services, and removing any barriers that arise to open and fair competition.
- Harmonizing, as far as practicable, effective domestic and international spectrum policies, including of radio-frequency use and, for space services, for any associated orbital position in the geostationary-satellite orbit or of any associated characteristics of satellites in other orbits.
- Working in collaboration with regional and other international colleagues to develop coordinated regulatory practices, i.e. working in collaboration with regulatory authorities of other regions and countries to avoid harmful interference.
- Removing any regulatory barriers to free circulation and global roaming of mobile terminals and similar radiocommunication equipment.

[4] Whenever the term "services" is used in this Handbook, it means applications and recognized radiocommunication services.

- Using internationally recommended data formats and data elements for exchange of data and coordination purposes, e.g. as in the Radio Regulations Appendix 4, and in the ITU Radiocommunication Data Dictionary (Recommendation ITU-R SM.1413).
- Using "milestone" management steps and phases to monitor and control lengthy radiocommunication system implementation.
- Adopting decisions that are technologically neutral and which allow for evolution to new radio applications.
- Facilitating timely introduction of appropriate new applications and technology while protecting existing services from harmful interference including, when appropriate, the provision of a mechanism to allow compensation for systems that must redeploy for new spectrum needs.
- Considering effective policies to mitigate harm to users of existing services when reallocating spectrum.
- Where spectrum is scarce, promoting spectrum sharing using available techniques (i.e. frequency, temporal, spatial, modulation coding, processing, and so on), including using interference mitigation techniques and economic incentives, to the extent practicable.
- Using enforcement mechanisms, as appropriate, i.e. applying sanctions for non-compliance with obligations and for inefficient use of radio-frequency spectrum under relevant appeal processes.
- Utilizing regional and international standards whenever possible, and where appropriate, reflecting them in national standards.
- Relying to the extent possible on industry standards including those that are included in ITU Recommendations, in lieu of national regulations.

6.3 Part 2. Key applications and regulatory considerations driving the future use of spectrum

Introduction

In an increasingly digital environment, adequate access to spectrum is key to expanding the deployment and coverage of telecommunication networks, and addressing the ever-increasing demand for data services. These networks support a variety of online applications, extending the impact of spectrum management to several sectors of the economy by transforming the way people access resources for health, transportation, education, agriculture, employment, government, and financial services. As a scarce resource, spectrum requires proper management from regulators, to ensure equitable access and an interference-free environment among different users and services, as well as to introduce new technologies. Accordingly, there is a need to strike the right balance between regulatory requirements that provide certainty and protect consumers, and the need to ensure flexibility for the development of new wireless technologies.

This chapter discusses key applications driving the future use of spectrum, highlighting some of the main points that regulators are invited to consider on the national level, based on the relevant experience of different country examples.[5] It presents some of the mechanisms for spectrum allocation and licensing of new spectrum, with due consideration to technology evolution. It also looks at promoting the use of spectrum for these key applications, as well as business models that can strengthen existing and new approaches for the deployment of wireless broadband. Another aspect discussed is the implementation of policies that enable

[5] For more detailed examination of the topics covered in this chapter, see relevant thematic sections on the *Digital Regulation Platform*.

stakeholders to leverage these emerging technologies, such as the fifth generation (5G) of mobile technologies and the Internet of Things (IoT).

Key trends in spectrum management for emerging technologies

Spectrum management defines the radiocommunication service allocations, the technical specifications, and determines which types of services and technologies can operate in a country. As such, it can determine the pace of deployment of such technologies.

Wireless technologies have become the most common way to access the Internet around the world, using both licensed and unlicensed spectrum bands, and through a variety of devices. The need to use more teleworking and e-learning applications and the growing popularity of online entertainment (e.g. movie and music streaming, and gaming) have contributed to increasing data traffic, especially using smartphones and tablets. At the end of 2019, about 5.3 billion people had mobile broadband subscriptions, highlighting its importance in providing connectivity (ITU 2019c). Wireless broadband can be accessed in different ways, including mobile networks, Wi-Fi hotspots, satellites, and, more recently, drones and balloons. In the context of constant technology innovation, an effective spectrum policy is meant to foster the deployment of different services.

Mobile broadband requires sufficient spectrum to be identified for International Mobile Telecommunications (IMT) use – commonly known as 3G, 4G, and 5G – while technologies leveraging unlicensed spectrum require sufficient unlicensed/licence-exempt spectrum. As a result, governments must identify the best possible ways to plan, allocate, and assign spectrum to meet the future needs of operators and consumers, while assuring efficient use of valuable spectrum resources and fostering competition. As spectrum plays a critical role in realizing the full extent of access to broadband capabilities, its efficient use has a direct social and economic impact in multiple sectors of society.

Recently, new technologies and applications have been developed with the goal of enhancing and expanding access to broadband connectivity. Regulators should take them into consideration when looking at the future of their national spectrum management plans, while ensuring the development of existing technologies. For example, in addition to terrestrial 5G networks, applications such as high-altitude platform stations (HAPS) and satellites in non-geostationary orbit (NGSO) have also evolved to support the expansion of coverage of existing telecommunication services. Additionally, digital applications in general, and the IoT ecosystem in particular, are composed of various applications with a wide range of spectrum requirements.

Technology innovations driving new spectrum demand

The demand for access to many segments of spectrum is increasing, as new technologies allow a variety of applications to make use of a broader range of frequency bands. For example, IMT applications using 5G now compete with incumbent services in low-, mid-, and high-band spectrum. While the most common frequency bands for mobile networks to date have been focused on low- and mid-band spectrum, interest in the use of the high-bands for 5G, such as millimetre wave (mmWave) between 24 GHz and 86 GHz, has put them in focus as well. This increased demand makes efficient spectrum use even more important. In addition, applications such as HAPS and NGSO satellites have also increased the pressure to access spectrum in different bands. At the same time, interconnected devices operating through applications like

Bluetooth and Wi-Fi have proliferated, further increasing competition for valuable and finite spectrum (see Figure 6.1).

Figure 6.1. Technologies driving spectrum demand

5G spectrum needs

- 5G mobile networks offer significant potential to increase data transfer capacity, as well as spectrum efficiency.
- 5G network implementation will create additional demand for frequency bands below 6 GHz, often already assigned to incumbent services or required for 4G coverage.
- Sub-6 GHz bands have relatively better propagation characteristics, offering a wider coverage area than mmWave, but their heavy incumbent use limits large, contiguous spectrum blocks.
- mmWave bands offer more spectrum due to less incumbent use, allowing for wider bandwidths, supporting higher throughputs. But its use is limited, by lower propagation characteristics making them more suitable for coverage of relatively small areas, usually in dense environments.

Advancing the use of IoT

- IoT devices in use are increasing, reaching 22 billion connected devices worldwide by end of 2018.
- Increased connectivity and capacity introduced by technologies using licensed and unlicensed spectrum are fostering more connected devices as part of IoT ecosystem.
- Successful consumer and public applications of different IoT technologies are reliant on effective and efficient spectrum management.
- Spectrum requirements for various segments of the IoT landscape depend on use-cases specific to their application. For example, connections for use by industrial automated robots are more latency-sensitive than connected kitchen appliances.
- In the context of a smart city, automated vehicles for public transportation require high-capacity, low latency connectivity. However, dispersed sensors monitoring air pollution have less restrictive needs.

The evolution of Wi-Fi

- Wireless network technologies are critical to connected devices implementation and IoT ecosystem advancement.
- Wi-Fi and other wireless technologies operate in unlicensed spectrum and can transmit in a relatively wide range of frequencies.
- In addition to previous use of 900 MHz, 2.4 GHz and 5 GHz bands, newer Wi-Fi technologies are being implemented in 60 GHz (57-66 GHz) and 6 GHz (5 925-7 125 MHz) bands.
- Several countries (e.g. United States and United Kingdom) are increasing availability of 6 GHz band for unlicensed use.
- New rules in the United States make available 1 200 MHz of spectrum for unlicensed use in the 6 GHz band.
- Overall, regulators should be mindful of the potential value of unlicensed technologies including Wi-Fi when allocating and designating spectrum.

HAPS connectivity

- HAPS applications (i.e. radio stations located in the stratosphere between 20 and 50 kilometres above the Earth's surface) can expand access to wireless connectivity.
- HAPS support other terrestrial technologies with potential to expand connectivity and telecommunications services in rural and remote areas.
- HAPS can serve as a tool to extend existing terrestrial networks and provide higher quality service to already connected areas as well as connectivity during emergency situations.
- HAPS applications can have frequency bands either authorized directly to its provider or to an existing partner telecommunications operator, such as a mobile operator.

NGSO satellites

- NGSO satellites systems, comprised of hundreds or even thousands of satellites, provide connectivity in areas currently unreached by terrestrial telecommunications infrastructure.
- This presents some spectrum management challenges, in terms of managing use of different frequency bands and allowing GSO and NGSO satellite systems to operate simultaneously, while mitigating the risk of harmful interference.

Source: ITU (no date); ITU 2016; Mercer 2019; Wi-Fi Alliance 2020; Ofcom 2020a; FCC 2020b; FCC 2020c.

Managing changes in spectrum demand for emerging technologies

While the examples in the previous section show how new technologies are using new frequency bands, it should be noted that these technologies also bring technical advancements that provide a more efficient use of existing spectrum. There are different industry solutions, and it is important to understand their functionalities and impacts on national frameworks. One way is to obtain information through consultation processes in order to review how their spectrum assignment regulation is implemented. This gives opportunity for the industry to demonstrate that interference or sharing issues can be addressed.

Furthermore, regulators should recognize the need for flexible frameworks that foster the deployment of spectrum for new applications. Effective management of competing demands for spectrum is necessary to maximize the use of finite spectrum resources and fully realize the potential consumer benefits of these new technologies, as well as broader social and economic goals, with the overall goal of expanding access to connectivity. Spectrum sharing for both licensed and unlicensed uses can contribute to market expansion, increased competition among providers, and data offloading for telecommunication networks (García Zaballos and Foditsch 2015, 21). These benefits increase consumer choice and allow users to take advantage of new and more efficient telecommunication technologies. Once frequency bands are allocated, it is important for regulators to leverage regulatory flexibility to maximize efficiency among competing services in those bands.

Spectrum management and standards for emerging technologies

Elements of spectrum management

Spectrum management is an important tool for governments to optimize the use of a finite public resource. With spectrum demand continually growing, competition for particular frequency bands will become even greater and efficient use of that spectrum more critical.

Effective spectrum management is needed to:

- protect frequencies used by critical services by preventing harmful interference;
- identify opportunities to maximize efficiency
- allow new technologies to develop and deploy within flexible frameworks; and,
- reduce the cost of telecommunication equipment.

To keep up with the evolving demand and use of spectrum, regulators should implement best practices in spectrum planning, engineering, and authorization. That means staying abreast of how new and existing technologies are using spectrum. A key aspect of this process is monitoring current spectrum use to identify areas where efficiency can be improved. Spectrum monitoring enables regulators to ensure the compliance of spectrum users with current regulations, identify and address interference issues, and gauge the use of different frequency bands. As new technologies compete with incumbent services across the spectrum, a proactive and modern approach to monitoring is increasingly necessary (Lu and others 2017). Evaluating the efficiency of spectrum use can present challenges, as it may be difficult to compare the relative benefits provided by different services. Governments should consider promoting efficiency by incentivizing spectrum users to deploy more efficient technologies as well as by allowing spectrum sharing, leasing, or trading. For example, in 2017 Singapore's Infocomm Media Development Authority (IMDA) required operators to phase out their 2G networks in

favour of more efficient mobile technologies on a scheduled timeline (IMDA 2017). These kinds of effort are important to advance spectrum efficiency at the national level. Cooperation at the international level provides further benefits and opportunities for efficiency in terms of avoiding interference.

The harmonization of frequency allocations at the global and regional levels can bring significant benefits to consumers, as manufacturers can produce devices and equipment at greater scale, lowering their costs, and consumers can use their devices in different countries, effectively permitting the use of roaming. The decisions taken at the International Telecommunication Union (ITU) World Radiocommunication Conferences (WRC) drive long-term international harmonization and balanced allocation of spectrum among competing services. For those decisions to be implemented at the national level, and for new services to flourish, national governments must proactively integrate the WRC decisions into their national regulatory frameworks.

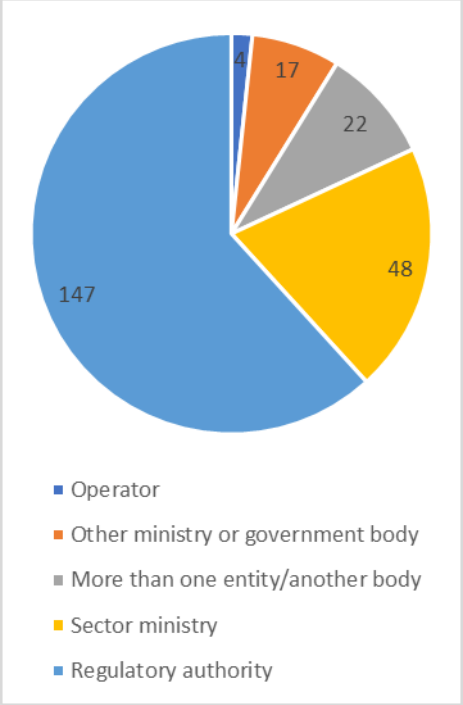
For example, the results of WRC-19 included several important spectrum decisions, especially related to new technologies, such as new frequency allocations for HAPS and NGSO satellite systems. The conference also identified additional frequency bands for use by IMT to foster the deployment of 5G applications. In preparation for WRC-23, new studies include identification of new low- and mid-band frequencies for IMT, and several proposals for NGSO satellite networks in existing fixed-satellite service (FSS) bands. These studies will continue the effort of managing scarce spectrum to allow multiple services to operate and can guide the long-term planning for national spectrum management initiatives.

The role of the regulator on national spectrum issues

It is important for administrations to consider how spectrum issues are addressed in the national government structure. Considering the technical nature of the spectrum management functions, there is often pressure to design regulatory structures and internal procedures to optimize the use of resources available and to increase its efficiency. This is even more evident when supporting the deployment of new technologies.

It is important to establish a management or administrative body providing leadership and supervision for the implementation of spectrum planning, as long-term planning is almost always a primary task at management level and one which cannot be delegated, because of the consequences and significance of the decisions to be taken (ITU 2019a, 4). Most countries include the spectrum management functions as a branch within the relevant regulator or ministry dealing with information and communications technologies (ICT), and about one in five countries have separate, dedicated spectrum management agencies (ITU 2019d). It is also important to clearly separate the spectrum from content discussions, especially in cases where separate entities within the government deal with ICT and broadcasting and media issues.

Figure 6.2. Spectrum management entity



Source: ITU 2019d.

In terms of spectrum planning, long-term planning presents significant challenges for spectrum managers as it requires them to foresee spectrum demand far into the future, generally for periods of 10 to 20 years. This highlights the importance of a well-established structure to bring transparency to the process, resulting in a more stable regulatory environment. While relevant for any country, this is particularly important for developing countries that need to attract investment for infrastructure development. Transparency mechanisms can include issuing public consultations, spectrum road maps, regulatory agendas, public access to spectrum inventory and availability of spectrum, as well as spectrum plans for specific services. For example, the Australian Communications and Media Authority (ACMA), the country's ICT regulator, regularly publishes detailed public consultations on spectrum issues as well as an annual five-year spectrum outlook that sets out an action plan and regulatory priorities (ACMA 2019). The report itself is released for public comment in advance of its official publication, in a further effort to increase transparency and public input. ACMA also maintains an online progress report to allow interested parties to track the implementation of its current action plan (ACMA 2020).

Importance of technical standards for mobile broadband and other applications

The widespread adoption of technology at a global scale depends on a robust consensus over technical standards. Technical standards are agreed upon through discussions at the ITU, as well as various telecommunication standard development organizations (SDO). For example, the 3rd Generation Partnership Project (3GPP) is a group that publishes the specifications for mobile technologies.[6] Regulators need to be mindful of the work done in the SDOs to better anticipate and prepare for new developments that could require changes in their spectrum frameworks.

[6] https://www.3gpp.org/about-3gpp

Box 6.1. Guidelines for limiting human exposure to electromagnetic fields

Another important aspect of international standards is compliance with guidelines for limiting human exposure to electromagnetic fields (EMF). The advance of new technologies, especially with the deployment of 5G networks, is driving the densification of telecommunications networks. More and more small cells are being deployed, supporting high-capacity networks in small high-density areas. Additionally, previous editions of standards for the calculation of maximum acceptable limits, which are often referenced in national regulations, did not include frequency ranges for mmWave bands.

In order to address this situation, the International Commission on Non-Ionizing Radiation Protection (ICNIRP) has updated its guidelines on limiting exposure to EMF for the protection of humans exposed to radiofrequency electromagnetic fields (RF) in the range 100 kHz to 300 GHz (ICNIRP 2020). As of June 2020, no countries have formally adopted the new guidelines yet, though most countries around the world, and nearly all of Asia, Europe, and South America, adopted the 1998 guidelines, incorporating them into national EMF regulations (GSMA 2019). Some countries implement limits stricter than those in the ICNIRP guidelines, when incorporating them into the national regulatory framework. As noted by an ITU study, until 2022 up to 63 per cent of mobile data traffic demands would not be served in countries and regions where EMF limits are significantly stricter than those defined in the ICNIRP guidelines. This emphasizes the need for EMF exposure limits be harmonized worldwide (ITU 2019e). Regulators should take the ICNIRP guidelines into consideration and update their national regulatory frameworks to address the limits when using new technologies, such as 5G and small cells.

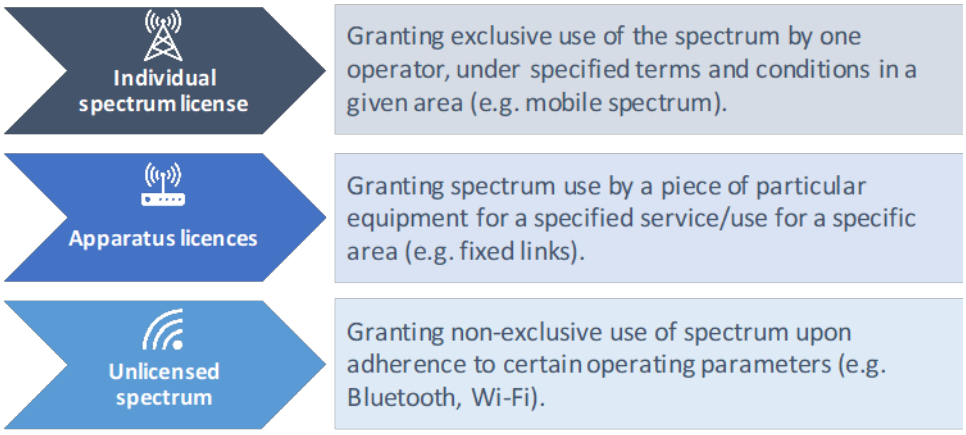
Source: GSMA 2019; ICNIRP 2020; ITU 2019e.

National spectrum licensing

Spectrum is a limited natural resource that is managed and assigned by national administrations, taking into account the decisions made at the regional and international level. Regional agreements may facilitate the spectrum licensing process in a determined area, especially to coordinate on potential cross border issues. Furthermore, the ITU Radio Regulations (RR) is the international treaty dealing with spectrum management.

Spectrum is used to support many different applications, including mobile, fixed, satellite, broadcasting, and amateur radio services. To manage the wide variety of different services and mitigate harmful interference, regulators issue national frequency allocation tables and establish licensing frameworks that govern how spectrum will be awarded in the country. Most generally, spectrum is licensed through one of the mechanisms shown in Figure 6.3.

Figure 6.3. Spectrum licensing mechanisms



Individual spectrum licences are usually assigned through an administrative assignment or "beauty contest" approach, an auction approach, or a hybrid approach which contains elements of both a direct assignment and an auction. Mobile spectrum is usually issued under an individual spectrum licence via either direct assignment, auction, or a hybrid approach.

Apparatus licences are commonly issued by direct assignment, on a first-come, first-served basis. The apparatus licence authorizes the operation of an individual device or type of device to deliver an approved service at a defined location. They are frequently used for fixed point-to-point links, and for bands with adequate spectrum supply for the demand of the different users. For example, Australia authorizes fixed links under an apparatus licence framework.

Unlicensed spectrum are frequency bands that are exempt from licensing, normally used for the operation of low-power, short-range devices. Devices in unlicensed bands should operate under defined technical conditions to ensure that they do not cause harmful interference to other radiocommunication users. Unlicensed bands enable widespread use of various technologies, including Bluetooth, Wi-Fi, and the IoT.

All three types of licences play important roles in national spectrum licensing frameworks, as well as the concept of technology neutrality in the licence terms. Fixed link apparatus licences for backhaul services play a key role in supporting mobile networks. For example, the United States has introduced a light licensing model for fixed point-to-point links. Under the light licensing model, the Federal Communications Commission (FCC) issues non-exclusive nationwide licences applicable for the 71-76 GHz, 81-86 GHz, and 92-95 GHz bands, and the licensee must then register each link through a designated third-party database manager (FCC 2003).

Given the general difficulty in obtaining spectrum under individual spectrum licensing compared to other licence types, regulators are often careful when designing assignment processes to consider market conditions and to foster an enabling environment for investment. Regulators seek to increase regulatory certainty and encourage investment by granting licences for longer terms. While licence terms can vary from to 25 years, most commonly they are issued for terms of between 10 and 20 years (ITU 2019d). For example, the generally preferred approach in the United Kingdom is to issue a licence for an indefinite term with an initial period, after which time the Office of Communications (Ofcom) will be able to revoke the spectrum under specific spectrum management reasons with notice to the licensee (Ofcom 2005). Colombia is also trending toward longer licence terms with the passage of its new ICT Modernization Act,

which extended licence terms from 10 years to 20, with the possibility of a renewal of up to 20 years (Law No. 1978 of 25 July 2019, Art. 12). The European Union's European Electronic Communications Code mandates 20-year licence terms, although some Member States have interpreted the guidelines by assigning licences with a 15-year term and the possibility of a five-year renewal (Directive 2018/1972, Art. 49).[7] Also, in Brazil, new amendments to its telecommunications law allow spectrum licences to be renewed indefinitely for terms of up to 20 years, subject to rules to be defined by the National Telecommunications Agency (Anatel) (Law No. 13879 of 3 October 2019, Art. 167). Most African countries are still using fixed term licences varying from 10 to 15-year term for dedicated technologies.

These examples show how regulators are increasingly balancing regulatory certainty for operators with a measure of flexibility for the regulator to adjust to market conditions. In the above examples, operators are guaranteed spectrum for a defined period, while regulators maintain some oversight and flexibility during licence renewals. This allows regulators to match spectrum holdings to fit the market and ensure the most effective use of the resource, which could include a decision to refarm the band as a result of market demand.

In addition to longer licence terms to increase regulatory certainty for operators, regulators have also been cognizant of operators' investment and deployment burdens to improve networks. These costs, coupled with other overhead costs such as spectrum utilization fees, may impact operators' ability to invest. Recent assignments, through both administrative, auction, and hybrid approaches, have shown the trade-off between spectrum revenue maximization and fulfilment of other policy aims, such as ensuring connectivity access to all the population.

Recent trends in administrative assignment processes

Administrative assignments are common for many types of services, like fixed links, gateway earth stations, and other apparatus licences, and is also an approach to licence mobile spectrum. For common spectrum uses, e.g. for fixed links for backhaul services, the assignment process is generally straightforward and well defined. As most regulators have already issued such licences, guidance and relevant application forms are usually available and applications are processed and assigned on a rolling basis. As for other types of licences that are not as commonly requested or licences for new technologies, the applicable licensing frameworks and procedures may not be as clear. This increases regulatory uncertainty for potential applicants of new technologies or business models, as the procedure, processing time, and the likelihood of a successful application are often unknown.

