TRENDS IN TELECOMMUNICATION REFORM 2016

REGULATORY INCENTIVES TO ACHIEVE DIGITAL OPPORTUNITIES

© ITU 2016 International Telecommunication Union
Place des Nations
CH-1211 Geneva, Switzerland

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of the International Telecommunication Union.

Denominations and classifications employed in this publication do not imply any opinion on the part of the International Telecommunication Union concerning the legal or other status of any territory or any endorsement or acceptance of any boundary. Where the designation "country" appears in this publication, it covers countries and territories.

ISBN 978-92-61-16551-2

This report was prepared by the ITU experts Iqbal Singh Bedi, Ian Brown, Urs Gasser, Mercy Wanjau, Malcolm Webb, under the direction of the ITU Regulatory and Market Environment Division. John Alden edited the report.

We would especially like to thank the moderators of the ITU Global Symposium for Regulators (GSR-15) held in Libreville, Gabon in June 2015, for their support and appreciation on the content of the various chapters expressed during the event.

These contributions, together with the support from ICT ministries and regulators, and others who have provided data and background material, are gratefully acknowledged. Without their support, a report of this nature would be impossible.

Foreword

The digital world of the 21st Century offers a world of opportunities through apps and services in the fields of e-governance, telemedicine, mobile banking and online education. ICTs help in achieving the Sustainable Development Goals by opening doors to economic growth, socio-economic development and vast improvements in the lives of individuals and communities. To realize the full potential of the digital economy, policy-makers and regulators have a key role to play in building policy and regulatory environments in which new technologies can flourish. That is why this 16th annual edition of *Trends in Telecommunication Reform* focuses on the theme of "exploring regulatory incentives to achieve digital opportunities." I believe the theme upholds the ultimate goal of regulators: serving our citizens. This edition is a compilation of discussion papers presented at the 2015 edition of the ITU flagship event, the Global Symposium for Regulators (GSR) and seeks to explore ways to ensure that citizens can benefit from economic and social opportunities brought about by the digital economy, recognizing that for digital opportunities to fully materialize, an adaptive, consultative and innovative approach to policy and regulation is needed, more than ever before.

Across the globe, mobile broadband is growing rapidly as 3G and 4G networks are deployed. The "Internet of Things" will make our cities smarter and our utility grids more efficient and cost-effective. More interconnected networks and interoperable systems will blossom into greater network effects, boosting value for every subscription. Greater capacity and localized content will generate more demand, creating even more incentives for greater investment, which in turn will create even more capacity.

While interoperability brings the full value of a digital ecosystem, it also entails vulnerabilities to cyber-crimes, malware and privacy abuses. This edition attempts to identify solutions to these challenges.

I believe that the cross-sectoral nature of the digital world will require more versatility, more agility and more cooperation with regulators in other fields, such as health, education, finance, broadcasting and law enforcement.

Regulators need more than ever to engage in a balancing act through public-private partnerships, technology test-beds and new product incubation programmes.

ITU-D's effort to engage and hold an inclusive dialogue for regulators to serve their citizens continues. With this new edition, I invite you once again to take part in this inclusive dialogue, which has been so fruitful over so many years. Let us welcome each other again as partners in exploring how to open up the online world for all of us, for all the world's digital explorers.

Brahima Sanou
Director
Telecommunication Development Bureau (BDT)

Table of Contents

List of tables, figures, charts and boxes

Tables

Figures

Boxes

Chapter 1: Investment strategies for broadband deployment and access to the digital economy

This chapter describes both common and innovative investment strategies that have been implemented to support the deployment