Regulators also assign mobile spectrum by direct assignment. Unlike other services, assignments for mobile spectrum are not usually issued on a rolling basis but rather the regulator opens a call for applications to issue all or part of available spectrum in a certain band at one time. When assigning spectrum, many regulators award spectrum according to criteria in alignment with policy objectives. While some of the spectrum auctions for 3G and 4G networks were based on government revenue maximization, which might have led to failed auction results, more recently countries are focusing on deployment requirements such as the expansion of coverage, and access to faster mobile broadband in underserved areas. The high expected costs of 5G have encouraged some regulators to discount spectrum or offer it in exchange for network investment and deployment commitments to encourage 5G networks in the country. Japan and China are recent examples of countries that have taken this approach (MIC 2019a; MIC

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN.

2019b; GSMA 2020, 44). Other regulators, e.g. in Hong Kong, China and Uruguay, reflected on the policy impetus of deploying 5G networks and the relative abundance of 5G spectrum and decided to offer or refarm the spectrum without a fee (OFCA 2019b; URSEC 2019).

When assigning spectrum administratively, regulators should be clear and transparent in the assignment criteria, procedure, relevant documents, and timeline, no matter for which service the spectrum is being assigned. For assignments of a limited number, such as mobile spectrum, regulators should open the process to new entrants in the market by publishing rules and announcements publicly and avoid closed-door processes. As shown in the above examples, direct assignment processes allow regulators to encourage and drive certain policy aims, such as to facilitate 5G network deployment or increase coverage to underserved or unserved areas of the country. Using assignment processes in such a way gives regulators an effective tool to meet policy goals. Also, allowing spectrum trading in the licence terms, including those for mobile services, can help to balance spectrum demand with supply by allowing operators to sell underutilized spectrum to another party that values this licence more highly. Tradable spectrum rights provide incentives to licensees to use spectrum in a more efficient manner (ITU 2018a).

Apart from mobile services, many new services and emerging technologies are being developed, which require spectrum to operate. Regulators should proactively issue guidance on the applicable licensing regime, especially for those services whose use has been designated at the regional or international level. Licensing new services may require some trial and error, highlighting the importance of allowing for temporary and experimental licences. Regulators should openly communicate with new service providers to ensure regulation does not inadvertently hinder innovative services or business models. Additionally, regulators could consider streamlining the assignment process for certain applications that require little coordination and oversight, such as when applying for highly directional fixed link spectrum, where coordination can be more easily managed, and harmful interference mitigated. Prompt processing times for spectrum applications that are accepted on a rolling basis should be the goal to facilitate access and expand services. Additionally, posting information on the availability of relevant bands publicly would be helpful for applications requesting spectrum that is assigned on a first-come, first-served basis in a crowded band.

Spectrum management practices amid extraordinary events

In general, regulators should be aware of the various demands for spectrum in their markets and release sufficient spectrum to support applications that allow high-quality connectivity and viewing, especially in the situation of extraordinary events. As an example, in 2020 several regulators have addressed spectrum issues in response to increased demands on communication networks, driven by the shelter-at-home orders in many countries around the world to combat the spread of COVID-19 pandemic.[8]

Recent trends in auction and hybrid processes

Spectrum auctions represent the market's valuation of spectrum and are a common means of awarding spectrum. Regulators have a degree of flexibility in auction design, allowing them to incorporate specific targets tailored to the unique policy aims of the country and the circumstances of the market. When deciding which obligations to incorporate, regulators should

[8] A live compilation of these different initiatives is summarized at https://reg4covid.itu.int/.

consider conducting public consultations on planned guidelines to ensure the scope and timeframe of the obligations are realistic and do not unintentionally discourage potential bidders from participating. To promote new entrants, auction guidelines can differentiate incumbent and new entrant obligations. Similarly, establishing spectrum caps or requirements for the winning bidders to provide wholesale access are additional actions that may support smaller players, ultimately to promote competition in the market. Auctions that have "use it or lose it" rules are sound obligations that can prevent potential hoarding and promote effective use of spectrum, although regulators should give due consideration to the realistic amount of time needed by operators to use spectrum, especially if network upgrades or deployments are needed.

In their most basic sense, auctions focus on an operator's willingness to pay as a determinant to receive spectrum. However, regulators are increasingly designing auctions that consider other criteria. For the continuous deployment of 4G, and more recently of 5G networks, many countries have incorporated clauses in licence terms requiring the licensee to meet certain coverage, deployment, speed, or other service quality requirements, or to uphold competition in the market.

Several auctions have established measures to improve coverage and services including in Germany, the Slovak Republic, and the Czech Republic, among others (BNetzA 2019; RU 2020; CTU 2020). Other common elements of auctions are aimed specifically to promote competition, such as establishing spectrum caps, requiring licensees to offer wholesale access or provide national roaming. Additionally, many licence terms include "use it or lose it" policies that require spectrum to be used before a certain date to ensure effective use of the spectrum and prohibit spectrum hoarding.

In some cases, countries have discounted the prices paid for use of the spectrum in exchange for coverage commitments to encourage the narrowing of the rural digital divide. In Sweden, the winning bidder of a 700 MHz block of spectrum with coverage and deployment requirements received a credit of SEK 300 000 000 on the spectrum price in exchange for meeting these requirements and improving service in underserved areas (PTS 2018). In the United States, for the planned auction of the 3.5 GHz band, operators providing service to predominantly rural areas are eligible for a 15 per cent discount on the winning bid price (FCC 2020a). Colombia's ICT Modernization Law allows operators to make in-kind payments in terms of network deployments to cover a portion (up to 40 per cent) of the cost of frequency licences (Law No. 1978 of 25 July 2019). In a recent auction, winning bidders committed to deploying service in specified rural areas over the next five years as in-kind payments (MinTIC 2019; MinTIC 2020).

Hybrid processes, which have elements of both direct assignments and auctions, are also integrating goals to increase coverage, encourage network deployment, and ensure competition in the market. France's assignment procedure of the 3 400-3 800 MHz band is an example of a hybrid process. In the first "direct assignment" phase, only bidders who commit to optional commitments are eligible to receive one of four 50 MHz blocks.[9] In the second "auction" phase, bidders can bid for additional 10 MHz blocks in subsequent rounds, up to a spectrum cap of 100 MHz per operator. The regulator has also set a minimum cap of 40 MHz over the two phases of the auction, presumably to ensure that all operators are guaranteed a portion of the spectrum for the provision of 5G services. All winning bidders will be subject

[9] The optional commitments include actions to foster innovation by providing customized solutions to economic actors or assign frequencies locally, provide indoor coverage, supply fixed access products on mobile networks, improve mobile virtual network operator (MVNO) hosting, and increase transparency (Arcep 2019).

to 5G deployment, coverage, and speed obligations and are also required to make mobile networks IPv6-compatible and use network slicing (Arcep 2019).

Regardless of the obligations established, regulators must have the means to effectively monitor adherence to the licence's obligations, such as coverage and timely deployments, to ultimately make progress towards achieving the policy goals.

Licensing for local and private networks

Different from other IMT generations, the opportunities from 5G are often discussed in terms of the new use cases and applications they enable. To use spectrum efficiently, some regulators are offering spectrum to non-traditional players for private networks to support localized 5G applications. Localized spectrum allows operators to tailor private networks according to their specific needs, especially for applications requiring a high degree of precision and low latency. Deployment costs in the small localized area are much lower and can be rolled out at a much quicker pace than waiting for a national provider to establish high-quality and reliable national service to support their foreseen 5G applications.

Industrial actors have been interested in the possibilities of designated spectrum to support various industrial applications within 5G private networks, such as smart factories. Designated spectrum allows industrial players to customize their networks according to their needs and the applications they wish to support, potentially more so than if they had to rely on a mobile operator's network. For example, Germany opened 100 MHz in the 3.7-3.8 GHz band for 5G local spectrum licences for "Industry 4.0" purposes. The localized assignments allow many more users to obtain a large bandwidth of frequency in different areas of the country, meaning that local users could have up to 100 MHz of spectrum solely to support their private needs (BNetzA 2020). Several regulators have released spectrum for local networks or plan to do so in the future (Table 6.1).

Table 6.1. Examples of licensing for local and private networks

Country	Band	Envisaged usages
Germany	3.7-3.8 GHz (available) and 24.25-27.5 GHz (potential)	Industry 4.0, agriculture, forestry; Local 5G applications (industrial, mobile broadband, fixed wireless access)
United Kingdom	1 800 MHz, 2 300 MHz, 3.8-4.2 GHz, and 24.25-26.5 GHz (first-come, first-served basis)	Private networks, or to offer rural or indoor coverage, or fixed wireless access
Chile	3.75-3.8 GHz (planned)	Local private networks
Brazil	3.7-3.8 GHz (consultation)	Local private networks
Japan	2 575-2 595 and 28.2-28.3 GHz MHz (awarded)	Local private network (used for high-definition, AI-powered security system)
Hong Kong, China	27.95-28.35 GHz (available on first-come, first-served basis)	Provision of localized wireless services in defined areas of no more than 50 square kilometres
Malaysia	26.5-28.1 GHz (plans to award on first-come, first-served basis)	Localized/private networks for enterprise and industrial services

Source: BNetzA 2020; Ofcom 2019; Chile, *Resolution 2400 of 28 November 2019* (https://www.leychile.cl/Navegar?idNorma=1139171); Anatel 2020; Fujitsu 2020; OFCA 2019a; MCMC 2019.

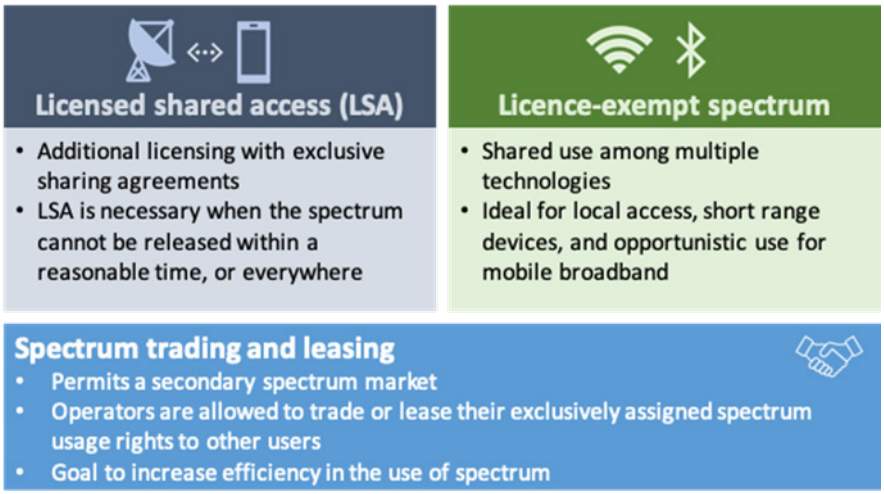
The trend towards local licensing is linked to the usage scenarios enabled by 5G, especially those for industrial applications that require high bandwidth and low latency, over a small coverage area. This approach encourages the deployment of industrial 5G use cases while national 5G networks are being deployed at a more measured pace, a goal that various regulators support. Many regulators are issuing these licences on a first-come, first-served basis, which is aligned with policy goals to promote access to spectrum for quick deployment and adoption of new 5G applications.

Sharing regimes: licensed shared access and licence-exempt

Shared access regimes can either be part of a licensed or unlicensed regime (see Figure 6.4). Under licensed shared access (LSA), use is authorized by a licence for a set of different types of services or between users, under conditions defined in the licence. Spectrum is managed between services to avoid harmful interference. This could be managed statically, where use is not allowed under specified terms, or dynamically, where spectrum use can vary, considering use on a certain frequency, in a given area, at a specific point in time. The number of users allowed under a licensed shared access regime is usually limited and the terms of use define the priority of users in the band, where incumbent users are protected. Under a licence-exempt regime, no licence is required, and the number of users is not limited by the regulator. However, users usually must adhere to technical restrictions (e.g. power limits for receivers and transmitters, maximum levels of out-of-band transmissions, and so on).

Shared access regimes are one way for regulators to open spectrum to more users and to facilitate efficient use of spectrum bands. Licence-exempt spectrum bands have proven to be a breeding ground for innovation, as evidenced by the importance of Wi-Fi and Bluetooth technologies in enabling new applications and Wi-Fi's importance in mobile operator's traffic management regimes to offload traffic. However, at times regulators must manage shared use to avoid harmful interference, making licensed shared access a more attractive option to open additional spectrum while protecting existing services.

Figure 6.4. Spectrum sharing regimes



Licence shared access arrangements

Licensed shared access regimes have benefited from technical advances, such as geolocation databases and sensing, that enable more dynamic management of spectrum (OECD 2014, 25).

The shared access framework proposed in the United States for the 3.5 GHz band dynamically manages spectrum use between incumbent users, priority access licensees, and general authorized access users. Incumbent users are most protected against harmful interference, whereas general users receive no protection from other users. The three-tier approach was adopted to manage spectrum use between incumbent federal and non-federal users of the band and citizens broadband radio service, and to accommodate new applications, including 5G and the IoT (FCC 2020a).

A recent trend in licensed shared access is in local licensing for mobile spectrum, because of the localized nature of private 5G networks and the possibility of coexistence with mobile national networks. The United Kingdom and Hong Kong, China have adopted a licensed shared access approach to their local licences (Ofcom 2019; OFCA 2019a). Local shared access is seen in other formats as well. For example, China authorized four mobile operators to use spectrum on a shared basis, but for indoor use only (MIIT 2020).

These shared arrangements provide a tool for regulators seeking to assign spectrum to new services in bands already allocated to incumbent services. This approach can also leverage spectrum that may be underused or unused by the current licensees in certain areas. Regulators looking to establish licensed shared access in certain bands should establish clear mechanisms for spectrum sharing that protect incumbent users while still maximizing the amount of spectrum available and the certainty for its use by other users.

Both static and more dynamic management of spectrum may be relevant, depending on the circumstances of the incumbent use in the band. Spectrum management costs to implement these solutions differ considerably and should be taken into account when deciding on the licensing arrangements.

Licence-exempt spectrum

In addition to licenses issued for exclusive or shared use of spectrum, licence-exempt spectrum is also important in spectrum management frameworks. Several applications operate in licence-exempt bands, including Bluetooth, Wi-Fi, radiofrequency identification (RFID), industrial, scientific, and medical (ISM) equipment, and other short-range devices. These bands are expected to continue to play an important role in the future, considering that Wi-Fi and IoT applications often operate in licence-exempt bands. Countries around the world have opened certain bands for unlicensed use, acknowledging their substantial benefits and the wide range of applications that operate in them.

The light regulatory burden of these spectrum bands supports innovation. Unlicensed use is especially important when considering the important role that Wi-Fi plays in offloading mobile network traffic and the expected increase in IoT use and breadth of IoT applications in 5G. Both the United Kingdom and the United States have released or are considering the release of additional bands for unlicensed use in the 6 GHz and above 100 GHz bands (Ofcom 2020a; Ofcom 2020b; FCC 2020b; FCC 2019b). Other countries are considering unlicensed use as a possible solution to rural broadband connectivity. For example, Argentina consulted on a proposition to allow unlicensed use on a secondary basis in rural areas with less than 100 000 residents (Resolution 21/2019).[10] Other countries, such as Kenya, have considered the use

[10] https://www.boletinoficial.gob.ar/detalleAviso/primera/221017/20191111.

of segments of unused broadcast television channels, known as TV white spaces, to provide broadband in rural areas.[11]

Regulators should consider the role of licence-exempt spectrum and the possibilities of releasing additional spectrum on a licence-exempt basis in certain bands to support future networks and applications using spectrum. Regulators should conduct due diligence to ensure coexistence with other users and establish clear guidelines and operating parameters for unlicensed use to avoid possible harmful interference.

Spectrum trading and leasing

The concept of spectrum trading and leasing is permitting a secondary spectrum market, in which licensed operators are allowed to trade their assigned spectrum usage rights to other users. About one in three countries allow the secondary trading of spectrum, mostly in Europe (ITU 2019d).

New business models and spectrum usage innovations

Active infrastructure sharing: joint networks

Especially with mobile networks, more operators are teaming up with competitors to share infrastructure and investment costs. This trend started because of the need to densify networks in urban centres, and also to fulfil coverage obligations in less-populated areas. Widely implemented for 3G and 4G networks, infrastructure sharing is especially important to reduce the costs of 5G network deployments. While cooperation is more commonly focused on passive infrastructure, there are some instances of sharing of active infrastructure, including spectrum resources. In Sweden, Tele2 and Telenor agreed to roll out a joint national network to provide 5G services and share spectrum through their joint company, Net4Mobility, including 2x10 MHz in the 700 MHz band. The two operators have cooperated in the past to deploy and operate a 2G and 4G national network and have updated their agreements to quickly build out the joint 5G network (Tele2 2018). Other examples of sharing of spectrum resources include radio access network (RAN) agreements, where operators agree to share their respective networks under defined terms. Mobile operators in France, Finland, Denmark, and Poland have undertaken sharing agreements, although these are often qualified with terms defining the geographic area of sharing and/or the timeframe of the sharing agreement (BEREC 2018, 10-11).

Such sharing arrangements allow operators to split the burden of network investment and shorten the time needed to deploy national networks. Many regulators are in favour of actions that encourage network deployment and investment, which aligns with the goals of spectrum sharing models. However, this model does have potential risks to competition, depending on the conditions of the sharing agreements, the extent of the joint activities, and the competitiveness of the market. However, these risks can be managed with regulatory oversight. For instance, spectrum sharing could be allowed only for a specific period, or until sufficient spectrum is released to avoid only one national network being deployed in a specific area and to encourage network redundancy and competition in the market. Other measures could be put in place to prevent the parties from acting like a merged entity or gaining dominance in the market, compared to other competitors. Regulators may consider allowing active infrastructure sharing

[11] https://ca.go.ke/public-consultation-on-the-draft-dynamic-spectrum-access-framework-for-authorisation-of-the-use-of-tv-white-spaces/.

to encourage a quicker deployment of networks and a shared burden of investment among operators.

Network slicing

In addition to new trends in spectrum licensing by regulators, new types of innovations are facilitating more efficient use of spectrum. Network slicing, a form of network virtualization made possible through software-defined networks and network function virtualization, for example, allows several service networks, or slices, to be served with the same physical infrastructure (OECD 2019, 28-29). This enables operators to provide different types of services per network slice, tailored to the necessary service characteristics, such as latency, speed, security, or reliability.

As mobile operators transition from 4G to 5G networks, network slicing can help them to use their spectrum and networks efficiently to meet network needs as more data-heavy 5G applications begin to be supported. Network slicing is expected to have most impact once 5G networks have been fully rolled out, when different 5G usage scenarios take root, and networking slicing can be applied on a large scale.

Spectrum repurposing and refarming

To maximize the use of spectrum and thereby better address spectrum demand from relevant stakeholders, regulators are undertaking administrative, financial, and technical measures to recapture spectrum and reassign it for new uses. Spectrum repurposing and refarming is not a new concept, but it takes on even greater relevance as countries seek to make more spectrum available to meet the spectrum demand of new services and technologies. Such approaches have considered both spectrum used for existing mobile technologies and spectrum used by other services. The main point is the optimization of the use of the same spectrum through the migration from older technologies (e.g. 2G) to newer technologies (e.g. 4G or 5G). For instance, 4G networks are about 15 to 30 times more optimized in the use of spectrum than 2G, and can be implemented in frequency bands that were originally designed for 2G, such as the 850 MHz, 900 MHz, and 1 800 MHz bands.

An overarching principle that can be applied to all licence types is the concept of technology neutrality. This would facilitate the migration from one technology to the next and remove regulatory impediments.

One high-profile repurposing target has been driven by the migration of television broadcasting from analogue to digital transmission, which enables the provision of improved television services while using less spectrum. The spectrum that can be repurposed from analogue broadcasting to other uses – referred to as the digital dividend – has been earmarked by many policy-makers for the provision of mobile broadband services. In fact, the creation of the digital dividend has been a major driver of digital broadcasting migration around the world, as about two-thirds of countries have already reallocated the digital dividend spectrum to cellular mobile services (ITU 2019d).

6.4 Key findings

The key findings from this review of best practices for applications and regulatory considerations that are driving the future use of spectrum are given below.

- In the context of constant technology innovation, an effective spectrum policy should be flexible enough to foster the deployment of different services. As new technologies and applications are developed, regulators should take them into consideration when looking at the future of their national spectrum management plans. Effective management of competing demands for spectrum is necessary to manage the data traffic demand increase. It also fully realizes the potential consumer benefits of new technologies, as well as broader social and economic goals, with the overall goal of enhancing and expanding the access to connectivity.
- Administrations should carefully consider the importance of spectrum management when defining how it is addressed within the government structure. It is important to have a well-established structure to bring transparency to the process, resulting in a more stable regulatory environment.
- In addition to longer licence terms to increase regulatory certainty for operators, regulators should be cognizant of operators' investment and deployment burdens to improve networks, as spectrum utilization fees may impact operators' ability to invest. Furthermore, regulators should consider streamlining the assignment process for certain applications that require little coordination and oversight, which can facilitate access and expand services in the country. Posting information with an up-to-date registry of spectrum assignments for different services and bands also facilitates access to the different frequency bands.
- There is a trend towards local licensing linked to the usage scenarios enabled by 5G, especially those for industrial applications that require high bandwidth and low latency over a small coverage area. This approach encourages the deployment of industrial 5G use cases while national 5G networks are being deployed at a more measured pace.
- Shared access regimes are a way for regulators to open spectrum that is currently used by incumbent services to new users. Licence-exempt spectrum bands have proven to be fertile ground for innovation, as evidenced by the importance of Wi-Fi and Bluetooth technologies in enabling new applications.
- An overarching principle that should be applied to all licence types is the concept of technology neutrality. Many regulators have adopted this approach to foster innovation and decrease regulatory restrictions.
- Finally, regulators should conduct a review of international best practices in terms of spectrum licences. This includes adhering to international and regional frequency allocation decisions, and worldwide technical standards, maximizing harmonization. This supports lowering the costs of equipment, and effectively enables roaming.

References

ACMA (Australian Communications and Media Authority). 2020. *FYSO 2019–23: Progress Report for July–Dec 2019*. April 24, 2020. Canberra: ACMA. https://www.acma.gov.au/fyso-2019-23-progress-report-july-dec-2019.

ACMA (Australian Communications and Media Authority). 2019. *Five-Year Spectrum Outlook 2019–23: The ACMA'S Spectrum Management Work Program*. Canberra: ACMA. https://www.acma.gov.au/publications/2019-09/publication/five-year-spectrum-outlook-2019-23.

Anatel (National Agency of Telecommunications). 2020. *Public Consultation No. 9*. https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2308&Tipo=1&Opcao=andamento.

Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2019. "5G: 3.4-3.8 GHz Band Frequency Awards Procedure: Arcep Invites all Players Wanting to Participate to Submit a Bid Package." Press Release. December 31, 2019. https://en.arcep.fr/news/press-releases/p/n/5g-10.html.

Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). 2020. "5G: The Companies Bouygues Telecom, Free Mobile, Orange and SFR Have all Qualified to Participate in the Auction for 3.4 – 3.8 GHz Band Frequencies. The Auctions Have Been Postponed Due to the Current Health Crisis." Press Release. April 2, 2020. https://en.arcep.fr/news/press-releases/p/n/5g-13.html.

BEREC (Body of European Regulators for Electronic Communications). 2018. *BEREC Report on Infrastructure Sharing*. Brussels: BEREC. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/8164-berec-report-on-infrastructure-sharing_0.pdf.

BNetzA (Bundesnetzagentur). 2019. "Frequency auction 2019." https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html?nn=268128.

BNetzA (Bundesnetzagentur). 2020. "Regional and Local Networks." https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/LokaleNetze/lokalenetze-node.html.

CTU (Czech Telecommunications Office). 2020. *Call for Comments on Draft Invitation to Tender for the Award of Rights to Use Radio Frequencies for the Provision of Electronic Communications Networks in the 700 MHz and 3 440-3 600 MHz Frequency Bands*. https://www.ctu.cz/vyzva-k-uplatneni-pripominek-k-navrhu-textu-vyhlaseni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k-7.

FCC (Federal Communications Commission). 2003. *Allocations and Service Rules for the 71-76 GHz, 81-86 GHz and 92-95 GHz Bands*. Report and Order: FCC-03-248. https://docs.fcc.gov/public/attachments/FCC-03-248A1.pdf.

FCC (Federal Communications Commission). 2019a. *Amendment of Part 15 Rules for Unlicensed White Spaces Devices*. Report and Order: FCC 19-24. Washington, DC: FCC. https://www.fcc.gov/document/amendment-part-15-rules-unlicensed-white-spaces-devices.

FCC (Federal Communications Commission). 2019b. *FCC Opens Spectrum Horizons for New Services and Technologies*. Report and Order: FCC 19-19. Washington, DC: FCC. https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies-0.

FCC (Federal Communications Commission). 2020a. "FCC Establishes Procedures for 3.5 GHz Band Auction." Public Notice. https://www.fcc.gov/document/fcc-establishes-procedures-35-ghz-band-auction-0.

FCC (Federal Communications Commission). 2020b. *Unlicensed Use of the 6 GHz Band*. Report and Order: FCC-CIRC2004-01. Washington, DC: FCC. https://docs.fcc.gov/public/attachments/DOC-363490A1.pdf.

FCC (Federal Communications Commission). 2020c. "FCC Adopts New Rules for the 6 GHz Band, Unleashing 1,200 Megahertz of Spectrum for Unlicensed Use." Press Release. April 23, 2020. https://docs.fcc.gov/public/attachments/DOC-363945A1.pdf.

Fujitsu. 2020. "Fujitsu Launches Japan's First Commercial Private 5G Network." Press Release, March 27, 2020. https://www.fujitsu.com/global/about/resources/news/press-releases/2020/0327-01.html.

García Zaballos, A. and N. Foditsch. 2015. *Spectrum Management: The Key Lever for Achieving Universality*. New York: Inter-American Development. https://publications.iadb.org/publications/english/document/Spectrum-Management-The-Key-Lever-for-Achieving-Universality.pdf.

GSMA. 2019. "EMF Policy." https://www.gsma.com/publicpolicy/consumer-affairs/emf-and-health/emf-policy.

GSMA. 2020. *The Mobile Economy China*. London, United Kingdom: GSMA. https://www.gsma.com/mobileeconomy/china/.

ICNIRP (International Commission on Non-Ionizing Radiation Protection). 2020. "Guidelines for limiting exposure to electromagnetic fields (100 kHz to 300 GHz)". *Health Physics 118*(5):483-524. https://doi.org/10.1097/HP.0000000000001210.

IMDA (Infocomm Media Development Authority). 2017. "2G Services to Cease on April 1, 2017." Press Release. March 27, 2017. https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2017/2g-services-to-cease-on-1-april-2017.

ITU (International Telecommunication Union). no date. *HAPS – High-Altitude Platform Systems*. https://www.itu.int/en/mediacentre/backgrounders/Pages/High-altitude-platform-systems.aspx.

ITU (International Telecommunication Union). 2008. *Supplement to Handbook on Spectrum Monitoring*. Geneva: ITU. https://www.itu.int/pub/R-HDB-53.

ITU (International Telecommunication Union). 2011. *Handbook on Spectrum Monitoring*. Geneva: ITU. https://www.itu.int/pub/R-HDB-23.

ITU (International Telecommunication Union). 2015a. *Handbook on Computer-aided Techniques for Spectrum Management (CAT)*. Geneva: ITU. https://www.itu.int/pub/R-HDB-01.

ITU (International Telecommunication Union). 2015b. *Handbook on National Spectrum Management*. Geneva: ITU. https://www.itu.int/pub/R-HDB-21.

ITU (International Telecommunication Union). 2016. *Radio Regulations*. Geneva: ITU. https://www.itu.int/pub/R-ACT-WRC.14-2019/en.

ITU (International Telecommunication Union). 2018a. *Economic Aspects of Spectrum Management*. Report ITU-R SM.2012-6. Geneva: ITU. https://www.itu.int/pub/R-REP-SM.2012.

ITU (International Telecommunication Union). 2018b. *Guidance on the Regulatory Framework for National Spectrum Management*. Report ITU-R SM.2093-3. Geneva: ITU. https://www.itu.int/pub/R-REP-SM.2093.

ITU (International Telecommunication Union). 2019a. *Methods for Determining National Long-Term Strategies for Spectrum Utilization*. Report ITU-R SM.2015. Geneva: ITU. https://www.itu.int/pub/R-REP-SM.2015.

ITU (International Telecommunication Union). 2019b. *Spectrum Monitoring Evolution*. Report ITU-R SM.2355-1. Geneva: ITU. https://www.itu.int/pub/R-REP-SM.2355.

ITU (International Telecommunication Union). 2019c. *The State of Broadband: Broadband as a Foundation for Sustainable Development*. Geneva: ITU. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

ITU (International Telecommunication Union). 2019d. *World Telecommunication/ICT Regulatory Survey*. Geneva, Switzerland: ITU. https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/RegulatorySurvey.aspx.

ITU (International Telecommunication Union). 2019e. *The Impact of RF-EMF Exposure Limits Stricter than the ICNIRP or IEEE Guidelines on 4G and 5G Mobile Network Deployment*. Recommendation ITU-T K. Series Supplement 14. Geneva: ITU. https://www.itu.int/rec/T-REC-K.Sup14-201909-I.

Lu, Q., J. Yang, Z. Jin, D. Chen, and M. Huang. 2017. "State of the Art and Challenges of Radio Spectrum Monitoring in China." *Radio Science* 52(10): 1261-1267. https://agupubs.onlinelibrary.wiley.com/doi/full/10.1002/2017RS006409.

MCMC (Malaysian Communications and Multimedia Commission). 2019. *Allocation of Spectrum Bands for Mobile Broadband Service in Malaysia: Final Report*. https://www.skmm.gov.my/skmmgovmy/media/General/pdf/FINAL-REPORT_ALLOCATION-OF-SPECTRUM-BANDS-FOR-MOBILE-BROADBAND-SERVICE-IN-MALAYSIA_20191231.pdf.

Mercer, D. 2019. *Global Connected and IoT Device Forecast Update*. Strategy Analytics. https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update.

MIC (Ministry of Internal Affairs and Communications). 2019a. *Approval of a Plan to Open a Specific Base Station for the Introduction of a 5th Generation Mobile Communication System (5G) (Summary)*. https://www.soumu.go.jp/main_content/000613734.pdf.

MIC (Ministry of Internal Affairs and Communications). 2019b. *Certification of Plan to Open Specific Base Station for Introduction of 5th Generation Mobile Communication System*. https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000378.html.

MIIT (Ministry of Industry and Information Technology). 2020. "The Ministry of Industry and Information Technology Permits China Telecom, China Unicom, and China Radio and

Television to Jointly Use the Indoor Frequency of the 5G System." Press Release, February 10, 2020. http://www.miit.gov.cn/n1146290/n1146402/c7671201/content.html.

MinTIC (Ministry of Information and Communications Technology). 2019. "Statement: Results of the Radio Spectrum Auction." Press Release, December 20, 2019. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/124713:Comunicado-Resultados-de-la-Subasta-del-Espectro-Radioelectrico.

MinTIC (Ministry of Information and Communications Technology). 2020. "MinTIC Issued the Resolutions that Assign the Permits to Use the Spectrum Blocks." Press Release, February 20, 2020. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/125966:MinTIC-expidio-las-resoluciones-que-asignan-los-permisos-de-uso-de-los-bloques-de-espectro.

OECD (Organisation of Economic Cooperation and Development). 2014. *New Approaches to Spectrum Management*. OECD Digital Economy Papers, No. 235. Paris: OECD. https://dx.doi.org/10.1787/5jz44fnq066c-en.

OECD (Organisation of Economic Cooperation and Development). 2019. *The Road to 5G Networks*. OECD Digital Economy Papers, No. 284. Paris: OECD. https://doi.org/10.1787/2f880843-en.

OFCA (Office of the Communications Authority). 2019a. *Guidelines for Submission of Applications for Assignment of Shared Spectrum in the 26 GHz and 28 GHz Bands*. Hong Kong: OFCA. https://www.coms-auth.hk/filemanager/statement/en/upload/515/gn132019.pdf.

OFCA (Office of the Communications Authority). 2019b. "Offer of Spectrum Assignments in the 26 GHz and 28 GHz Bands for Provision of 5G Services." Press Release, March 27, 2019. https://www.ofca.gov.hk/en/media_focus/press_releases/index_id_1891.html.

Ofcom (Office of Communications). 2005. *Spectrum Framework Review: Implementation Plan – Interim Statement*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/38162/statement.pdf.

Ofcom (Office of Communications). 2019. *Enabling Wireless Innovation through Local Licensing: Shared Access to Spectrum Supporting Mobile Technology*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0033/157884/enabling-wireless-innovation-through-local-licensing.pdf.

Ofcom (Office of Communications). 2020a. *Improving Spectrum Access for Wi-Fi: Spectrum use in the 5 and 6 GHz Bands*. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0038/189848/consultation-spectrum-access-wifi.pdf.

Ofcom (Office of Communications). 2020b. Supporting Innovation in the 100-200 GHz Range: Proposals to Increase Access to Extremely High Frequency (EHF) Spectrum. London: Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0034/189871/100-ghz-consultation.pdf.

PTS (Post and Telecom Authority). 2018. *Decision on Permission to Use Radio Transmitters in the 700 MHz Band*. https://pts.se/globalassets/startpage/dokument/legala-dokument/beslut/2018/radio/700-tilldelningsbeslut/tilldelningsbeslut-700-mhz-14-december-2018389611-0_tmp.pdf.

RU (Regulatory Authority for Electronic Communications and Postal Services). 2020. *Call for Tenders for Granting Individual Licenses for the Use of Frequencies*. https://www.teleoff.gov.sk/data/files/49605_call-for-tender.pdf.

Tele2. 2018. "Tele2 and Telenor Secure New Frequencies and Consolidate Joint Plan for 5G Network in Sweden." Press Release. December 10, 2018. https://www.tele2.com/media/press-releases/2018/tele2-and-telenor-secure-new-frequencies-and-consolidate-joint-plan-for-5g-network-in-sweden.

URSEC (Unidad Reguladora de Servicios de Comunicaciones). 2019. *Resolution No. 034/2019*. https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/sites/unidad-reguladora-servicios-comunicaciones/files/2019-05/034%20.%20ANTEL%20Tecnolog%C3%ADa%205G_0.pdf.

Wi-Fi Alliance. 2020. *20 Years of Wi-Fi*. April 17. https://www.wi-fi.org/discover-wi-fi/20-years-of-wi-fi.

Chapter 7. Regulatory responses to evolving technologies

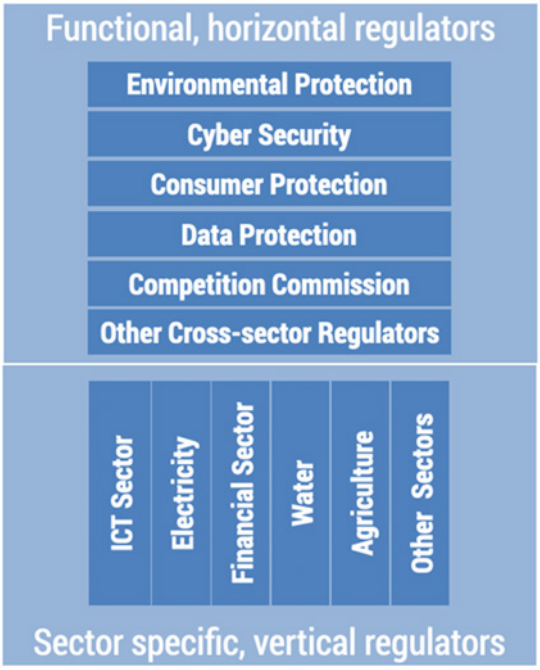
7.1 Introduction

The digitization of societies and economies is continuously generating record amounts of data. Digitization is driven by increased and faster connectivity of people and things. Fibre to the home (FTTx) and fast mobile networks provide the opportunity to engage in digital activities, and social media and user-generated content provide the motivation for it. At the same time, more objects become "smart", i.e. connected to the Internet to receive and send data. As a result of the explosion of data, new technologies have evolved that help to sift through data and derive value from combining and analysing large data sets. These technologies are often described in umbrella terms such as artificial intelligence (AI) and big data.

The new technologies require ICT regulators to reconsider the tools they deploy to facilitate fair competition in the ICT sector and protect consumers. New technologies also pose legal, ethical, and macroeconomic challenges. Central banks, consumer protection agencies, competition commissions, and ICT regulators scramble to assess the implications for their fields of responsibility. The implication is that roles of sector-specific regulators such as for the ICT sector, water, electricity, and banking, and subject-specific regulators such as a consumer protection agency or the competition commission may need to be redrawn and, in some cases, more specialized regulators may need to be established.

Figure 7.1 depicts how a sector specific ICT regulator is complimented by functional regulatory agencies that have responsibilities across all sectors of an economy.

Figure 7.1. The digital regulatory ecosystem

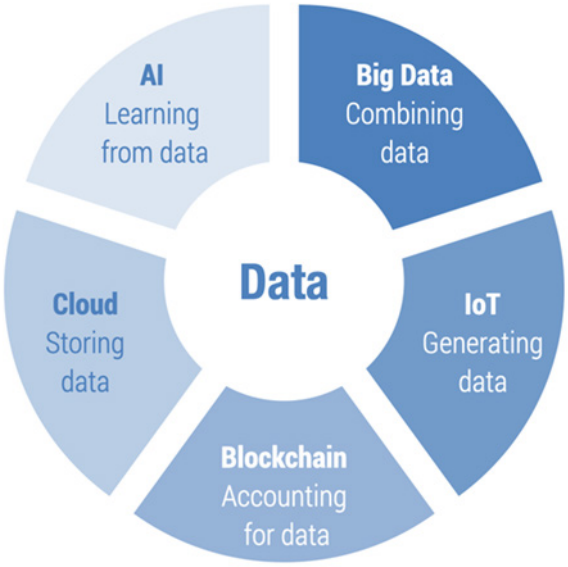


This chapter discusses the general trend in redefining the roles of the various regulatory authorities in response to cloud computing, AI, blockchain, big data, and the Internet of Things (IoT). While the desired outcomes – fair competition, consumer protection and economic development – remain the same, the approaches to achieve them are changing across time and differ between countries. This chapter aims to provide a framework to identify a suitable regulatory approach in response to arising technologies. The next section explains selected technologies in the context of the Internet value chain and evolving ICT sector business models. The last section discusses the evolving regulatory environment and options for allocating regulatory responsibilities to sectoral and/or functional regulators.

7.2 Evolving technologies

Blockchain, AI, big data, the cloud, and the IoT have in common that they all deal in one way or the other with data and that they facilitate new business models that may shift value creation within and between segments of the value chain. The IoT generates data (sensing and collecting), the cloud stores and processes data, big data derives data by combining large data sets, AI learns from data, including big data, and blockchain is a mechanism to reliably capture a data transaction history in a distributed manner (see Figure 7.2).

Figure 7.2. Linking technologies covered in this chapter



These technologies are different in that the IoT is subject to ICT sector regulations, while the others currently are not. While applications based on these technologies may be subject to ICT regulators or subject-specific regulators, such as data protection and consumer protection regulators and the entity in charge of cybersecurity, the technologies themselves are not. Cryptocurrencies, for example, use blockchain technology and the regulatory responsibility lies with central banks.

Cloud computing

Cloud computing converts IT infrastructure and software into services, delivered over the public Internet, including servers, storage, networking, software and data analysis. Cloud computing allows businesses to upscale and downscale the computing and networking power available to them within a few minutes. Cloud computing includes vendors that offer storage as a service, such as Dropbox and iCloud, and companies that focus on file transfer such as WeTransfer. Streaming services such as Netflix and YouTube and social media applications such as TikTok and Facebook all use cloud-based infrastructure.

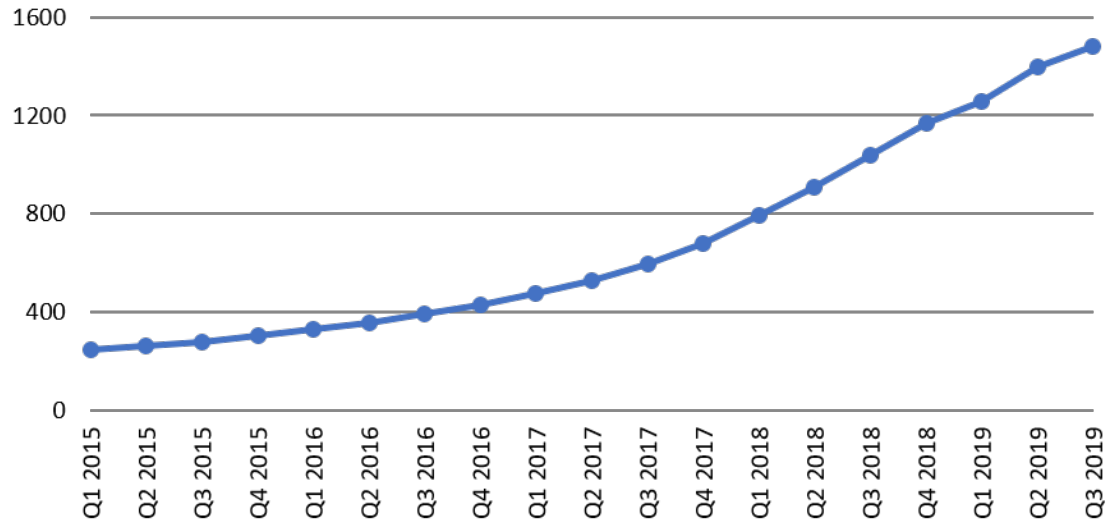
The International Telecommunication Union (ITU) (2018b) defines cloud computing as a "[p]aradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand".

In a sense, computing has come full circle. It started with centralized computing, with mainframe computers and dumb terminals, transitioned to individualized computing with personal computers (PCs) and laptops, and has now returned to centralized infrastructure (cloud computing) with smart terminals and devices, including smartphones and tablets. Cloud computing is part of the Internet value chain and regulatory issues are mainly related to data and consumer protection across multiple jurisdictions.

Internet of Things

The IoT is an umbrella term for technologies that allow objects to communicate. Ofcom defines it as the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.[1] The IoT includes close range technologies, such as passive radio-frequency identification (RFID) and near-field communication (NFC); and technologies that cover large distances such as machine-to-machine (M2M) communication. M2M uses standard subscriber identity module (SIM) cards for identification and authentication on mobile networks. Figure 7.3 displays the number of SIM cards that are being used for IoT connectivity in the world. Ericsson's Mobility Report (Ericsson, 2019) estimates that there will be 25 billion IoT devices in 2025.

Figure 7.3. Global connections, licensed cellular IoT (millions)



Source: GSMA Intelligence.

The IoT value chain is shorter than the Internet value chain, consisting of three to four segments (BEREC 2016):

- The **IoT service provide**r is the company that incorporates the IoT in its products or services, for example, a car manufacturer or an electricity provider.
- The **IoT connectivity provider** could be a mobile operator or an Internet service provider (ISP) whose Internet connection is being used via Wi-Fi like Amazon's Alexa or the Apple Watch.
- The **IoT user** purchases the IoT embedded product or service. Products and services can be combined or purchased separately. A car manufacturer could have a free tracking service included for a specific period of time or for the life of the car or charge for it separately.

[1] Definition of IoT, https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/internet-of-things . ITU Recommendation ITU-T Y.2060 provides an overview of the Internet of things (IoT) and more detailed definition: "Internet of things (IoT) is defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications." https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 .

The use of the IoT has several regulatory requirements:

- Spectrum use of the IoT needs to be regulated. Other than using SIM cards, IoT objects can communicate at different frequencies using Wi-Fi, NFC, or RFID. NFC can use the 300 MHz-3 GHz spectrum range, for example. RFID may be used in a low-frequency band of 125-134 kHz or at 13 MHz (ITU 2016).
- Competition issues revolving around customer lock-in resulting from fixed SIMs in devices. The costs of number portability in terms of switching mobile providers for IoT objects might be prohibitive. BEREC (2016) believes that the current number portability regulations might not be appropriate and new flexible approaches need to be developed.
- Data protection is paramount for the IoT. Who owns the data generated and what are the legal obligations for the data owner in terms of data use, storage, and liability for data breaches?
- Roaming may need to be addressed for IoT deployment using SIM cards. IoT devices may require permanent roaming across multiple jurisdictions (e.g. cars with built-in trackers). The question is whether roaming regulations apply to IoT objects. For the European Union (EU), for example, should IoT objects be subject to the principle of "roam like at home"?
- BEREC (2016) argues that if the number of roaming connections were to suddenly multiply, this might lead to access issues.

Addressing and numbering issues can be resolved by the adoption of eSIM cards that identify devices by international mobile subscriber identity (IMSI) and allow online switching of providers. The GSMA has produced a standard for eSIMs.[2]

The eSIM will bring new wholesale opportunities, including for companies that are not in the connectivity business. Private networks, e.g. in mines or ports, can have their own eSIMs, thus increasing security and controlling data use for specific applications. Hotel chains and hospitals could provide e-SIMs for their customers/patients with a set data allocation. IoT service providers can offer their products with data included and customers can top-up conveniently online, or change their provider while on holiday or when moving to another city.

Big data

Big data can be summarized as deriving value out of combining large data sets. Big data is a combination of various data sources and of data with different properties. UNSTATS (2015) describes the data characteristics in terms of volume, velocity, variety, the number of variables, veracity, selectivity, structure, and frequency (event-based or continuous). Big data is often described in terms of these "V" attributes (ITU 2014):

- **Volume:** Large data sets can come from a large number of sources such as call destination records (CDRs) from mobile phone calls and smart devices (IoT).
- **Velocity:** Velocity refers to the speed of data generation. Audited annual financial reports have a new record after 12 months. Supermarket sales records for a product can occur many thousand times a day.
- **Variety:** Data comes in different formats and types. It can be structured data from stock exchanges or unstructured data from text documents, emails, videos, audio recordings, and so on.
- **Veracity:** Veracity refers to the quality of data with some data being more reliable than others. An example of veracity of data is the difference between election opinion polls and election data, the latter having higher veracity.

[2] Embedded SIM or embedded universal integrated circuit card (eUICC), https://www.gsma.com/iot/embedded-sim / .

- **Value:** Data has intrinsic value, which only materializes once the value is discovered and utilized.

Table 7.1. Sources of big data

Data types	Examples
Administrative data	Administrative data are the data collected by the state, e.g. tax payments, birth certificates, social security numbers and contributions.
Survey data	The state conducts a serious of surveys throughout a year and some in cycles of five or 10 years. Examples include the census, labour force surveys, health surveys, and multipurpose household surveys.
High-frequency data	The private sector collects a wide range of high-frequency data. Examples include: • CDR from mobile operators • Supermarket and online purchases • Bank and credit card transactions • Transactions from stock and commodity exchanges • Road and traffic sensors • Weather stations • GPS tracking devices • Online search and social media activities and page views
Unstructured data	Text documents, videos, pictures are examples of structured data Blogs and posts and other authored and unauthored online content
Geospatial data from satellites	Infrared imagery, to estimate population, for example

Big data can be used to estimate ICT indicators for monitoring development targets in the ICT sector. It can also be used by mobile network operators (MNOs) to reduce churn, optimize networks, and provide better customer support:

- Churn prediction and individualized top-up packages and rewards are office tools to reduce churn. Acquiring a new customer is more expensive than retaining an existing customer. Big data, via the combination of customer usage, complaints, transactions, social media, and customer segmentation, can help identify customers that are likely to leave and design products/services that meet their specific needs (Deloitte 2015).
- Network optimization: operational expenses are a significant cost to operators. The upgrade to 5G could also require more base stations and managing the network will be more complex. In Nigeria, network and infrastructure maintenance costs for MTN are nearly 52 per cent. Big data analytics can be used to improve the performance of networks, by comparing real-time data with historical data (MapR 2020).
- Chatbots are widely used across the world by mobile operators for customer support. Chatbots can improve customer service.

Since big data involves the combination of different data sets, it is increasingly likely that the resulting data are able to identify individuals. Various data sets may also have different levels of consent and obligations for data owners, which heightens the need for stringent data protection laws.

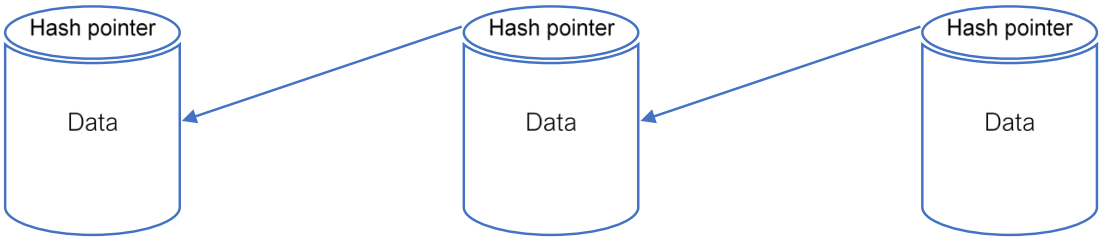
Blockchain

Blockchain is a technology that links records, called blocks, in a sequence using cryptography. Each record contains a set of information including a timestamp, who is participating in the transaction, and two unique identifying codes called a hash. A record contains the hash of the previous record as well as a hash for the current record, thus establishing a chain (see Figure 7.4). It is a type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision (ITU 2019a). The distributed verification process makes blockchains resilient and nearly impossible to tamper with since there is no single point of failure. Even better, it becomes increasingly difficult to alter as further blocks are added to the chain.

An important distinction is between private and public blockchains. A public blockchain is also referred to as open or permissionless and allows anybody to join the network as a node and store a local copy of the ledger (Michels 2018). In contrast, in private blockchains (permissioned), data processing is restricted to a closed group of nodes.

Blockchain technology is not subject to any regulation in the same way that Hypertext Transfer Protocol Secure (HTTPS) or 3D printing is not subject to regulation. Blockchain is a technology that can be used for applications in a wide variety of sectors and with different properties and functionalities. A regulatory response may be needed depending on the sector and the use of blockchain technology.

Figure 7.4. Blockchain



Bitcoin, for example, is a decentralized digital currency that uses blockchain technology. Its use poses challenges with regard to preventing money laundering and fraud. Since the ledger is distributed across computer networks around the world, it would be difficult to stop transactions and/or inspect them only within one jurisdiction. Collaboration across jurisdictions is thus important.

Bitcoin was the first application of blockchain technology as a cryptocurrency. Since then many other cryptocurrencies have been launched but also non-currency applications are being tested. An ITU (2019b) report on distributed ledgers summarizes more than 50 blockchain use cases, including applications in the ICT sector. Recent examples of blockchain ICT sector implementation include:

- The Telecommunications Regulatory Authority of India (TRAI 2018) requires telecommunication to use blockchain-based technologies in creating a "do not disturb" registry to prevent spam. In the regulation, TRAI refers to distributed ledger technology (DLT) and blockchain is one type of DLT.
- Identity and data management: blockchain can be used to maintain trust and security among the billions of sensors that will be connected to the network (e.g. smart fridges, Wi-Fi routers, smart watches, and so on).

- Ofcom is holding a trial for blockchain technology to manage U.K. landline telephone numbers.[3] Blockchain is being trialled to improve the number portability process. Number ownership management and voice call routing can be created by capturing the parties to number porting and time swaps in a record (or block).
- The ID2020 Alliance[4] aims to develop a new global model for the design, funding, and implementation of digital ID solutions and technologies. Blockchain, along with biometrics, is being explored for this.[5]
- Deloitte (2016) released a report listing business opportunities for mobile operators and ISPs based on blockchain technologies. One application is to store cell-level network performance in blockchains to analyse network performance.

While regulatory concerns differ for each blockchain application, some issues, like data protection, will apply across most blockchain applications. Public blockchains allow anyone to see the entire transaction history, which may have data protection implications based on what information is recorded in the blocks. Private blockchains raise questions on the ownership of the data and the obligations for the data owners.[6]

Sector-specific regulation may be required for certain applications. Central banks are responsible for cryptocurrencies and would need to ensure compliance with money laundering regulations.

An example of the need for an ICT regulator to intervene may be when an operator abuses its market power by charging high prices based on its market power for services derived from a combination of blockchain-based digital IDs, eSIMs, and mobile money accounts. The emphasis must be on the abuse of market power. Existing legislation and regulation already prohibits the abuse of market power by dominant operators. In this instance, the tools to intervene in the market already exist and do not need to be reinvented.

Artificial intelligence

The Internet Society (2017) defines AI as "artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language". It refers to systems that are designed to mimic human abilities to understand and solve problems. AI has many applications including predictive maintenance for cars and chatbots for customer support.

The ITU (2018a) notes that AI includes five "technologies:" computer vision, natural language processing, deep learning, robotics, and other automation systems. Limitations for deploying AI revolve around obtaining sufficiently large data sets, the ability to explain and generalize results from AI systems, and the risk of bias (ITU 2018a).

AI tools are what makes it feasible to process big data. The regulatory requirements are thus closely related to that of big data. However, further regulation may be needed because of the risk of bias that may stem from the data and algorithms used (McKinsey 2018). Additional steps may be required to resolve the risks of bias that go beyond the data and the algorithms.

---

3 Ofcom, How Blockchain Technology Could Help to Manage U.K. Telephone Numbers, https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/blockchain-technology-uk-telephone-numbers.

4 https://id2020.org/alliance .

5 ID2020: Digital Identity with Blockchain and Biometrics, https://www.accenture.com/us-en/insight-blockchain-id2020 .

6 A report by the ITU (2019b) provides more details on regulatory implications of specific applications of blockchain technology.

There is a risk that the collected data have a selection bias or that it reflects societal biases and therefore hardwires injustices into a system. A famous example is the case of the U.S. Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm that predicted black offenders to be 77 per cent more likely to reoffend than whites, with all other factors being similar.[7] Knowing the underlying bias in society, this could have been avoided by omitting race as one of the variables used to feed the learning algorithm. What is more important, though, is how this bias was discovered. It required an organization that was concerned about the outcomes and a mechanism to request the underlying data, which was done through a freedom of information request. The ability to detect biases will become more difficult with time as algorithms become more complex.

Regulators need to consider ways to address the "black-box" problem, where algorithms make decisions or give recommendations and the people affected by them have no way of understanding how these decisions and recommendations were derived (Deloitte 2018b). The EU, in response to these issues, formulated seven key requirements for AI regulation in a white paper that includes non-discrimination and fairness (European Commission 2020).

The General Data Protection Regulation (GDPR) of the EU, in Article 22, gives consumers the "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[8] This means that every consumer has the right to know what the data and underlying rationale are for making a decision, if it was an automated decision. For example, if a consumer is denied a loan based on an automated profile, the consumer can request the bank's rationale.

However, the application of data protection and AI opens up a range of challenges. In the EU, the GDPR requires that data processors only use the minimum amount of data necessary to make the decision. The EU is trying to draw limits on the amount of data used and to limit the invasion of privacy. This is more complicated than it seems because the EU has not clearly defined what constitutes the required minimum. At the same time, other jurisdictions do not have this limitation so companies can use as much data as they like, potentially putting EU firms at a disadvantage and reducing innovation in the AI sector.

Similarly, every EU citizens has the right to see the raw data prior to profiling as well as the results after profiling (Article 15 of the GDPR). Unscrupulous companies could get access to the results of the profiling and reverse engineer the algorithms utilized by the initial company. These challenges show that considerable work has to be done to refine traditional regulatory tools to address the complexities of technologies like AI and their impact on issues like data protection.

The key question for the EU and regulators, in general, is whether the current data protection framework can create and maintain trust among suppliers and consumers. More stringent rules may be a competitive disadvantage on one level but, through the trust that is being built, achieve a competitive advantage on another level.

Smart capabilities and data protection

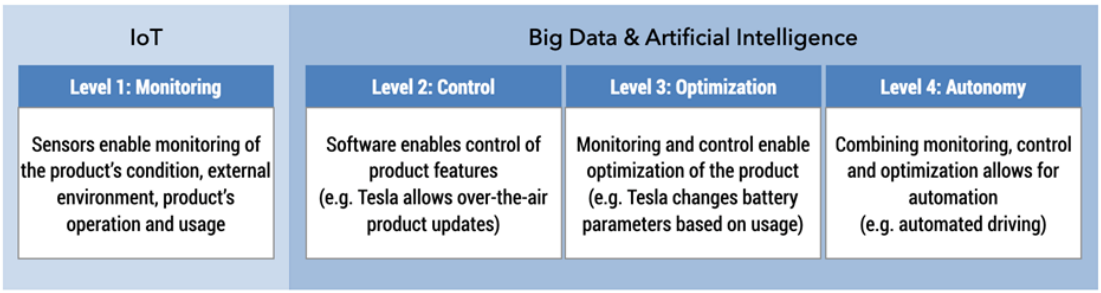
Technologies such as the IoT, AI and big data allow for the development of new capabilities for products and services. In Figure 7.5, IoT sensors monitor product usage, sending that data to

[7] How We Analyzed the COMPAS Recidivism Algorithm, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm .

[8] https://gdpr-info.eu/art-22-gdpr/ .

the manufacturer for processing for updates or improvements. Manufacturers have a level of control over the features of the product. Tesla, for example, can change the battery range of a car via a software update, as it did for drivers caught in Hurricane Irma in 2017 (Liptak 2017). The combination of control and monitoring means that product performance can be improved or optimized. Monitoring, control, and optimization enable automation, which is dependent upon the learning capabilities of artificial intelligence.

Figure 7.5. Capability approach



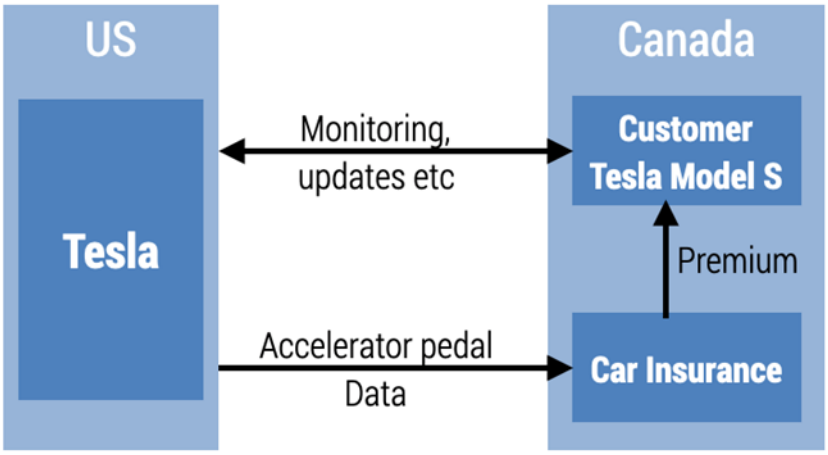
Source: Modified from Porter 2014.

The smart capabilities of products and services will create new models for collaboration that will need to address multiple, sometimes contradictory objectives: the protection of individual privacy versus the benefits of sharing knowledge across borders and industries.

There are already initiatives to foster collaboration across the value chain. Telecommunication and financial services have been collaborating on the regulation of mobile money. Similarly, Google and Apple's recent announcement that they would partner to develop an open-source Bluetooth-based contact tracing technology for the COVID-19 pandemic that will require collaboration between public health authorities, ICT regulators, data protection agencies, and governments.

Moving data across jurisdictions has consequences for how to protect and share that data. Take a car company like Tesla that sells its cars entirely online, bypassing the traditional auto-dealer network, for example. Once the car is delivered to the customer, Tesla can monitor the status of the car and the car can either remotely call Tesla to schedule repairs or send a notification to the customer. It is not hard to imagine a scenario where usage data could be captured to provide tailored products to owners. Careful and calm driving behaviour could be rewarded by bigger discounts on car insurance. Pressing the accelerator aggressively by the driver could see an increase in insurance premiums because of the increased risk of an accident (see Figure 7.6).

Figure 7.6. Illustrative example of a Tesla sale across borders and third party use of data



In this scenario, the data protection and privacy implications across so many different segments of the value chain require collaboration between different regulators. How should data be protected when they are collected using mobile networks (overseen by the ICT regulator), shared with insurance companies (overseen by the financial services regulator), and shared with car manufacturers (regulated by transport and safety authorities)? What recourse do consumers have if they do not want their car usage data shared with third parties like insurance companies? This complexity is exponentially increased in a scenario where a Canadian resident orders a Tesla from the United states online.

Data protection as the common denominator

AI, big data, and the IoT all require regulators to address five questions (Deloitte 2018b):

- Who owns the data that are being collected?
- What obligations does the owner of the data have in terms of storing and protecting that data?
- Can collectors of data price discriminate for users that agree that their data can be used versus those that have not provided consent?
- Do citizens have the right not to be evaluated by algorithms?
- May citizens request access to the data that were used to derive a decision or recommendation that affects them?

Essentially, data protection is about privacy.[9] Many countries consider the right to privacy to be a fundamental human right. More important, an actual or perceived lack of privacy results in consumers being resistant to new things (such as smart wearables like a smart watch) and generally risk-averse behaviour. Accenture (2016) found that 47 per cent of consumers had concerns about privacy and security preventing them from purchasing smart devices. Assuring consumers that their personal data belongs to them and they can control their use is a prerequisite for consumers to trust online transactions. When it comes to data protection, the first requirement is that the following high-level principles must exist in some form:

- Personal Information must be defined to relate to any information about an identifiable, living, natural person.

[9] See Chapter 5 on "Data protection and trust" for an examination of on the regulatory aspects of data protection.

- Organizations[10] must be responsible for the personal information they collect.
- Organizations must state what they will use the personal information for and that those uses are reasonable.
- Organizations must use the personal information they need, not the personal information they want.
- Consumers[11] must know when and which organizations collect personal information about them and must consent to what organizations do with that data.
- Organizations must take reasonable steps to make sure the personal information is safe and, if there is a security breach, they need to inform consumers and help limit the damage.
- Organizations must do their best to ensure that the personal information they are entitled to have is of good quality.
- Some personal information, like biometric information and personal information about children, is more sensitive and must be subject to additional protection.

The data protection ecosystem consists of laws, institutions, and industry and consumer forums. Table 7.2 provides a framework to assess the data protection ecosystem for a country. Any questions answered with "no" provide an opportunity to improve the framework.

As the data protection checklist highlights, the existence of appropriate legislation is necessary but not sufficient. The implementation of data protection legislation and regulation requires funding to both educate about and enforce data protection legislation. In developing countries, this is a significant challenge. The economic and social benefits that new technologies can bring are premised upon consumers having trust that their data are protected and that they have some level of control.

[10] Organizations and individuals can collect data. In legal terms, organizations/individuals that collect data are referred to as data controllers. The term "data controller" comes from the EU's GDPR and is defined as "a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body)" (https://www.atinternet.com/en/glossary/data-controller/).

[11] In legal terms, a consumer is known as a "data subject". The term data subject comes from the EU's GDPR and is defined as "any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected" (https://www.atinternet.com/en/glossary/data-subject/).

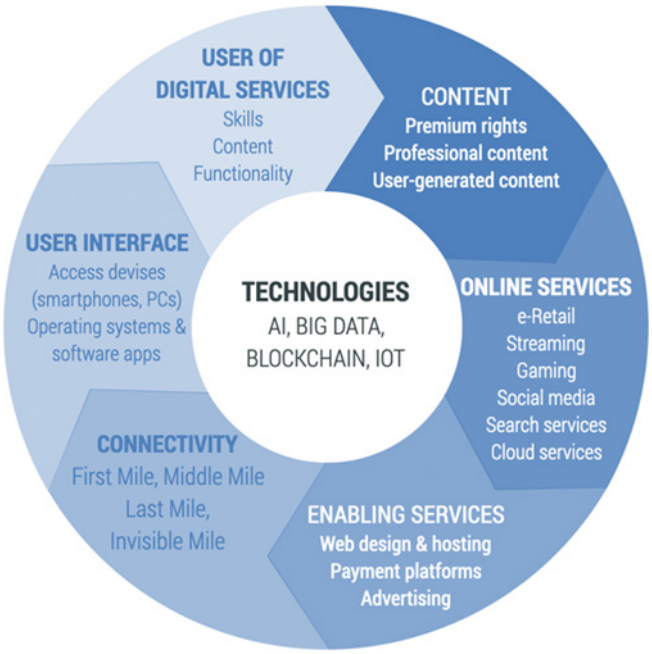
Table 7.2. Data protection ecosystem

Data Protection Checklist			Yes	No
Does your country have a data protection law?				
Data Protection Law	Personal data	Does the definition of personal information include all aspects? Is personal data of organizations included? Is personal data of dead people included?		
	Accountability	Is it clear who the data controllers are and what they are responsible for?		
	Purpose	Are the lists of acceptable purposes consistent with other countries?		
	Minimality	Are organizations (or data controllers) forced to only use the personal information they need?		
	Notification/ openness	Are consumers (data subjects) told that their personal data are being used and given a chance to object to the use? What is the notification procedure in case of security breaches?		
	Security	Is security a standard requirement and is the recurring security loop explained?		
	Quality	Must organizations (data controllers) have a strategy in place to ensure that their data quality is good?		
	Sensitive personal data	Is sensitive personal data treated more carefully?		
	Data protection authority	Is there a specific independent body tasked with enforcing data protection and do they have enough funding and capacity?		
	International cooperation	Does the law set out that cooperation with international data protection authorities is required?		
	Direct marketing	Does the law regulate direct marketing without stopping it altogether?		
	Codes of conduct	Are there mechanisms to work with industry and concerned civic society groups to allow for self-regulation where appropriate?		
Is data protection law adequate to cope with the way data are being used by evolving technologies?				
Does the regulating authority have sufficient expertise and funding to educate and enforce the data protection law?				
Does the regulating authority have sufficient jurisdictional power and international cooperation to operate in multiple countries with multiple regulating authorities?				
Does a freedom of information request mechanism exist?				

7.3 The evolving Internet value chain

Cloud computing, AI, big data analytics and blockchain are all part of the Internet value chain. Kearney[12] compiled an Internet value chain analysis in 2010 and the study was updated in 2016 for the GSMA.[13] The study distinguished five segments of the Internet value chain GSMA (2016a). For this Handbook, the Internet value chain has been extended to include the demand for digital services, which includes Internet access. Now the Internet value chain is seen not as a traditional set of sequential components but rather as a self-reinforcing circle (see Figure 7.7).

Figure 7.7. Internet value circle



These six components are:

- **Content rights:** Includes premium rights with content that is produced professionally. It also includes user-generated content which is made available via social media platforms, such as YouTube, Twitter, Instagram, Vimeo, and Facebook, amongst others.
- **Online services:** Covers a wide range of services provided over the Internet including e-commerce; entertainment (gaming, gambling, video, music, publishing); search and reference services (Wikipedia, Google, Yahoo); social media and cloud services.
- **Enabling technologies:** Consists of essential services for the smooth running of the Internet such as the design and hosting of websites; payment platforms (credit cards, PayPal, MPESA), platforms enabling machine-to-machine (M2M) based services; advertisement platforms (ad exchanges and brokers).
- **Connectivity:** The connectivity segment can be distinguished between first, middle, last and invisible miles. The first mile refers to international data connectivity, i.e. how a country connects to the rest of the world via the Internet. The middle mile encapsulates national data connectivity including fibre networks and data centres. The last mile represents wireless or wired end-user access. The invisible mile captures regulatory and legislative factors that impact the ICT sector.

[12] Internet value chain economics, https://www.kearney.com/communications-media-technology/article?/a/internet-value-chain-economics .

[13] https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf

- **User interface:** Devices used by the end user to access the Internet include smart and feature phones; PCs, laptops and tablets; as well as digital TVs or digital set-top boxes. Operating software (OS) for these devices also falls into this segment as well as applications that run on top of the OS.
- **Use of digital services:** The demand for digital services depends, apart from disposable income and availability of connectivity, on skills of users, the desirability of content, and functionality.

In the past, the data flow was from content owners to the end user via the public Internet. Today, users create content through social media applications and other ways of uploading data, thus contributing to the content that is being consumed.

The Internet value chain combines various previously unrelated industries together on one platform, not just within a country but globally. To give just a few examples:

- Telephony started as voice calls, were enriched with texting, and now may be video calls over the public Internet.
- Shopping started at farm gates, moved to local markets, and now to online marketplaces.
- Shows and plays started on stages, moved to television and DVDs, and are now content on demand.
- Bookkeeping is increasingly automated via mobile apps and online services.

Traditionally TV and movie content had their own delivery channel. Today, the Internet is the unifying content delivery platform. The broadcasting business model remains the same, based on subscriptions or advertisements, while the mode of delivery is increasingly shifting to the IP platform. This has advantages for consumers who are now able to control what, when, and where to watch, instead of having to plan their entertainment time around the programming schedule of broadcasters.

Cloud computing, big data, blockchain, and AI enable value creation from the self-reinforcing Internet value circle. These technologies can profile users in terms of the content they consume and the content they produce, allowing online services to be individually targeted. The ability to provide targeted content, services, and advertising provides opportunities for a customized usage experience and new services and new business models. This also applies to the connectivity segment of the value chain, in particular for fixed-line and mobile operators, which are discussed in the next section.

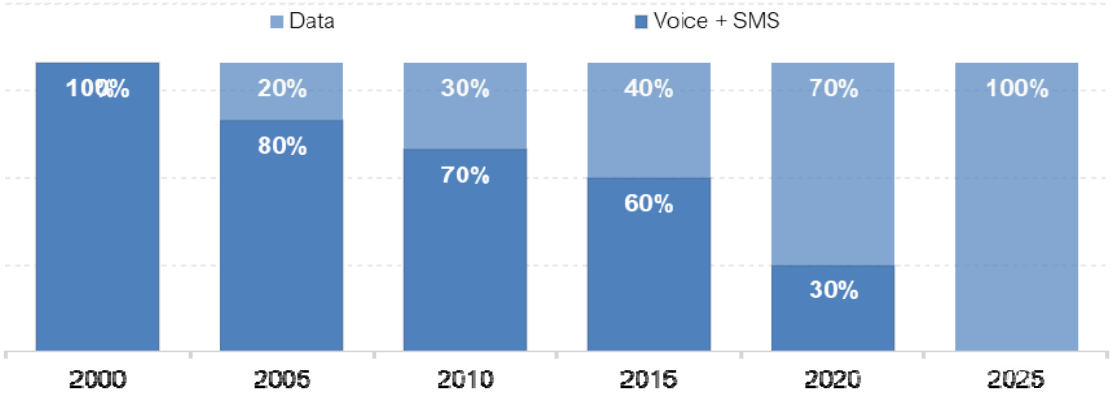
7.4 Evolving business models in the ICT sector

The increasing digitization of the way we work and live also impacts the way we communicate. Instead of making traditional voice calls and sending 160 character SMS messages, people can communicate more conveniently, with full video and in groups using Internet applications. Services that were previously provided by MNOs are seeing competition from the public Internet. Voice calls and SMS have to compete with over-the-top (OTT) applications, such as Skype, WhatsApp, and Facebook Messenger. Cryptocurrencies based on blockchain technology may compete with mobile money. The business models of domestic connectivity providers need to adjust to these new services, as do regulators, who have to reconsider their scope of responsibilities.

MNOs are mobile ISPs and data are the primary source of revenues. The mobile business model will follow that of fixed-line operators, which started out as voice service providers but

now make their money mostly from data connectivity, either retail or wholesale. Over the past two decades, the majority of MNO investment has gone into data networks. The transition from a voice and SMS to datacentric-business model is inevitable (see Table 7.3). MNOs will eventually entirely become mobile Internet access providers, distinguishing their products by speed and quality of service, and competing with other forms of access, such as Public Wi-Fi and connectivity in places of work, study and home. MNOs will no longer charge for voice and SMS, only for bandwidth and/or data consumption. The mobile ISP business model can also be described as a data-centric or a digital business model. Figure 7.8 illustrates this transition.

Figure 7.8. Illustrative trends towards digital mobile business models



Source: Esselaar and Stork 2019.

Apart from competitive pressure, the trend described in Figure 7.8 also depends on smartphone penetration and 3G+ network coverage. The migration to a digital mobile business model will take longer for countries that have little 3G, 4G, and public/private Wi-Fi coverage and low smartphone penetration. Insufficient 3G+ network coverage is one of the main reasons why some mobile operators struggle to generate enough data revenues to compensate for declining voice and SMS revenues.

Table 7.3. The evolving digital business model is inevitable

	Analogue mobile	Digital mobile
Business model	Service	Connectivity
Metric	Minutes and SMS	Bandwidth or throughput
Cost sensitivity	Distance, duration and location matter	Time, distance and location insensitive
Billing	Access and usage billing: Detailed billing systems for voice and SMS that can distinguish between off-net/ on-net, peak/off-peak	Simple access billing
Traffic monitoring	Detailed traffic monitoring as part of the billing system	Usage monitoring limited to data use
Postpaid subscribers	Detailed vetting to reduce risk or revenue loss and expenses that arise from call termination and subsidized handsets	• Postpaid risk limited to revenue of one billing cycle • No external expense risks • Prepaid and postpaid do not need to be distinguished by pricing • Postpaid may be extended without significant vetting
Network infrastructure	GSM 1G and 2G	2.5G, 3G, 4G, 5G

Source: Esselaar and Stork 2019.

The digital business model is all about knowing the customer. The actual battle is not that of cannibalization of one product for another, i.e. replacing voice and SMS with data revenues, but one of maintaining information on subscriber leadership. For years, MNOs were in the lead, knowing where their customers were in space and time, whom they communicated with and when. While this information is still available to MNOs, social media and online shopping provide a more potent and detailed information source. The information that Amazon and Facebook have about a customer is likely to be more economically valuable than the information that an MNO has about the same customer. To enter this market is a business decision, not a regulatory decision.

EBITDA margins along the Internet value chain show that end-user access is still a profitable business. More important than the size of each segment in terms of revenues is the profitability of major players in each of the value chain segments. Table 7.4 displays the earnings before interest, taxes, depreciation, and amortization (EBITDA) margin for selected players for each of the value chain segments. On average, EBITDA margins for connectivity are higher than the other segments of the value chain. It would be difficult to argue that MNOs are facing more adverse conditions than other segments. The variance of EBITDA margins between segments also shows that each segment has its own value proposition, investment criteria, and returns. Netflix is, for example, much more profitable than Disney.

Table 7.4. EBITDA margin along the value chain based on audited financial statements (%)

Segment	Company	2016	2017	2018
Content rights	**Netflix**	60	61	59
	Warner Media	–	–	18
	Disney	30	30	29
	Fox Corporation	–	–	22
Online services	**Amazon**	9	9	12
	Alphabet	33	30	26
	Facebook	53	57	52
Enabling technologies	**Cisco**	30	30	31
	Akamai	41	37	40
Connectivity	**Airtel Group**	35	38	37
	Etisalat	50	50	49
	Maroc Telecom Group	48	49	50
	MTN Group	35	33	35
	Ooredoo	41	42	41
	Sonatel	49	47	45
	Safaricom	42	48	48
	Vodacom Group	38	38	38
	Average Connectivity	42	43	43
User interface	**Apple**	33	31	31
	Samsung	24	31	35

Source: Esselaar and Stork 2019.

As MNOs transition into a fully datacentric model, they can expect their profit margins to decline to the levels of other segments of the value chain. The transition to a datacentric model also means less need for ICT sector-specific regulation. With the exception of the radio spectrum, telecommunication regulation will become less sector specific over time.

7.5 Summary

Evolving business models and technological progress mean that regulatory tools and institutional arrangements may have to change and regulatory oversight may be shifted to new or different organizations (see Figure 7.9). While the line ministry was an adequate supervisory body for landline monopolies, sector-specific regulators were needed as soon as ISPs and MNOs entered the market. The transition to an all-digital, all-IP world means that laws, policies, and regulations need to evolve to maintain fair competition. This has consequences for national regulatory institutions including ICT and broadcasting regulators, competition commissions, and consumer protection agencies. Big data, AI, and the IoT are driving the need for a redesign of the regulatory landscape because these technologies are able to combine, analyse, and utilize disparate sources of data, providing insights that do not only apply to one sector but across sectors and not only to one jurisdiction but to many. New, highly specialized regulatory institutions are increasingly required to deal with the issues that arise from the globalization of personal data, especially in terms of protecting personal data and resolving consumer disputes.

Figure 7.9. Changing regulatory approaches over time

Any application based on the technologies in this chapter is subject to horizontal regulation by agencies responsible for consumer protection, data protection, competition, cybercrime, and so on. Whether or not ICT sector-specific regulatory oversight is warranted depends on the functionalities of the applications and how they are used in a sector. The priority must be to have a robust horizontal regulatory ecosystem in place. This may require updating laws and establishing new agencies.

Given the cross-border nature of the Internet value chain, in particular of online services, collaboration and harmonization across jurisdictions is key to facilitate the digitization of economies and societies and the benefit of economic growth and social development that this brings.

References

Accenture 2016. *Igniting Growth in Consumer Technology*. https://www.accenture.com/t20151231t013104__w__/us-en/_acnmedia/pdf-3/accenture-igniting-growth-consumer-technology.pdf .

BEREC. 2016. *BEREC Report on Enabling the Internet of Things*. BoR (16) 39. https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-%20the-internet-of-things .

Deloitte. 2015. *Opportunities in Telecom Sector: Arising from Big Data*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-opportunities-in-telecom-sector-noexp.pdf .

Deloitte 2016. *Blockchain @ Telco: How Blockchain Can Impact the Telecommunications Industry and its Relevance to the C-Suite*. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf .

Deloitte 2018a. "Regulating the Future of Mobility: Balancing Innovation and the Public Good in Autonomous Vehicles, Shared Mobility, and Beyond". *Deloitte Insights*, December 21, 2018. https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/regulating-transportation-new-mobility-ecosystem.html .

Deloitte 2018b. "The Future of Regulation: Principles for Regulating Emerging Technologies". *Deloitte Insights*, June 19, 2018. https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html .

Deloitte 2018c. *The Regulator's New Toolkit: Technologies and Tactics for Tomorrow's Regulator*. https://www2.deloitte.com/content/dam/insights/us/articles/4539_Regulator_4-0/DI_Regulator-4-0.pdf .

Deloitte 2018d. Government Trends 2020: What are the Most Transformational Trends in Government Today? *Deloitte Insights*, June 24, 2019. https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html .

Ericsson 2019. *Ericsson Mobility Report*. https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf .

Esselaar, S. and C. Stork. 2019. "Evolving Business Models are Driven by OTT Applications". Paper presented at the ITU Study Group on OTT, Geneva, September 2019. https://researchictsolutions.com/home/wp-content/uploads/2019/11/RIS-evolving-business-models.pdf .

European Commission. 2020. *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*. COM(2020) 65 final. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf .

Internet Society. 2017. *Paths to Our Digital Future*. https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf .

ITU (International Telecommunication Union). 2014. "The Role of Big Data for ICT Monitoring and for Development", In *Measuring the Information Society Report 2014*, Geneva:

International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Documents/bigdata/MIS2014_Chapter5.pdf .

ITU (International Telecommunication Union). 2016. *Trends in Telecommunication Reform: Regulatory incentives to Achieve Digital Opportunities*. Geneva: International Telecommunication Union. https://www.itu.int/pub/D-PREF-TTR.17-2016 .

ITU (International Telecommunication Union). 2017. *Global ICT Regulatory Outlook 2017*. Geneva: International Telecommunication Union. Geneva: International Telecommunication Union.https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Outlook/2017.aspx .

ITU (International Telecommunication Union). 2018a. *Assessing the Economic Impact of Artificial Intelligence*. ITU Trends: Issue Paper No.1. Geneva: International Telecommunication Union. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-ISSUEPAPER-2018-1-PDF-E.pdf .

ITU (International Telecommunication Union). 2018b. *Cloud Computing Standardization Roadmap*. ITU-T Y.3500-series. Geneva: International Telecommunication Union. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup49-201811-I!!PDF-E&type=items .

ITU (International Telecommunication Union). 2019a. *Distributed Ledger Technology Terms and Definitions*. Technical Specification FG DLT D1.1. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf.

ITU (International Telecommunication Union). 2019b. *Distributed Ledger Technology: Regulatory Framework*. Technical Paper HSTP.DLT-RF. Geneva: International Telecommunication Union. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DLT-2019-RF-PDF-E.pdf .

Liptak, Andrew. 2017. "Tesla Extended the Range of Some Florida Vehicles for Drivers to Escape Hurricane Irma". *The Verge*, September 10, 2017. https://www.theverge.com/2017/9/10/16283330/tesla-hurricane-irma-update-florida-extend-range-model-s-x-60-60d .

MapR. 2020. *MapR Guide to Big Data in Telecommunications*. https://mapr.com/whitepapers/data-convergenece-in-telecommunications/assets/data-convergenece-in-telecommunications.pdf . Accessed April 24, 2020.

McKinsey. 2018. *Notes from the AI Frontier: Insights from Hundreds of Use Cases*. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20ai%20frontier%20applications%20and%20value%20of%20deep%20learning/notes-from-the-ai-frontier-insights-from-hundreds-of-use-cases-discussion-paper.ashx .

Michels, Johan David. 2018. "Blockchain and Telecoms". *InterMEDIA*, (46) 4. https://ssrn.com/abstract=3324482 .

Porter, M. and James E. Heppelmann. 2014. "How Smart, Connected Products Are Transforming Competition". *Harvard Business Review*, November 2014. https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition .

TRAI (Telecom Regulatory Authority of India). 2018. "Information Note to the Press". Press Release No. 58/2018. https://www.trai.gov.in/sites/default/files/PRNo.5829052018.pdf .

UNSATS. 2015. *Deliverable 2: Revision and Further Development of the Classification of Big Data*. United Nations Global Working Group on Big Data for Official Statistics Task Team on Cross-Cutting Issues. https://unstats.un.org/unsd/trade/events/2015/abudhabi/gwg/GWG%202015%20-%20item%202%20(iv)%20-%20Big%20Data%20Classification.pdf .

Chapter 8. Technical regulation

This chapter on technical regulation comprises two parts: quality of service (QoS), and numbering, naming, addressing, and identification (NNAI). On QoS, the chapter explains the role of the regulator in informing users, restraining operators in strong competitive positions, ensuring efficient use of scarce resources, and assessing the national infrastructure. The activities of regulators related to QoS monitoring are explored including: selecting indicators; defining measurements; setting targets; making, auditing and publishing measurements; stimulating improvements; and reviewing developments. The second part explains the importance of NNAI, refers to NNAI resources described in ITU-T Recommendations, and outlines the key objectives of NNAI management. The emergence of the digital age and the impact of new technologies on NNAI is explored, and the instruments at the disposal of the regulator are described.

8.1 Part 1. Quality of service

Introduction

What is quality of service?

People everywhere depend on ICT services. Unless these services are good enough, people need face-to-face contact in order to hold conversations, send and receive messages, obtain news, transfer money, play games, monitor and control machines, take part in markets, meetings, lessons, and entertainment, and so on. The range of services continues to grow.

What "good enough" means depends on many factors, such as user feelings and expectations, which themselves vary with applications and environments. To be good enough, services usually have to be not annoying, even if they are not delightful. In the words of ITU-T Recommendation P.10/G.100, the quality of experience (QoE) is "the degree of delight or annoyance of the user of an application or service" (ITU-T 2017).

Assessments of quality find out the degree of delight or annoyance under certain circumstances. Just as the range of services continues to grow, so does the range of assessments of quality; for instance, there are now standards for assessing the quality of over-the-top (OTT) streaming of multimedia to both televisions and smartphones and for designing tests of the quality of digital financial services (ITU-T 2020b; ITU-T 2020c).

The quality of service (QoS) restricts attention to some of the factors on which the quality of experience depends; it is defined to be "the totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service" (ITU-T 2017).

QoE and QoS relate to both information technologies and communication technologies. For instance, the users of interactive systems are interested in the speeds with which the systems respond, not in how the responses are produced, and parts of the systems might be "in the cloud", not on the user terminals (in what in earlier jargon were client-server relationships with thin clients): both the speed of transmitting information and the speed of processing information are important.

"Quality of service" and similar terms have been used in many ways over many years. In some documents (such as specifications of WiMAX), "quality of service" refers to techniques for managing traffic having particular types, such as voice or video; in other documents, "class of service" and "type of service" are used for this purpose, while "grade of service" refers specifically to successful call set-up. When QoS is used just to describe traffic management techniques, QoE is needed to assess how annoying or delightful ICT services are.

QoS as discussed here is closely connected with QoE and only indirectly related to traffic management techniques. However, QoE includes aspects of user characterization that QoS, as frequently understood, excludes.

Extra attention is devoted to QoE here because it is less known than QoS. Nonetheless, QoS remains relevant to whether, why, and how people use ICT services.

What should the regulator do?

Operators make many QoS assessments of their own, in their usual engineering activities and responses to customer complaints. If they have competitors they want to keep their market shares, so they look for the best combinations of quality and price and necessarily examine QoS. Of course, they might not do this if there is no competition or compulsion. Even if there is competition, there can be parts of the population that are poorly served and national needs that are not met.

In general, the regulator should be involved, with the purposes of:

- **Informing users**. Any checks on the claims made by operators need to be done by others. Any comparisons of quality between operators should use comparable measurements,

which no one operator can provide. These checks and comparisons can help to redress the balance of information between customers and operators if they are publicized suitably.

- **Restraining operators in strong competitive positions**. Such operators might lower quality to raise revenues, especially if they have significant market power or are appointed to provide universal service. This is so for wholesale as well as for retail; for instance, an operator that controls the international gateway switches in a country is in a position to dictate interconnection service level agreements.
- **Ensuring efficient use of scarce resources**. People are entitled to know how well public property, such as the radio spectrum and rights of access to land, are being used. These are "scarce resources": they might be exploited more or less efficiently but they do not expand. Using them well could entail serving diverse communities fully throughout the country.
- **Assessing the national infrastructure**. The infrastructure should be satisfactory for emergency support, business investment, human development and government services. No one operator is responsible for this; the regulator can take an overall view. Unaided, a competitive market might not fill the gaps in the infrastructure and might even lead to lower quality as all of the operators try to cut costs.

These purposes can delimit the scope of involvement of the regulator but do not determine the scale. The quality of services can differ greatly in different places and at different times. The services themselves vary enormously; assessing them is not always just a matter of calculating call completion rates. The regulator might have to select areas of involvement carefully or find ways of getting others to perform the assessments, either by working with the operators or by crowdsourcing.

The extent to which the regulator is involved depends on several factors, such as market maturity, financial constraints, political attitudes, and institutional arrangements. Even if the regulator does not make, audit or publish QoS measurements, there are ways in which the regulator and the operators together can perform some degree of monitoring.

QoS regulations can exist on paper but be ignored in practice. Regulators might not receive measurement results and might not enforce compliance. In those circumstances an operator might reach the targets but not feel a need to report the results.[1] Small countries where there are subsidiaries of large operators are particularly likely to suffer from them.

What are parameters and targets?

QoS is assessed by making measurements and checking whether the measurement results are satisfactory. The measurement results relate to:

- **Parameters**. These are quantities that can be measured to assess the quality of some aspect of the service. In other documents, they might be called "indicators", "metrics", "measures", or "determinants". Examples are "the successful call set-up ratio" (or "the proportion of call set-ups that are successful") and "the average complaint resolution time" (or "the mean of the times taken to resolve complaints").
- **Targets**. These are values of parameters for which the given aspect of the service is regarded as "good enough"; they might be intended to be reached immediately or within a certain timeframe. In other documents, they might be called "objectives", "benchmarks" or "thresholds". Examples are "97 per cent" (for a ratio, such as the successful call set-up ratio) and "6 hours" (for a time, such as the average complaint resolution time).

[1] Both shortcomings are illustrated in the *Digital Regulation Platform* thematic section on "The ECTEL experience of quality of service regulation".

Usually international standards for QoS, from the International Telecommunication Union (ITU), the European Telecommunications Standards Institute (ETSI), the 3rd Generation Partnership Project (3GPP) and other organizations, identify parameters and describe measurement methods but usually do not set targets. Also, in many countries, parameters are defined but targets are not set.

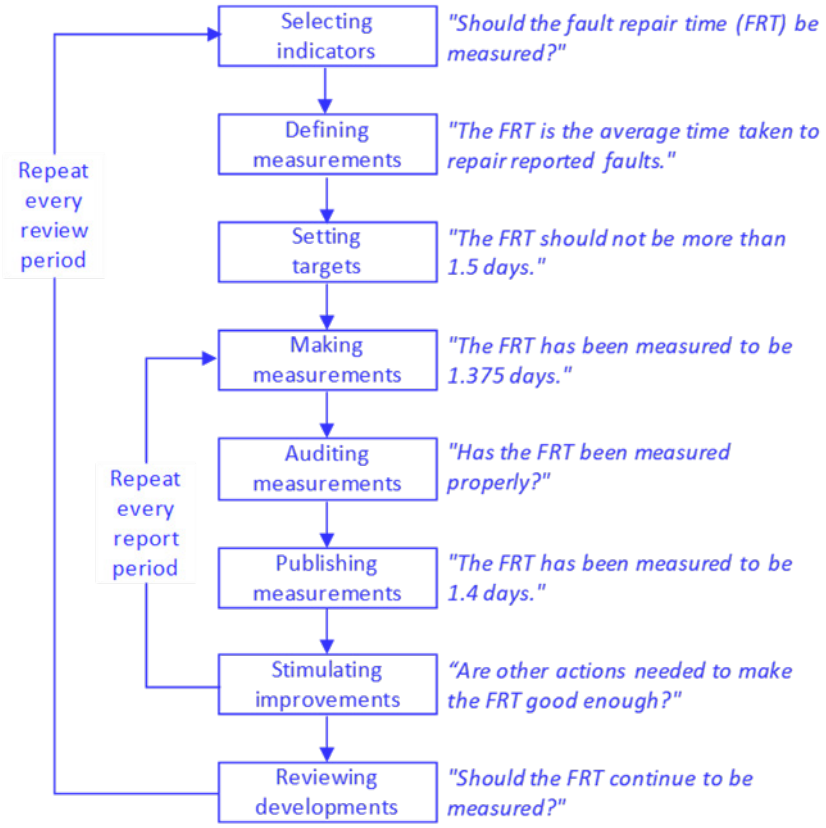
Among regional organizations, the Eastern Caribbean Telecommunications Authority (ECTEL) and the East African Communications Organisation (EACO) are unusual in identifying parameters for their member states. The parameters are intended for voice and data services and, In EACO, for digital financial services using certain Unstructured Supplementary Service Data (USSD), Short Message Service (SMS), and Hypertext Transfer Protocol Secure (HTTPS) messages (EACO 2017).

The ITU has produced a manual on quality of service regulation intended mainly for regulators (ITU-D 2017). It includes many examples of parameters from countries across the world, as well as discussions of several other relevant topics. A shorter account of some of these topics can be found in ITU-T Recommendations Series E.800 Supplement 9 (ITU-T 2013a).

What does quality of service monitoring involve?

Figure 8.1 sets out the activities of regulators related to QoS monitoring, in a slight variant of a widespread flow chart.

Figure 8.1. Activities during QoS monitoring



Source: Adapted from ITU-D 2006.

The outer loop of activities, which is repeated in every review period, involves:

- **Selecting parameters**. The parameters selected for measurement should relate directly to the aspects of their experience that are most important to users.
- **Defining measurements**. The measurements should be defined so that different operators can be compared in the respects having significant implications for users.
- **Setting targets**. Any targets that are to be associated with the parameters should be set with a prior knowledge of what improvements in quality can reasonably be expected.
- **Reviewing achievements**. The achievements are examined at the end of the review period to see whether the intentions of QoS monitoring are being fulfilled.

The inner loop of activities, which is repeated in every reporting period, involves:

- **Making measurements**. The measurements are made by the operators, the regulator, or both the operators and the regulator. If the measurements are made by the operators, they are recorded and reported to the regulator at the end of the reporting period.
- **Auditing measurements**. The measurements might be audited by the regulator. If the measurements are made by the operators, often the regulator relies on self-certification by the operators (when senior managers in the operators certify the validity of the measurements) and occasional or annual checks, perhaps combined with drive and walk tests or crowdsourcing tests.
- **Publishing measurements**. The measurements are published by the operators, the regulator, or both the operators and the regulator. They can then also be publicized by journalists online and offline.
- **Stimulating improvements**. The improvements in quality might be stimulated in various ways, ranging from proposing improvement plans to imposing fines. In some circumstances, poor publicity from published measurements might provide enough stimulus.

Especially on the inner loop there can be bursts of activity that do not correspond neatly to reporting periods with constant lengths and frequencies. For instance, regulators might make measurements in particular places that had been neglected in network expansion or that had been responsible for many complaints, and in doing this they might need to forgo making measurements elsewhere.

Improvements in services, other than customer care, often require improvements in networks. Consequently, they need to be assessed only on a timescale like that for bringing about improvements; anything else can impose unnecessary burdens on the operators who make and report the measurements and on the regulators who audit or publish the results. This suggests leaving at least three months between QoS assessments. Accordingly, regulators often require that the operators report measurements quarterly. However, they themselves might make measurements annually, to investigate the circumstances in particular places or to check the reports by the operators.

There is a further discussion of these activities in the ITU manual on quality of service regulation (ITU-D 2017). They are also considered more in ITU-T Recommendation E.805 (ITU-T 2019a). They are looked at one-by-one in subsequent sections here, in the order in which they happen.

Selecting parameters

Regulators can get an initial view of how to concentrate their QoS monitoring from press reports, meetings with the public, contacts with consumer organizations, complaints to operators, and discussions with operators. Analysing social media posts can be illuminating but is complicated by potential exaggeration or misinformation.

In addition, regulators can conduct consumer surveys face-to-face, in telephone calls, or online, which need not be expensive or laborious. Even the answers to general questions, such as "how satisfied are you with the quality of the services that you receive?", can be helpful. A simple example gives customer responses to nine questions about three services from three operators in two islands (CICRA 2019).

One especially thorough approach involves asking people to record their ICT activities in diaries. The diaries would indicate the relative importance of the activities, which could affect the priorities for QoS monitoring. The results can be detailed, with up to thirty different ICT activities for different age ranges, social groups, and genders in one case (Ofcom 2016).

The selection of parameters should satisfy the following criteria:

- **Relevance to users**. QoS monitoring is concerned more with user experience than with network performance. Operators might need to examine network performance parameters when designing their networks, but regulators, who do not design networks, do not need to do so. For instance, regulators need not require operators to report parameters about wireless handovers: these might be important to network designers but they are not directly relevant to users, who just want to know the proportion of calls that continue. In QoS monitoring, regulators are aiming to assess the QoS achieved by the operators against the QoE wanted by the users.[2] In summary, the QoS parameters monitored by regulators should be directly relevant to user experience.
- **Importance to society**. There might be some parameters that are of no immediate interest to individual users but are of importance to society as a whole. In particular, the national infrastructure should be satisfactory for emergency support, business investment, human development, and government services. Assessing the national infrastructure might entail, for example, knowing the call capacity on crucial network routes to ensure that enough calls could be made after disasters. Any need for such parameters should be considered by the working group on emergency telecommunication planning.
- **Commonality between services**. For purposes of QoS monitoring, different regulators group services in different ways; for instance, they might group fixed broadband with mobile broadband or they might separate fixed broadband from mobile broadband (in which case they will often ignore mobile broadband). The groupings reflect the particular circumstances of countries but make comparisons between countries difficult. However, some parameters can be the same for different services, especially if they relate to customer care.
- **Independence of technology**. Parameters should not depend on technology unless users regard the technology as characteristic of the services being monitored. For instance, voice calls remain voice calls, regardless of whether the underlying networks are fixed or mobile, so the parameters for telephony might be common to fixed and mobile services (and to traditional and OTT services). This is in line with the increasing substitution of mobile services for fixed ones, when user requirements on, and expectations of, telephony are largely independent of network technology.

  By contrast, the parameters for service supply might be common to wireless and wireline services needing fixed access (as they are complicated mainly by visits to customer buildings) but disregarded for services needing mobile access.
- **Minimality of requirements**. QoS monitoring can be burdensome for both regulators and operators. Its costs should be weighed against its benefits. There are many parameters that could be monitored: eighty-eight are listed for customer care in ITU-T Recommendation E.803 (ITU-T 2011). However, customer complaints and customer surveys do not show a need for most of them: for instance, in the UK, for four services (fixed broadband, fixed telephone, mobile broadband and telephony, and subscription television) "not

[2] The appropriate sorts of assessment are described in the *Digital Regulation Platform* thematic section on "The relation between quality of service and quality of experience".

performing as it should" (often because of loss of service, poor delivery, or inaccurate advertising) and billing cause 75-95 per cent of complaints (Ofcom 2019).

Once parameters are selected they tend to remain when they are no longer needed; for instance, voice call set-up time is still reported in various countries where it is rarely high. If parameters become obsolete or unnecessary they should be discarded. This has been done in Brazil, for example.[3]

Further advice on selecting parameters can be found in ITU-T Recommendation E.802 (ITU-T 2007). It discusses the relations between different aspects of quality and the parameters that can be regarded as measuring those aspects from several viewpoints.

Defining measurements

Operators are likely to have already developed and implemented plans for regular QoS monitoring. Discussions with them, and with third parties that perform QoS monitoring for others, can enhance the understanding of the usefulness of particular parameters, the practicability of making and auditing measurements, and the realism of potential targets.

The following guidelines are relevant to the details of how to make measurements:

- **Correspondence with usage**. Measurements should be made at times and places to match user experience as far as possible. In particular, they should use data about actual user activity, not data from planning tools. Similarly, measurements should use data from potential user locations, not data from base stations, when they test activities such as call set-up that might fail before communications with the base stations can be established.
- **Awareness of time and place**. Large differences in quality can occur at different times of day, even within the working day, and at different seasons of the year. This can be a symptom that a service does not yet have enough users for statistical multiplexing to be effective: allocating more bandwidth is difficult to justify when there are few users, so the variation in demand is a high proportion of the allocated bandwidth.

  Large differences in quality can also occur between places near each other that have different population densities, land uses, traffic, and environment. For instance, moving fast or being inside can attenuate signal strengths by 15 dBm (Marina et al 2015).

  If differences in quality are large in different times and places then different measurement results are needed. The regulator and the operators together need to determine what these should be (typically after separating indoors, driving outdoors, and walking outdoors). In any event, the regulator should receive measurements annotated with their times and places.
- **Comparability between operators**. The measurements made by different operators and by the regulator can be compared fully with one another only if they are made in ways that are the same in all respects having significant implications for users. This can be difficult to achieve: not only do different operators make measurements in different times and places, they also have different practices and equipment. Simply naming parameters (as in many regulations and licences) rarely identifies the measurement methods precisely: standards can contain many options, and equipment vendors might use the same names for different network element counters.
- **Representativeness**. Often measurement results are formed from sampled values, typically by calculating the "mean" (or average) of the values. There is then always a sampling error. It is reduced by having a large enough sample to give confidence that the measurement

[3] Hence eight out of fourteen entries are struck through in the table in the *Digital Regulation Platform* thematic section on "The Anatel approach to quality of service monitoring for mobile services".

result formed from it is close to the value that represents the user experience.[4] Ideally, the sample is large enough that different measurement results represent perceptibly different user experiences. This point is frequently ignored in reports on drive and walk tests by regulators, which give results for small districts without saying how many tests were performed in each of them.

- **Perceptibility to users**. Differences between measurement results that do not represent perceptible differences between user experiences might be said to be below a threshold, which is the "just noticeable difference". The threshold is not independent of the measurement results: often, for given differences in measurement results, the differences between user experiences are more easily perceived if the measurement results are smaller (just as the difference between 2 and 3 per cent is perhaps more easily noticed than that between 97 and 98 per cent).

  Means do not always summarize everything useful; for instance, a mean repair time might result from many fast repairs and some slow repairs. Hence, sometimes the most suitable parameter is not the mean of the sample but the maximum in a "quantile", which is the proportion (such as 80, 90, 95, or 99 per cent) of the smallest values sampled. Taken together, the mean and the maximum in a suitable quantile can do much to characterize the sample; if just one of them is published, it will usually be the mean, because users are more likely to understand it.[5]

Setting targets

Parameters do not always need targets, as remarked in ITU-T Recommendation E.805 (ITU-T 2019a). The popularity of OTT voice services shows that many users are willing to sacrifice quality for economy: they prefer low prices with low quality to high quality with high prices. QoS requirements should not prevent users from choosing particular quality levels or operators from offering particular quality levels, regardless of whether they have traditional or OTT services.

Regulators can provide advice on quality levels (to both users and operators) without setting targets. However, setting targets can help to protect consumers when there is no practical choice between quality levels. This can happen because:

- There is a monopoly (or sometimes even an oligopoly with feeble competition), perhaps offering "universal service".
- There is competition but switching costs discourage switching and quality levels have fallen without prices falling to match.

Useful advice on setting targets can be found in ITU-T Recommendation E.802 (ITU-T 2007). Targets that are realistic but demanding are often difficult to set. They should be introduced only after measurement of what is achievable; they could be made more demanding after every review period in which they are achieved.

Targets set in other countries need to be treated cautiously because the environments are different and the regulators might be ignoring their own rules.

---

4 The relation between confidence levels and sample sizes is explained in the *Digital Regulation Platform* thematic section on "Basic statistics for quality of service assessment". Another account, concentrating on how to score and rank operators against each other, can be found in ITU-T Recommendation E.840 (ITU-T 2018).

5 Descriptions of means and quantiles are given in the *Digital Regulation Platform* thematic section on "Basic statistics for quality of service assessment". Further descriptions, accompanied by details about several useful distributions, can be found in an ETSI technical specification (ETSI 2019).

Making measurements

Measurements might be subjective or objective, as described in ITU-T Recommendation E.802 (ITU-T 2007).[6] Here the focus is on objective measurements, as subjective ones are expensive and difficult to design for representative samples of users.

Measurements for a real network can be made in the network or in the field. A further classification of them is the following:

- **System readings**. These are obtained in the network from network nodes and support systems. They might require visits to outside plant, but more often they rely on collecting data centrally in network and support systems (though they could still involve customer equipment in tests, if the equipment is operating and open to operator intrusions). The data might be collected by the operator and forwarded to the regulator; alternatively, it might be collected by the regulator directly from a server inserted into the network of the operator. However, the data might not always represent the user experience fully; for instance, a network element count of wireless call attempts will not count the call attempts that fail because they never reach the base station.
- **Campaign tests**. These are performed in the field according to plans for particular times and places. The test equipment should use wireline or wireless connections to the networks like those that a customer would need. Campaign tests for fixed access are often done in the buildings or outside plant of the operators, to avoid needing access to houses and offices; campaign tests for mobile access are often drive and walk tests, done in vehicles or public spaces (such as shops and malls) using mobile phone arrays or special test equipment, with assumptions about extending the results into houses and offices. Though drive and walk tests are initiated by people alongside the equipment, similar tests of "unattended probes" might be initiated remotely when particular places require monitoring.

  Drive and walk tests are expensive. To have confidence in them needs hundreds of tests, which should be repeated in every place where distinct results are wanted. To reduce costs, the regulator or the operators might choose an agent to conduct the tests for all the operators together. In the simplest arrangement, the regulator chooses the agent and recovers the costs from the operators in their normal fees (or in proportion to the number of tests per operator, for example). In an alternative arrangement, the operators choose the agent; the regulator can assist and reduce opportunities for delay by convening meetings of the operators and proposing ways of cost sharing. In either arrangement, the agent must be prepared to conduct tests for all of the operators on equal terms, so all of them can enjoy the same economies of scale and scope.
- **Crowd tests**. These are performed in the field by crowdsourcing. The terminals of users, or test equipment distributed to users, make measurements that collectively indicate user experience. Such tests are not matched for different operators: they are done wherever and whenever the users are present, and they might or might not be initiated by the users. Crowd tests for fixed access require personal computers or test equipment; crowd tests for mobile access require smartphones (unless they rely just on text messages to and from users). Though the tests might be initiated by users, the results are more likely to reflect the general situation if they are initiated automatically, not because of momentary user feelings.

A useful description of these techniques provides examples from French-speaking countries in Africa (Fratel 2019; Fratel 2020). It also mentions making estimates of quality from statements about coverage (typically as displayed in maps). If the statements about coverage are derived just from geographic and demographic information, then such estimates are

[6] The purposes of subjective and objective assessments of quality are discussed in the *Digital Regulation Platform* thematic section on "The relation between quality of service and quality of experience".

not substitutes for measurements. However, they can influence decisions about where measurements should be made.

In the past measurements for fixed access have typically been system readings while measurements for mobile access have often been drive and walk tests, but crowdsourcing now provides an alternative to them. These techniques for QoS assessment in mobile networks are discussed in ITU-T Recommendation E.806 (ITU-T 2019b). It provides guidelines on the choice between active and passive measurements, the measurement of particular parameters, the characteristics of monitoring systems (except for crowdsourcing), data processing, and sampling. It is complemented by ITU-T Recommendation E.812 (ITU-T 2020a). That recommendation includes further advice on several of these topics (and on the characteristics of test servers for crowdsourcing).[7]

Auditing measurements

When different operators make measurements at different times and places, the results are not strictly comparable with one another. The costs can be reduced, and comparability can be achieved, by making measurements for all of the operators at the same time. However, operators might not be prepared to have their own drive and walk tests done by a common agent. In these circumstances, the results need to be checked by the regulator.

To this end, each operator should hold records of its measurements for perhaps a year after they have been made. The records should include details of the observations and calculations, and any fault reports or service complaints, on which the measurement results depended. They would be provided to the regulator to be compared against other measurements made by the regulator or other operators. The comparisons would determine whether:

- The measurement results were likely to be valid.
- The measurements needed more precise definitions because different operators interpreted them differently.

If the operators use crowdsourcing, they might have different data collectors to collect and process the data into measurement results. To check the extent to which the measurement results for different operators are comparable, the regulator would examine in detail the data collection and processing done for each operator and would ask for changes if necessary.

In crowdsourcing, each individual user is testing only one network at a time. However, there can be so many users that there are enough tests of each service. If extra tests are wanted, the regulator can arrange that calls are set up on multiple smartphones (one for each network) at particular times and places.

Even if crowdsourcing is not the main QoS measurement method, it can be useful in auditing, when the measurement results stated by the operators can be compared with ones obtained by crowdsourcing.

[7] A related discussion can be found in the *Digital Regulation Platform* thematic section on "Crowdsourcing techniques in quality of service assessment".

Publishing measurements

Publishing QoS information is important if customers are to make informed choices. Publication can be by the regulator or the operators. It is most cheaply and consistently done by one organization; moreover, the regulator is better placed than the operators to offer impartial comparative figures side-by-side. However, often the operators have more resources than the regulator, so they need to publish their own QoS information as approved by the regulator, in formats agreed by the regulator.

In providing information to users, a balance must be struck: users should not be overloaded but should have enough information on which to base their decisions. In particular:

- Measurement results could be displayed in rankings, tables, bar charts, or star charts (possibly with "traffic light" colours or other marks to indicate whether the measurement results were "good enough").[8] They might be accompanied by explanations by the operators or by the regulator of the causes of any unsatisfactory measurement values.
- Measurement results should use the same numerical conventions as each other, as far as possible. Thus, in all, or almost all, cases either a high value or a low value should indicate good quality; for instance, alongside the dropped call ratio would be the unsuccessful call set-up ratio, not the successful call set-up ratio. As users find small numbers easier to assess than large numbers, low values should probably indicate good quality, at least for parameters that are percentages. However, mean opinion score (MOS) treats high values as good.
- Measurement results should be written with at most two significant figures. Further figures would rarely express distinctions in quality that users would appreciate.
- Measurement results could be presented in layers, with each layer providing pointers to a more detailed layer. Users are likely to be interested in particular parts of the QoS information, not all of it; for instance, one might be interested in speech quality on main roads, while another was interested in broadband availability in remote places.[9] Different presentations, with different levels of detail, are needed by different people. For instance, policy-makers, opinion formers, service providers, and large businesses might want web pages and newspaper statements, but private consumers and small businesses will prefer leaflets, bill inserts, social media feeds, radio and television advertisements, freephone messages, and community meetings.
- Measurement results should be presented fairly. For instance, results for an operator that needs to use the network of another operator might be annotated with explanations if they are worsened by deficiencies of that network.

Stimulating improvements

If improvements in quality are needed, then investments might be needed and imposing fines could be counter-productive, as noted in ITU Recommendation E.805 (ITU-T 2019a). For instance, the regulator in Chad, having noted that the fines imposed over several years had had no effect, replaced fines with requirements to invest amounts equivalent to the fines in improving the networks within six months (ARCEP 2020).

Devising and implementing plans to stimulate improvements can help the operators and the regulator to work together in the associated task of developing and modifying the parameters and targets so that they stay suitable. Giving users information that compares operators allows competition to be a spur to improvement, especially if changing operators is easy.

---

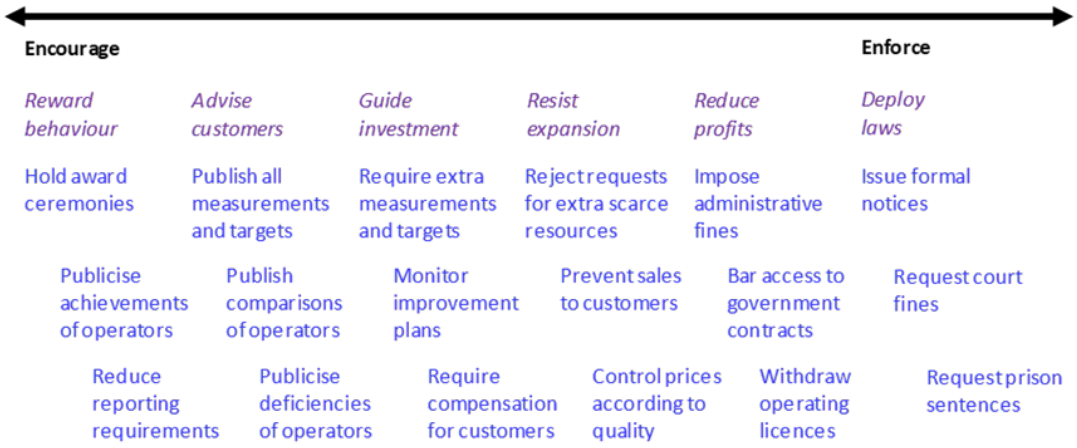
[8] Most of these possibilities are illustrated in the *Digital Regulation Platform* thematic section on "Examples of quality of service presentation by regulators".

[9] The range of information provided in Brazil is shown in the *Digital Regulation Platform* thematic section on "The Anatel approach to quality of service monitoring for mobile services".

Both good and bad publicity can act as ways of stimulating improvement. For instance, operators that perform far better than the others (or than the targets require) could be publicized by the regulator and awarded titles such as "broadband operator of the year" (or at least of the review period). Currently few regulators do anything like this; indeed, many do not even name and shame the operators that are deficient or publish separate figures for separate operators.

There is a wide range of techniques available to stimulate quality, as depicted in Figure 8.2.[10] Their applications should have reasoned justifications; otherwise ultimately the rule of law might be disregarded (by citizens or the government). They can be graduated to fit how far operators are trying to improve quality without raising prices. They should also be proportionate and responsive, as discussed in ITU-T Recommendation E.805 (ITU-T 2019a). For instance, penalties should be related to the persistence and severity of failures to comply with regulations and licences.

Figure 8.2. Techniques for stimulating improvements in quality



Source: Adapted from ITU-D 2006.

The costs of QoS measurements bear most heavily on small operators, because the number of measurements needed for precise enough results is independent of the size of the operator. There is, therefore, a case for exempting operators from making QoS measurements for regulators in places where their customers form small proportions of the population (less than 5 per cent, for example), as in Brazil (Anatel 2020). Nonetheless, they might choose to make these measurements, because of the beneficial publicity that good test results can provide, especially if they are intent on building their market shares.

If small operators are not exempted from making QoS measurements for the regulator, they might still be exempted from full enforcement. In particular, they might be exempted from being fined, even when they are not exempted from being required to implement improvement plans. This is in keeping with the view that enforcement should be proportionate and responsive, as discussed in ITU-T Recommendation E.805 (ITU-T 2019a).

[10] Several of these techniques are mentioned in the *Digital Regulation Platform* thematic section on "Examples of quality of service presentation by regulators".

Reviewing achievements

In reviewing QoS monitoring against its purposes, changes during the review period in the market environment, as well as those in QoS, are relevant. For instance:

- Parameters can be discarded if they are no longer important.
- Targets, and exemptions from QoS monitoring for small operators, can be discarded if competition has grown strong enough.
- Crowdsourcing might play a greater role in QoS monitoring if smartphones have become widely available.
- Reporting periods might be lengthened if improving on good results takes longer than improving on bad ones.

The QoS monitoring framework tends to be difficult to change if it is stated in licences that need to be negotiated with several operators or in regulations that need to pass through several government bodies before coming into effect. Such processes can sometimes be avoided for QoS monitoring requirements that are consistent with government policy and not controversial; for instance, the requirements might be stated in schedules or open letters to operators. However, avoiding such processes generally limits the powers of the regulator: some ways of encouraging improvements in QoS lose their legal foundations, so persuasion needs to replace compulsion.

8.2 Part 2. Numbering, naming, addressing, and identification (NNAI)

Why do numbering, naming, and addressing matter?

Telephone numbers were devised well over a century ago to provide a way of identifying destinations of telephone calls uniquely. They then became used to identify sources of telephone calls, in calling line identification (CLI). They could contain information about tariffs and value-added contents. They are now used much more generally as unique identifiers, in money transfers, over-the-top (OTT) messages, Internet of Things (IoT) devices, and so on. In effect "destination" has been expanded to refer to people and things generally.

The rotary dials originally used to input numbers have long since disappeared (though "dialling" is still used for the input of a telephone number). People now often send messages by touching screens or speaking commands; in doing so, they do not usually see or say telephone numbers, but the numbers might still be there in their contact lists.

Since the 1960s, numbering, naming, addressing, and identification (NNAI) resources have evolved to meet emerging requirements and technological innovation. The digital age is no different. In fact, the evolution of the uses to which NNAI resources are being put in the digital age could not occur were it not for the early evolutionary steps.

What are NNAI resources?

The term "NNAI resources" is a generic reference to resources that are described in ITU-T Recommendations and that are used to provide telecommunication services. Of those that are specified, three are considered in this section because of their usefulness in the digital age:

- Telephone numbers (Recommendation ITU-T E.164, *The International Public Telecommunication Numbering Plan*) (ITU-T 2010).

- International mobile subscription identifiers (Recommendation ITU-T E.212, *The International Identification Plan for Public Networks and Subscriptions*) (ITU-T 2016).
- Issuer Identifier Numbers (Recommendation ITU-T 118, *The International Telecommunication Charge Card*) (ITU-T 2006a).

Telephone numbers were originally used by the network to identify the destination of a call, and to route the call across the network between two fixed points. Each of the fixed points were known to the operator, and based on these fixed points that operator could charge the customer. The introduction of mobility required other mechanisms to be developed that would identify that connection could be established, and that charges could be made. International mobile subscription identifiers (IMSIs) are the means by which a user can be provided with service outside of their national network of choice to make and receive calls. An Issuer Identifier Number (IIN) is used to identify the charges that accrue from a call in a mobile scenario. The focus of the following sections is on the telephone number as it is the most visible resource.

NNAI management

NNAI management falls generally under the responsibility of the numbering plan administrator. Such administration can occur within a designated ministry, or within the mandate of a regulator. The scope of the responsibilities of the entity that has the responsibility is a national matter. In some cases, an official national authority might take the role, or agents might do so on behalf of the authority (as happens with some countries in the North American Numbering Plan). NNAI management by the regulator can fulfil the following objectives:

- **Identifying people and things uniquely**. By being responsible for NNAI resources of numbers, the regulator can ensure that numbers have unique uses, both nationally and internationally. Another organization might be authorized to supply numbers that the regulator had supplied to it, but the regulator would still be the original source.
- **Helping people to use numbers**. Operators would ideally prefer to have short numbers with meanings that fit their own services. The regulator can keep numbers short, uniform in length, and simple to understand. The numbers used by emergency services and other socially valuable services (such as helplines) are especially important; the regulator can ensure that they are independent of the operators and accessible through all of the national networks.
- **Avoiding future shortages of numbers**. The numbering space is a limited resource.[11] It can be wasted if operators keep numbers rather than recycle numbers that are no longer used. Though enough numbers might seem to be available, eventually more might be needed. Ultimately, this could mean that current numbers would be replaced by longer ones, with costs and inconvenience during the change process and difficulties in adapting to the longer numbers afterwards. The regulator can prevent wastage and plan far enough in advance to avoid shortages, usually without needing to change numbers that have already been assigned.
- **Developing orderly markets in communications**. Operators might make numbers difficult to supply fairly, especially if they have significant market power or managed numbers before the regulator was appointed. For instance, they could hoard numbers that they did not need, scatter used numbers widely across many blocks, or continue to assign old shorter numbers instead of new longer numbers. The regulator can take charge of the supply and use of numbers, to ensure that numbers are available for new market entrants and that customers can take services from these new market entrants without needing to change their numbers.

[11] The limitation is 15 digits and is specified in Recommendation ITU-T E.164.

Although customers are allocated individual numbers by operators and service providers, operators and service providers are allocated numbers in blocks by the numbering plan administrator. The numbering plan administrator is the entity responsible for the assignment of numbers. Originally this was the incumbent operator, but with the introduction of regulation and competition this responsibility has passed to the relevant ministry or the independent regulator, or their agent (as is the case for some members of the North American Numbering Plan). The size of the block varies according to the use to be made of numbers within that block.

The association of individuals with the telephone number and the reluctance to change telephone numbers to take an alternative service was identified in the early introduction of competition as a barrier to the take up of alternative services. The introduction of number portability, the ability of consumers to change service providers but retain their telephone numbers, did much to remove that barrier. The governance of, and the mechanisms to implement, number portability do vary between countries. ITU-T Recommendation E.164 Supplement 2 (ITU-T 2010) [12] that is continuously updated in ITU-T Study Group 2 (SG2), responsible for operational aspects, including NNAI, defines standard terminology for a common understanding of the different aspects of number portability within an ITU-T E.164 numbering scheme. It identifies numbering and addressing formats, call flows, network architectures, and routing approaches that will provide alternative methods of implementation. It also proposes some examples of the administrative and operational processes required for the successful implementation of number portability.

Global NNAI resources

The NNAI resources being used to support the provision of services until the 1990s focused on the national environment. The resources identified thus far were allocated and assigned to operators indirectly by the International Telecommunication Union (ITU), that is, the ITU allocated the resources to member states, based on rules agreed to by those member states. As a consequence, the rules governing these resources were a national matter. However, during the 1990s this changed with the introduction of global (or directly assigned) resources.

Directly assigned NNAI resources are specified in ITU-T Recommendations. They were originally used for services, such as toll-free, shared revenue, and premium rate services, but for customers that were global in nature, e.g. major hotel chains, helplines, and so on. Such global services had their own country codes allocated and to this day are directly administered by the ITU to service providers and operators. For example, the global, or International Freephone Service (IFS) (Recommendation ITU-T E.152) (ITU-T 2006b) was assigned the country code +800. The use of directly assigned resources has continued to evolve.

The digital age emerges

The relevance of NNAI resources remains even as the nature of telecommunications itself is evolving. The traditional model of communications, which used technology to support voice (known generically as circuit switched), has changed to one where other types of

[12] Supplement 2 to Recommendation ITU-T E.164 defines standard terminology for a common understanding of the different aspects of number portability within an ITU-T E.164 numbering scheme. It identifies numbering and addressing formats, call flows, network architectures and routing approaches that will provide alternative methods of implementation. It also proposes some examples of the administrative and operational processes required for the successful implementation of number portability.

communication, besides voice, exist (known generically as packet switched). The change of the model of communication has also meant changes in the use of NNAI resources.

The environment in which such NNAI resources exist has changed to reflect what is understood by the term telecommunications. The environment is becoming more complex and diverse. There are some national environments where telecommunications are operated by the government; there are other national environments that are fully competitive, with multiple service providers and an independent regulator, or are on the transition towards such an environment. Even the approach to setting the rules that govern the use of NNAI resources varies, with some governments vetting the entities wishing to operate telecommunication services, and so be allocated NNAI resources, while other governments only require such operators to agree to abide by the rules. The former is a licensing regime, and the latter is a general authorization regime.

It is in the context of the transition of national environments, of the changes to telecommunications itself as well as to emergence of new technologies, that the use of NNAI resources continues to evolve in the digital age. The evolution of the uses to which NNAI resources are being put in the digital age exploits previous evolutionary steps in the use made of NNAI resources.

Impact of new technologies

The emergence of new technologies has allowed new services and capabilities to also emerge that in turn has placed new requirements on the availability and deployment of NNAI resources, not only to meet these new demands but also for use by new providers. Such evolution has also impacted the evolution of the environment in which NNAI resources exist and the way in which consumers communicate.

The trends that have emerged in recent years, and that continue to drive the evolution of NNAI resources, are based on the greater use of technology in all aspects of people's lives. The greater use of technology in this way is reflected in the continued need for NNAI resources. That said, the predominant use of telecommunications has changed from one that was wholly voice based to the situation today where the predominant use is based on data associated with digital services.

One such area that has emerged has been over-the-top (OTT) services. These services have emerged as an alternative to traditional voice communication. Some OTT services make use of the telephone number for direct communication within the OTT service. This is allowed for within the terms and conditions to which a consumer agrees (but often does not read) when initially signing up to the OTT service. Some OTT service providers utilize alpha characters and therefore do not need to make use of telephone numbers for direct communication within an OTT service.

The decision as to how the telephone number is used is often taken out of the hands of the users in the call, and determined by the software of the OTT service as covered in the terms and conditions that the user has agreed to on taking the service. This can result in a caller dialing a telephone number and the called user receiving the call via an OTT service. This and similar issues related are under discussion in ITU-T SG2.

The reuse of telephone numbers in an OTT service is as identifiers rather than telephone numbers, and such identifiers map often to IP addresses within the application. One issue that emerges from the use of telephone numbers as identifiers is if the telephone number is reassigned to

a new customer who then registers with the same OTT service. In such circumstances, it has been possible for the new customer to get access to the original customer's data.

The characteristics of communications are evolving and this has consequences beyond the use of NNAI resources in terms of commercial arrangements. Communications for digital services, such as machine-to-machine (M2M) communications and the IoT, are becoming characterized by very short duration connectivity, that are low latency and perhaps less infrequent than the duration and occurrence of voice or human-to-human calls. Also, digital services are being used as an alternative to traditional telecommunications. OTT applications are readily available and are being used by consumers at a fraction of the cost, sometimes at the expense of quality.

Digital service communications are impacting the revenues that can be expected by operators for call-by-call charges associated with voice communication. Many operators are changing the commercial arrangements for traditional voice services, moving to add value to calls rather than just for the communication. For example, one business development that has emerged is that providers of machine-to-machine (M2M)/IoT connectivity are more likely to offer a complete management solution to a business rather than just the communication element. Another example of evolving business development is the manner by which service providers of traditional voice communications, in order to compete with OTT services, have sought to counter the introduction of OTT procedures by moving to a monthly fee rather than call-by-call charges.

The trend to interconnection between the old and new worlds of communications for consumers has given rise to many discussions. These discussions include the extent to which such interconnection might contribute to bypass fraud, or might be seen as an evolution of telecommunications. In some countries, OTT voice services, whether they interconnect with the traditional voice implementation or not, are considered to be network bypass. From an NNAI aspect, whichever view is taken of such interconnection, there have to be commercial arrangements in place and legal and regulatory permissibility for the interconnection to exist. This interconnection represents an evolution of the context in which NNAI resources are being used. Calls from the new services utilize the telephone numbers that are already in use. Calls to the new services require the new and emerging operators to be able to be allocated NNAI resources, which has occurred in many jurisdictions.

What instruments can the regulator use?

The regulator acts by maintaining, and changing as required, three main instruments. With these instruments the regulator can manage numbering effectively and efficiently. They are:

- **The numbering register**. This documents what number blocks have been allocated to which operators and which number blocks are available. It can be a spreadsheet listing the operators that have been supplied particular number blocks (though a simple database management system might offer better analytic techniques and user interfaces). Maintaining the numbering register involves the day-to-day business of supplying number blocks to operators and periodically auditing the numbering register against the records held by the operators. Changing the numbering register happens frequently, when the regulator supplies number blocks to operators that apply for them. It also happens when the regulator reclaims number blocks that had been supplied.
- **The numbering regulation**. This specifies the rules and procedures by which the regulator undertakes their role, and the rules that the regulator can outline for operators. The focus of such regulation are the goals for the regulator including promotion of competition, protection of consumer rights, and which rules may be applied to manage the use of NNAI

resources. For instance, it might state under which conditions operators might be charged for NNAI resources. Changing the numbering regulation happens relatively rarely, when the rules and procedures are revised. Typically, the changes are made only after public consultation.

- **The numbering plan**. This states which numbers can be available for use and in which ways. It can be a table listing the services or local dialling areas that can be associated with particular initial digits and lengths of numbers, as well as other elements, for example, national numbers. Regulators are encouraged to publish their national number plan and to share either the link or the structure with other member states by sending the information to the ITU in accordance with Recommendation ITU-T E.129 (ITU-T 2013b). Evolving the relevance of the numbering plan involves responding to emerging needs and observing trends that require uses of NNAI resources that need to be reflected in the numbering plan. This approach allows regulators to fulfil their requirements of promoting competition and ensuring that sufficient national numbers are available without disrupting existing uses of numbers. Changing the numbering plan happens relatively rarely (perhaps when numbers first become available for supply to operators). Again, the changes might be made only after public consultation, especially if they entail retrieving numbers that have already been supplied and used. Changes to the numbering plan can be disruptive, especially when changing telephone numbers that are in use, and should be seen as an action of last resort by the regulator. For other actions, such as charging for numbers, the regulator can assist in avoiding number changes.

New uses bring new Issues

The use of telecommunications to manage technology, for example in vehicles, is a clear example of the trends that are impacting NNAI. However, these continuing trends bring new issues associated with the use of NNAI. One example is driven by car manufacturers that have deployed the capability to remotely monitor and, if necessary, manage the performance of an individual's car. This capability requires remote access for data collection. Also being deployed is in-car emergency calling, that is, the ability to communicate from, and sometime to, the vehicle in the case of an emergency. This requires an element of voice communication between the vehicle and the public safety access point (PSAP). However, both capabilities are using NNAI resources.

An additional issue associated with in-car emergency calling is one of routing. It is questionable whether the continued use of NNAI resources from the country of a car manufacturer used in a third country would always facilitate access to a PSAP.

In some uses of in-car emergency calling, such as eCall voice calls in the European Union, these can be initiated from either the vehicle or an emergency service centre. However, the most that can be required is that eCall voice calls can be initiated from cars only to closed user groups. Of course, other IoT services, as yet unimplemented, might require calls broadcast to anonymous groups (all users within 1 kilometre, for example). M2M numbers might be intended primarily for data traffic (in domestic alarm systems, for example). For OTT calls, the use of NNAI should be governed by the same rules as the use of other similar numbers where a regulator has chosen to permit the use of similar numbers for OTT services, or specific rules can apply where the regulator chooses to use a specific number range dedicated to OTT services.

However, unlike mobile telecommunications, where the use of the NNAI resources outside of a geographic jurisdiction may be temporary, the use of such NNAI resources when associated with a vehicle may be permanent when the car is permanently exported to a third country. To

ensure that the use of NNAI resources for such capabilities is possible, national regulators are becoming aware of the issues and are adapting the regulations accordingly.

The example of the permanently exported car is but one example. Other examples could include management of shipping containers, or M2M/IoT devices that would require wireless connection in order to communicate, such as alarm systems. There are two issues for originating countries whose NNAI resources may be permanently exported. The first is to ensure that, as the NNAI resources are deployed permanently overseas, that there are sufficient NNAI resources for their own national use. The second is to ensure that, where their resources are used overseas, such use complies with the national regulation of overseas countries.

For those countries that require cessation of permanent roaming of NNAI resources within their jurisdiction after a period of time, then other issues emerge. One such issue is requiring the replacement of the NNAI resources from the originating country with NNAI resources from the national environment. A further issue is then "returning" the original NNAI resources to the originating country. It is possible to replace the NNAI resources but currently there is no solution for returning the original countries' resources.

The means of managing NNAI resources has also evolved and has contributed to the changing use of NNAI. The evolution of the mobile communications device that originally required a physical Subscriber Identification Module (SIM) now allows for an electronic, or virtual, version of the SIM. This has its own issues. For example, a car manufacturer that exports vehicles to an overseas market, and that uses physical SIMs, may incur costs to replace those SIMs if required by national regulation. Industry has developed the ability to update eSIMs over the airwaves (OTA) but this has its own associated costs. That said, regulators may see the implementation of eSIMs and the use of OTA technology as a means of promoting competition in those markets that would otherwise encounter barriers to competition with the need to physically replace SIMs. Such a circumstance may be faced by enterprises using smart meters for their customers and who use mobility NNAI resources to communicate if such enterprises wish to switch communications providers.

Global NNAI resources

One avenue to avoid some of these emerging issues is to avoid the use of national NNAI resources. There has been an increase in the past few years of operators and service providers, both old and new, wanting a direct allocation of NNAI resources from the ITU. While global allocations of NNAI resources address some of the issues of permanent deployment of national resources overseas, direct assignment brings its own set of challenges. The main challenge associated with global numbers for operators and service providers is getting recognition of the directly assigned NNAI resources, that exist behind the country code, to allow for routing and charging. For regulators, the use of global resources in a national context raises the issue of ensuring compliance with national regulation. Ensuring that use of such global resources comply with national regulation and does not, for example, offer competitive advantage, is challenging as the use of such resources is governed by ITU-T Recommendations not by national regulations. Nevertheless, allowing the use of a global resource in a national context may avoid unnecessary depletion of national NNAI resources and as such ensure a ready supply of national resources for the future. For an entity that has global NNAI resource to be used in multiple jurisdictions, there is the benefit of, for example, just one numbering range to be administered rather than a potential myriad of such resources. The rules governing the

use of such resources is enshrined in ITU-T Recommendations that have been approved by member states.

Future challenges for NNAI

The evolution of NNAI for use in new services is a continuation of events that started over 60 years ago. As new services and new technologies emerge, existing NNAI resources are continuing to play a role. This is because of the history of flexibility and evolution that started in the 1960s, both in terms of the use of the NNAI resources and the regulatory and legal environment in which the NNAI resources have existed. This means that the emergence of the digital age does not represent a step change for the use of NNAI resources but is, rather, a continuation of the evolution. The manner by which NNAI resources have been specified, managed. and that have evolved provide a sound foundation for their continued use in the digital age.

What can the regulator do to address these NNAI challenges?

For instance, to help people to use numbers, the regulator can:

- Make numbers easier to remember and dial, by moving towards more uniform number lengths whenever changes take place.
- Keep meanings in numbers simple, by distinguishing between services at most by tariff and destination (understood to include value-added content type).
- Help people that depend on more than one operator or that change operators by getting all operators to use the same short codes as each other for common network services (such as balance checking and fault reporting).
- Let numbers be written and dialled in the same ways throughout the country, by abolishing local number formats that are little used (if calls are mainly made from mobile networks, for example).
- Introduce short codes for socially valuable services (such as helplines for children), if there are organizations that can offer callers the right support.
- Encourage the use of standard ways of writing numbers (see Recommendation ITU-T E.123) (ITU-T 2001).
- Make numbers portable between different operators.

In addition, to avoid future shortages of numbers, the regulator can:

- Be adaptable in providing national NNAI resources for use by emerging requirements for the use of NNAI.
- Withdraw unused numbers to pools for future supply.
- Supply numbers in simple multiples of particular block sizes (such as 1000), and keep supplied numbers tidily close together, to leave large empty spaces for unknown future developments.
- Keep up-to-date records of all supplied number blocks, and check the records against the information held by the operators from time to time (perhaps each year).
- Compare forecasts of future demand for numbers against the available numbers from time to time (perhaps each year), and plan well ahead to avoid any shortages.

The demand for NNAI resources to support new and emerging services and technologies is unlikely to abate in the short to medium term. The challenges that are to be faced in managing the NNAI resources are likely to become more complicated. The challenges include having sufficient resources available, being able to adapt the rules governing the assignment of

NNAI resources to meet the needs of the market (as part of the responsibility of promoting competition) but doing so in a manner that ensures consumer protection and meets national legal regulation.

The rules governing the use of national NNAI resources have evolved to meet requirements that have emerged. While those requirements have been the same in many jurisdictions, the manner by which the use of NNAI resources have been deployed (and governed) have reflected different national environments. This is also true of the digital age.

References

Anatel. 2020. *Qualidade – Telefonia Móvel*. https://www.anatel.gov.br/dados/controle-de-qualidade/controle-telefonia-movel.

ARCEP. 2020. *Évaluation QoS et QoE et analyse comparative des réseaux mobiles au Tchad*. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/qos/202003/Documents/1.%20QoS%20and%20QoE%20assessment%20and%20comparative%20analysis%20of%20mobile%20networks%20in%20Chad.pdf.

CICRA. 2019. *Telecoms Customer Satisfaction in the Channel Islands 2018*. https://www.gcra.gg/media/597877/t1370gj-telecoms-customer-satisfaction-report.pdf.

EACO. 2017. *EACO Guidelines on Consumer Experience and Protection in Digital Financial Services*. http://www.eaco.int/admin/docs/publications/GUIDELINE%20FOR%20CONSUMER%20QoE.pdf.

ETSI. 2019. *Speech and Multimedia Transmission Quality (STQ); QoS Aspects for Popular Services in Mobile Networks; Part 6: Post Processing and Statistical Methods*. ETSI TS 102 250-6 V1.3.1 (2019-11). https://www.etsi.org/deliver/etsi_ts/102200_102299/10225006/01.03.01_60/ts_10225006v010301p.pdf.

Fratel. 2019. *Mesurer la performance des réseaux mobiles: couverture, qualité de service et cartes*. https://www.fratel.org/documents/2019/10/Document-Fratel-couverture-et-qualité-de-service-mobiles.pdf.

Fratel. 2020. *Measuring Mobile Network Performance: Coverage, Quality of Service and Maps*. https://www.fratel.org/documents/2020/05/document-Fratel-ENG-web.pdf.

ITU-D. 2006. *ICT Quality of Service Regulation: Practices and Proposals*. https://www.itu.int/ITU-D/treg/Events/Seminars/2006/QoS-consumer/documents/QOS_Bkgpaper.pdf.

ITU-D. 2017. *Quality of service regulation manual*. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.QOS_REG01-2017-PDF-E.pdf.

ITU-T. 1996. *Home Country Direct*. Recommendation ITU-T E.153. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=3856.

ITU-T. 2001. *Notation for National and International Telephone Numbers, E-Mail Addresses and Web Addresses*. Recommendation ITU-T E.123. https://www.itu.int/itu-t/recommendations/rec.aspx?rec=E.123.

ITU-T. 2006a. *The International Telecommunication Charge Card*. Recommendation ITU-T E.118. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8728.

ITU-T. 2006b. *International Freephone Service*. Recommendation ITU-T E.152. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8729.

ITU-T. 2007. *Framework and Methodologies for the Determination and Application of QoS Parameters*. ITU-T Recommendation E.802. https://www.itu.int/rec/T-REC-E.802-200702-I.

ITU-T. 2010. *The International Public Telecommunication Numbering Plan*. Recommendation ITU-T E.164. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10688.

ITU-T. 2011. *Quality of Service Parameters for Supporting Service Aspects*. ITU-T Recommendation E.803. https://www.itu.int/rec/T-REC-E.803/en.

ITU-T. 2013a. *Presentation of National Numbering Plans*. Recommendation ITU-T E.129. https://www.itu.int/itu-t/recommendations/rec.aspx?rec=E.129.

ITU-T. 2013b. *Supplement 9 to ITU-T E.800-series Recommendations (Guidelines on Regulatory Aspects of QoS)*. ITU-T Recommendations Series E.800 Supplement 9. https://www.itu.int/rec/T-REC-E.800SerSup9/en.

ITU-T. 2016. The International Identification Plan for Public Networks and Subscriptions. Recommendation ITU-T E.212. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12831.

ITU-T. 2017. *Vocabulary for Performance, Quality of Service and Quality of Experience*. ITU-T Recommendation P.10/G.100. https://www.itu.int/rec/T-REC-P.10/en.

ITU-T. 2018. *Statistical Framework for End-to-End Network Performance Benchmark Scoring and Ranking*. ITU-T Recommendation E.840. https://www.itu.int/rec/T-REC-E.840/en.

ITU-T. 2019a. *Strategies to Establish Quality Regulatory Frameworks*. ITU-T Recommendation E.805. https://www.itu.int/rec/T-REC-E.805/en.

ITU-T. 2019b. *Measurement Campaigns, Monitoring Systems and Sampling Methodologies to Monitor the Quality of Service in Mobile Networks*. ITU-T Recommendation E.806. https://www.itu.int/rec/T-REC-E.806/en.

ITU-T. 2020a. *Crowdsourcing Approach for the Assessment of End-to-End QoS in Fixed and Mobile Broadband Networks*. ITU-T Recommendation E.812. https://www.itu.int/rec/T-REC-E.812/en.

ITU-T. 2020b. *Video Quality Assessment of Streaming Services over Reliable Transport for Resolutions up to 4K*. ITU-T Recommendation P.1204. https://www.itu.int/rec/T-REC-P.1204/en.

ITU-T. 2020c. *Methodology for QoE Testing of Digital Financial Services*. ITU-T Recommendation P.1502. https://www.itu.int/rec/T-REC-P.1502/en.

Marina, M.K., V. Radu, and K. Balampekos. 2015. "Impact of Indoor-Outdoor Context on Crowdsourcing based Mobile Coverage Analysis". AllThingsCellular '15: Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges, August 2015: 45-50. http://doi.org/10.1145/2785971.2785976.

Ofcom. 2016. *Digital Day 2016: Media and Communications Diary: Aged 6+ in the UK*. http://www.digitaldayresearch.co.uk/media/1086/aged-6plus-in-the-uk.pdf.

Ofcom. 2019. *Comparing Service Quality Research 2018: Reasons to Complain*. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/145819/reason-to-complain-research-2018-chart-pack.pdf.

Chapter 9. Emergency communications

9.1 Introduction

Telecommunications and information and communication technologies (telecom/ICTs) are critical for disaster management and risk reduction as they are used for monitoring the underlying hazards and delivering vital information to all stakeholders, including the most vulnerable societies at risk. The effective management of disaster risk depends on the level of preparedness and communication and information sharing across all levels of government, within communities, and between public and private organizations. In that sense, National Emergency Telecommunications Plans (NETPs) can articulate a strategy to enable and ensure communications availability during all four phases of disaster management: mitigation, preparedness, response, and recovery. The implementation of an NETP allows a country to minimize economic losses, mitigate negative impacts to public well-being and above all, reduce human fatalities (ITU-D 2020a).

Why do emergency telecom/ICTs matter?

Telecom/ICTs are becoming ever more important for all of us, and they come to the fore in managing disasters because of the different possibilities they enable. First, telecom/ICTs can help monitor the environment and the underlying hazards, as well as analyse information and data regarding potential disasters. During the mitigation and preparation phases, telecom/ICTs are used to facilitate the implementation of strategies, technologies, and processes that

can reduce death and property damage in potential disasters. Also, they are key to facilitating the dissemination of warnings and alerts so the public is aware of actions they must take during an emergency. Second, during the response and recovery phases, that is, during and after a disaster, telecom/ICTs and broadcasting services can provide interoperable and continuous communications capabilities for responders delivering vital information to coordinate response efforts (ITU-D 2020a). They can also help assess the damage and needs of the affected areas and population, identify locations in need of recovery assistance, track recovery and coordinate reconstruction activities, and help connect affected people with their friends and families.

In the case of an emergency like the COVID-19 pandemic, telecom/ICTs can help in assessing the impact of the virus and limiting its spread through facilitating physical distancing while keeping people in touch, for example, through social media or news bulletins, teleworking and tele-education, among other possibilities.

Emergency management systems can take advantage of emerging technologies to become more intelligent, secure, and effective. Particularly important for disaster management can be machine learning and extensive modelling using big data; sensors and actuators in robotics and Internet of Things (IoT) devices; or artificial intelligence (AI) and blockchain. These technologies can read, process, and transmit emergency-related data and assist emergency management personnel in their decision-making process during crises.

In that sense, it is important that authorities planning for emergency management consider a multitechnology approach, that is, include all possible mature and emerging technologies available, in order to facilitate the flow of vital information in a timely manner to all agencies and citizens involved in the process.

Which are the different types of hazards?

There are different types of disasters that can come from a number of hazards, which include weather-related hazards such as hurricanes, floods, storms, droughts, landslides, and so on, geological hazards such as earthquakes, volcano eruptions, and biological hazards which include epidemics, and pandemics, or those generated by extraterrestrial phenomena, just to mention a few (see Figure 9.1).

Disasters arising from natural hazards can occur regardless of human activity, so they are more likely to be mitigated than avoided.

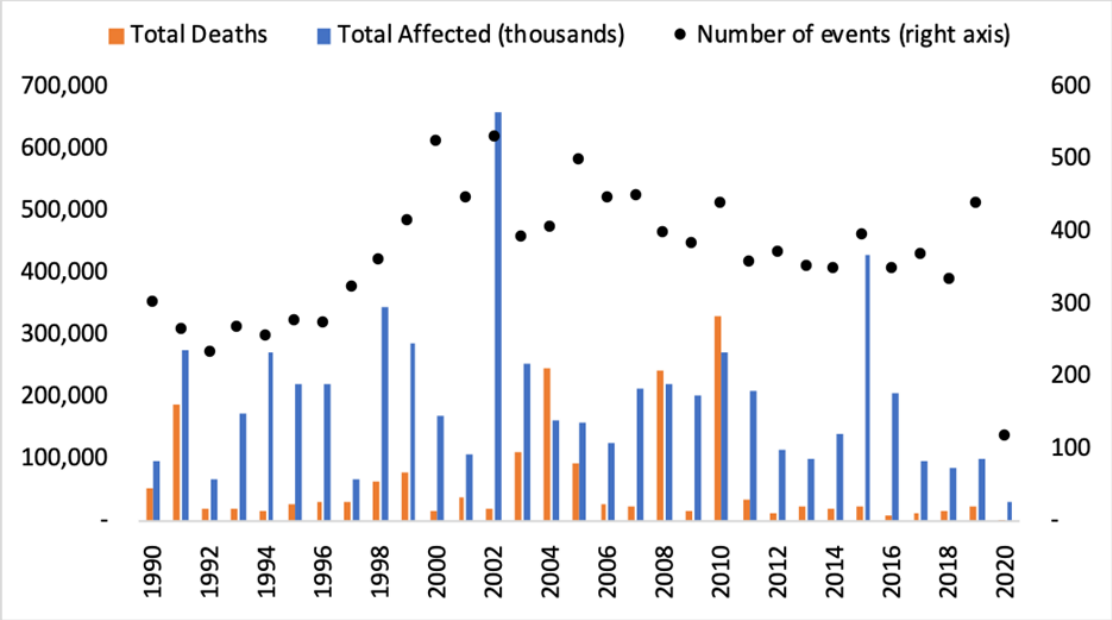
Figure 9.1. Types of natural disasters

Source: Guha-Sapir and others 2016.

The number and severity of disasters caused by natural hazards fluctuates year-by-year, as shown in Figure 9.2, covering the past three decades. Some years show a high number of disasters as well as a significant loss of life or an elevated number of people affected. Such is the case of the years 2002 and 2015, when the 532 and 440 disaster events reported, respectively, affected more than 650 million people in 2002 and nearly 270 million people in 2015, resulting in almost 330 000 deaths.

On the other hand, some years reflect that there is not necessarily a correlation between the number of events, the number of deaths, or the number of people affected. Such is the case of the year 2000, for example, when more than 500 natural disasters occurred, but only just over 16 000 deaths were reported.

Figure 9.2. Incidence of natural disasters worldwide, 1990-2020[a]



Note: a. Up to July 2, 2020.

Source: ITU, based on data from the Emergency Events Database (EM-DAT), https://www.emdat.be.

The previous figures show how different the effects of the various types of disasters can be on the population, and how much the impacts can fluctuate by year. The following are some examples of different disaster events that have occurred in the past two decades:

- In 2010, an earthquake in Haiti killed 222,570 people (66.7 per cent of all the deaths that year), while the people affected by that same ground movement (3.4 million) only represented 1.3 per cent of the total population impacted by disasters that year. On the other hand, two floods that also occurred in 2010 in China (riverine flood) and Pakistan (flash flood), respectively, generated 3,676 deaths (1.1 per cent of total deaths that year), but impacted nearly 150 million people, which represents 56.1 per cent of all the persons affected in 2010.
- In 2015, a drought caused by erratic rainfall in several provinces[1] in India affected 330 million people (77.1 per cent of the total affected population in 2015), but did not generate any reported deaths.
- In 2020, the COVID-19 pandemic is currently affecting or has affected almost every nation worldwide. The number of dead and affected are, as of yet, difficult to estimate, but it will likely have considerable effects on the global population and will account for severe economic impacts beyond the loss of human life.

Different types of disasters may show different effects on the population. Nonetheless, one commonality that they all share is that telecom/ICTs play important roles in the mitigation, preparedness, response, and recovery phases of the disaster management process. On one hand, even when disasters like floods and droughts, for example, do not have considerable impacts on telecommunications infrastructure, telecom/ICTs are key to warn or alert the population of incoming adverse weather conditions, or to facilitate coordination of response efforts, such as search and rescue or the distribution of food and the relocation of the population in shelters. On the other hand, during disaster events like earthquakes, which can cause severe damage to telecom/ICT infrastructure and numerous deaths, impacted areas can rely on telecom/ICTs to deliver vital information to first responders and government entities in charge of coordinating the response as well as in assessing the damage or identifying locations in need of recovery assistance, among other benefits. Finally, events such as the ongoing global pandemic also may take advantage of telecom/ICTs to facilitate social interaction, teleworking, education through online platforms and every other activity people perform on a daily basis, while maintaining physical distance to avoid continued propagation of the disease.

Accordingly, just as it is important to include all possible technologies available in order to facilitate the flow of vital information in a timely manner during the development of a NETP (i.e. a multitechnology approach), it is relevant to also consider a multihazard approach when developing or planning for telecom/ICTS for emergency management, and take into account all possible types of disasters that may occur.

[1] Tamil Nadu, Rajasthan, Jharkhand, Assam, Andhra Pradesh, Himachal Pradesh, Nagaland; Maharashtra, Bihar, Madhya Pradesh, Chhattisgarh, Telangana, Jharkand, and Odisha.

What should the regulator do?

Telecom/ICT regulators have major responsibilities in all four phases of disaster management. Taking as a starting point the national law or set of laws that describe high-level, general, and long-term telecommunication/ICT policies for disaster management needs, regulatory authorities need to issue appropriate rules and regulations to implement those national laws. Such rules and regulations should describe in detail the responsibilities, protocols, and strategies that each stakeholder should implement to effectively and efficiently use, provide, or facilitate emergency telecommunication/ICT services during national disasters. Considering that these rules and regulations also apply to telecommunication/ICT operators, it is important for the authorities to be open to understanding and flexible in the face of industry challenges (ITU-D 2020a).

These regulations should be established in advance of the actual occurrence of a disaster during the preparedness phase, with points of contact and general standard operating procedures widely known to all stakeholders. In the response phase, regulations should streamline the process to allow telecommunication/ICT services to be available as soon as possible. Therefore, regulators should consider, for example, expediting or facilitating temporary licences, issuing waivers, reducing any barriers for import/export of equipment, allowing for the free flow of experts who can assist in network restoration, or granting temporary spectrum permits and suspending spectrum/licence fees, among other actions (ITU-D 2020a).

It is important to consider that regulators, apart from the aforementioned responsibilities, must also actively contribute – or even lead – the development and implementation of the National Emergency Telecommunications Plan (NETP), which must include a description of the legislation, regulation, policies, as well as responsibilities of all authorities related to telecom/ICTs for disaster management. This plan should also be aligned with the country's established administrative structure and governance model for disaster risk management and should be developed based on a multistakeholder approach (see Box 9.1).

Box 9.1. Steps for developing a National Emergency Telecommunication Plan

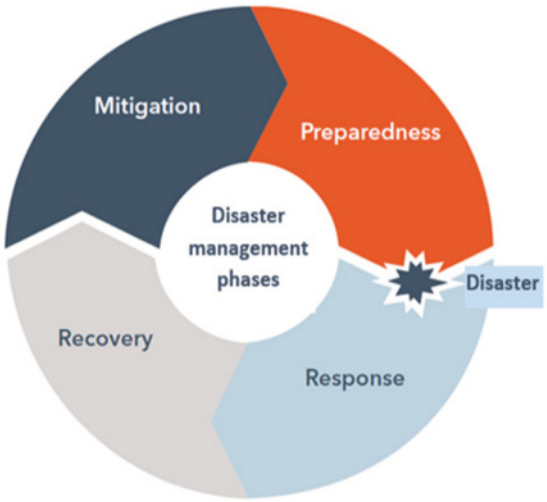
1. Conduct desk research to collect and analyse information regarding existing international cooperation, high-level government statements, policies, and regulation on telecom/ICTs for disaster management. Identify stakeholders and governance of the NETP development and acceptance process (ITU-D 2020a, Sections 3, 4, and 6).
2. Conduct desk research on historical disaster events, hazard profiles (ITU-D 2020a, Section 2), existing early warning and alerting systems, and telecom/ICT networks and services currently deployed (ITU-D 2020a, Section 5).
3. Hold a workshop to (a) present the overall need, strategy, and methodology to draft the NETP, including the development of capacities and drills, and support for people with specific needs (ITU-D 2020a, Sections 7 and 8); (b) present the initial findings from the desk research; and (c) discuss the findings and receive feedback. Government entities and private stakeholders related to disaster management and the provision of communications should be invited to the workshop.
4. Solicit input from and/or hold private meetings with each stakeholder to further discuss specific sections of the NETP, e.g. telecom/ICT network inventory with service providers, or specific regulations with national regulatory agencies, and so on.
5. Develop a first draft of the NETP, including the standard operating procedures, with the above inputs and following the guidelines set forth in this document.
6. Hold a second workshop to present the draft NETP developed in step 5. Receive additional feedback and modify the draft NETP as needed.
7. Request a peer review of the draft NETP from experts in the field. Also invite government entities and private stakeholders to review and comment on the NETP draft.
8. Review comments made to the draft NETP and make any necessary modifications to finalize the NETP.
9. Periodically review and update the NETP after every drill and operation to incorporate lessons learned, or at least every three years if no drill and operation occurs.

Source: ITU-D 2020a, Section 2.4.

What is the disaster management process?

The disaster risk management process adopted internationally by the United Nations Office for Disaster Risk Reduction (UNDRR) consists of four phases (ITU-D 2020a): mitigation, preparedness, response, and recovery, as described below (see Figure 9.3).

Figure 9.3. Phases of disaster management



Source: ITU-D 2020a, Figure 3.

- **Mitigation**: This phase seeks to carry out actions that lessen the likelihood of future disasters or the severity of their effects. The mitigation phase includes activities such as identifying existing risks, developing vulnerability assessments, and the construction or maintenance of the telecommunications infrastructure necessary to mitigate possible disasters.
- **Preparedness**: This phase comprises developing and testing plans to save lives and minimize disaster damage, ensuring readiness of the people and materials needed for disaster response, and issuing warnings about imminent disasters. Actions during this phase include the establishment of early warning systems, training, operational processes, and the development and implementation of written plans and procedures, such as a NETP.
- **Response**: This phase aims at providing emergency assistance, stabilizing the situation once a disaster has occurred, and reducing the chances of secondary damage. It includes activities such as search and rescue operations, the evacuation of affected areas, the opening of shelters, and distribution of food, among others. The role of telecom/ICTs during this phase is vital to connect stakeholders during the emergency response, especially considering that several entities carry out a variety of activities and procedures variously at the local, national and international levels.
- **Recovery**: The recovery phase focuses on providing the necessary aid to return to the initial levels of safety and functionality the community had before the disaster. Activities during this phase include debris removal, infrastructure reconstruction, and restoration of public sector operations, among others. This restoration and reconstruction must include the telecom/ICT infrastructure, especially because of the fundamental role that the sector plays within the community.

9.2 Mitigation phase

During this phase, telecom/ICTs play the role of disseminating information on how to mitigate the impacts of a possible disaster, and of supporting the implementation of strategies, technologies, and processes that can reduce those negative effects (ITU-D 2020a). In that sense, the telecom/ICT regulator is central to promoting the resiliency of critical telecom/ICT infrastructure, and to facilitate actions such as maintaining a periodically updated database that generates maps with all existing telecom/ICT networks; or a vulnerability and risk analysis

of all telecom/ICT networks. In addition, telecom/ICT regulations during the mitigation phase should consider regulatory actions like the following (ITU-D 2020a):

- Temporary licensing frameworks for both telecom/ICT services and radio frequencies for disaster relief.
- Suspension of licensing fees for temporary services for disaster relief.
- A process for waiving type approval/homologation of telecom/ICT equipment during disaster response.
- Require network redundancy and resilience for telecom/ICT operators of different services, i.e. mobile, fixed, terrestrial, satellite, and broadcasting, including contingency plans.
- Allow for priority call routing.
- Frequency allocation for public protection and disaster relief (PPDR) and other emergency needs (e.g. terrestrial and satellite services).
- Ensure regulatory flexibility, e.g. voluntary disaster reporting from telecom/ICT service providers, temporary licensing.
- Promoting the careful assessment of telecom/ICT network vulnerabilities based on the national risk assessments or vulnerability maps developed by the corresponding entity.
- Facilitating agreements among operators and between operators and emergency service organizations for the sharing of infrastructure and the prioritization of traffic, particularly in emergencies.
- Removing barriers to the import and deployment of people and equipment after disasters.

During the mitigation phase, an updated map of risks to, and vulnerabilities of, telecom/ICT networks should be in place in the country. This should be developed based on the national risk assessment or vulnerability maps for the country, and it should be developed for every hazard and for every region that may be at risk. It is essential to know the status of telecommunications, including what telecommunications carriers need to enable continued operation or restoration of networks and to take appropriate measures in advance to support the ability of carriers to exercise continuity plans in the event of a disaster (ITU-D 2020a).

According to the World Bank, different types of hazards can have distinct levels of impacts on telecommunications infrastructure. For example, earthquakes can have high negative effects on submarine cables and terrestrial underground cables, and medium effects on overland terrestrial cables, data centres, and wireless transmission antennas, as shown in Table 9.1.

The COVID-19 pandemic, on the other hand, is a type of disaster that does not directly damage physical infrastructure, but can cause indirect impacts such as network congestion owing to an increase in data traffic on both wired and wireless networks as confinement measures force a higher online communication demand. In consequence, the level of impact on the telecommunications infrastructure for this hazard could be considered low or medium in every case depending on the severity and duration of the measures taken to face the pandemic.

Table 9.1. Hazard effects on telecommunications infrastructure

Infrastructure	Inland and coastal floods	Earth-quakes	Tsunamis	Sea-level rise	High tempera-tures	Water scarcity	High winds and storms
Submarine cable (deep sea)	L	H	M	L	L	L	L
Submarine cable (near shore)	L	H	H	L	L	L	L
Landing station	H	H	H	H	L	L	L
Terrestrial cables (underground)	M	H	L	L	L	L	L
Terrestrial cables (overland)	L	M	L	L	L	L	M
Data centres	H	M	L	L	M	M	L
Wireless transmission antennas	L	M	L	L	L	L	H

Note: **H: High; M: Medium; L: Low.**

Source: Hallegatte, Rentschler, and Rozenberg 2019, Table 4.1.

Also, this phase should require considering infrastructure duplication. Making networks resilient calls for the elimination of single points of failure, especially for backbone cables and critical equipment such as authentication servers. Costs can be reduced by ensuring that competing operators have their own separately routed and equipped networks but agree that after a disaster they will make their networks available to each other. Such arrangements need care, both because they could weaken competition and because routes that are disjointed in one layer of a network could well be sharing a lower layer. However, having separately routed networks is not enough: there should actually be two routes from any point to any other point (except in "last mile" wireline access to customers). For this purpose, every network that provides interconnection services should offer two points of interconnection to networks that have no points of interconnection of their own.

Finally, mitigation should also comprise considering regulatory forbearance. External experts and equipment (including replacement or specialized equipment) are often needed urgently after a disaster strike. Therefore, before the occurrence of a disaster, it is important to have in place specific legislation that enables the arrival and timely installation of foreign communications equipment in the country, as well as the arrival of personnel who use emergency ICTs during catastrophes. Some of these goals might be achieved by national adoption of the *Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations* (ITU-D 1998). This international treaty aims to facilitate the use of telecommunication resources during the response and recovery phases of disaster management by establishing a framework for international cooperation between states, non-governmental entities, and

intergovernmental organizations. The Tampere Convention acknowledges the importance of countries temporarily abstaining from the application of national legislation on imports, licensing, and use of communications equipment during and after disasters, in order to facilitate the use of telecom/ICTs by emergency response teams. It also guarantees legal immunity to personnel who use emergency ICTs during catastrophes. In so doing, the Tampere Convention also ensures respect for the sovereignty of the country receiving assistance by giving the receiving state full control over the initiation and termination of the assistance, as well as the power to reject all or part of the assistance offered (ITU-D 2020a).

9.3 Preparedness phase

Telecom/ICTs in this phase of disaster management are essential for facilitating the dissemination of information and alerts so that the public is aware of the actions they must take during an emergency. Telecom/ICTs also facilitate the coordination and communication of the people involved in disaster management in this phase of response. In particular, key uses of telecom/ICTs in this phase are to provide early warnings and alerts and to develop or strengthen communications mechanisms. During the preparedness phase, it is important to develop the capacities of the personnel in charge of communications by executing training and drills, and to develop operational processes regarding communications by the establishment of written plans and procedures, such as the National Emergency Telecommunication Plan (ITU-D 2020a; ITU-D 2020b).

Drills and exercises, in particular, should include as many different stakeholders as possible from government, businesses, and non-governmental organizations (NGOs), as they enable stakeholders to rehearse procedures, identify gaps, and test plans that will come into effect during real emergency response operations. Also, during this phase, the outreach of the information given must be considered, as it should include not only certain key actors but the general public as well. Telecommunication providers, for example, can be expected to tell their customers about their own products, but not necessarily about communications more generally. In that sense, the regulator should require that telecommunication operators inform not just their employees but also their customers about the telecommunications plan before and after disasters. Included in such information should be explanations of warning messages, national emergency phone numbers, and rules and conventions to be applied after disasters. Additionally, this information should be repeated for each generation, and be disseminated by several different media (such as word of mouth, posters, newspapers, television broadcasts, radio broadcasts, web pages and social media), as it should reach homes, clubs, workplaces, schools, and rural communities.

Along with the above, the preparedness phase comprises hazard monitoring and forecasting. Monitoring environmental conditions using specialized equipment has long been a necessary part of preparedness. In this regard, it is important to consider that equipment has been falling in cost and rising in capability, and there are now many cheap and portable sensors and actuators available in IoT devices that can be powered using solar panels or long-life batteries that can communicate over long-range wireless networks. They are also well suited to risky and remote locations. Regarding hazard forecasting, which can demonstrate that a hazard is becoming worse and help determine whether warnings should be issued, there are now possibilities of exploiting cheap sensors, solar panels, and wireless networks from the IoT. In relation to disseminating these warnings, the Common Alerting Protocol (CAP) could be

considered, as it is a well-established mechanism for ensuring that early warnings and alerts are transmitted by different media (WMO 2012).

9.4 Response phase

The role of telecom/ICTs during this phase is vital to connect stakeholders that provide emergency assistance, as well as to help in stabilizing the situation once a disaster has occurred, and reducing the chances of secondary damage.

Following a disaster, networks might need to be repaired and supplemented by other elements. Spare equipment might need to be transported from relatively safe locations or even imported into the country. Temporary mobile base stations, sometimes with extensible masts, such as cells on wheels (COWs) and cells on light trucks (COLTs), have various commercial uses and are commonly available in disasters (GSMA 2020). If there is too little terrestrial connectivity, satellite networks might be used instead; while in circumstances where mobile base stations or the satellite network are not available, some unmanned aerial vehicles (UAVs) and high-altitude platform stations (HAPS) could be helpful, as they can relay traffic widely and observe sites from above (Li 2017).

During this phase, telecom/ICTs may also be helpful in assessing damage. Data about the impact of a disaster on people and assets must be collected, disseminated, and processed. Existing sensing equipment might still be able to operate and communicate useful readings. Aerial survey planes, satellites, and high-altitude UAVs can give broad pictures; drones, which are low altitude UAVs, can provide further detail when equipped with lights and cameras. Also, knowing where people are located is particularly important so that relief efforts can be efficient and effective. For this purpose, as mobile phones transmit to nearby base stations, population movements can be assessed by tracking which phones use which base stations (Bengtsson and others 2011). Mobile phone call detail records provide the information needed. Regarding search and rescue work, robots equipped with sensors and drones can be a helpful complement to humans and dogs.

Immediately after major disasters, many national and international organizations collect and analyse information in order to plan the response. Therefore, it is relevant that countries develop National Emergency Management Plans and, in the case of telecom/ICTs, National Emergency Telecommunications Plans with a multistakeholder approach, that take into account all agencies and people involved in the emergency management process, whether they are national or international actors.

9.5 Recovery phase

The recovery phase focuses on activities such as removal of debris, restoration of public sector operations, and reconstruction of infrastructure, including telecommunication infrastructure. Telecom/ICT networks and services should be used in this phase to help assess the damage and needs of the affected areas and population, identify locations in need of recovery assistance, track recovery activities, and coordinate reconstruction activities (ITU-D 2020a).

After a disaster, reviewing the available lessons learned is essential to reducing the effects of the next one. Therefore, reviews can be useful to consider what worked well and what needs improvement at national and local levels.

Reconstruction of the telecommunications infrastructure should follow soon after the disaster, and should consider rebuilding more resilient telecom/ICT network infrastructure and include potential redundant network deployments wherever possible to prepare for future disasters. Government and the private sector should also take advantage of the opportunity to rebuild relevant telecom/ICT infrastructure and, where possible, to deploy technologies that are more resilient, efficient, and less expensive (ITU-D 2020a).

In reconstructing their networks, operators can take the opportunity to ensure that they can conveniently monitor and control network nodes and supervise sensors. In particular, they might install sensors in outside plants, for reporting properties like temperature and humidity, and informing employees about urgent priorities. In utility sectors other than telecommunications, such as electricity and water, they might also stimulate actuators.

On the other hand, the regulator needs to monitor improvements so that the infrastructure is "built back better." In particular, the infrastructure as a whole (though not necessarily the network of any individual operator) needs to be resilient enough to deal with the next disaster and arrangements for coordination need to be put in place and practised.

References

Christian, E., 2012. "Introducing the Common Alerting Protocol (CAP)." https://etrp.wmo.int/pluginfile.php/16462/mod_resource/content/0/CAP-101-Notes.pdf.

GSMA, 2020. *Building a Resilient Industry: How Mobile Network Operators Prepare for and Respond to Natural Disasters*. London: GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/TWP5861_BuildingAResilientIndustry_v003.pdf.

Guha-Sapir, D., P. Hoyois, P. Wallemacq, and R. Below. 2016. *Annual Disaster Statistical Review 2016: The Numbers and Trends*. Brussels: CRED. http://emdat.be/sites/default/files/adsr_2016.pdf.

Hallegatte, Stephane, Jun Rentschler, and Julie Rozenberg. 2019. Lifelines: *The Resilient Infrastructure Opportunity*. Washington, DC: World Bank. https://openknowledge.worldbank.org/handle/10986/31805.

ITU-D. 2020a. *ITU Guidelines for National Emergency Telecommunication Plans*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/NETP-guidelines.pdf.

ITU-D. 2020b. *Emergency Telecommunications Table-Top Simulation Guide*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Publications/2020/TTX_Guide.pdf.

ITU-D. 1998. *Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Tampere_Convention/Tampere_convention.pdf.

Li, A. 2017. "Alphabet Deployed Emergency LTE to Puerto Rico with Project Loon in Under a Month." 9TO5Google. October 20, 2017. https://9to5google.com/2017/10/20/alphabet-x-project-loon-puerto-rico-live/.

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)
Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)
Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)
Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt
International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand
International Telecommunication Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU) Area Office
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland
International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-31661-7

Published in Switzerland
Geneva, 2020
Photo credits: iStock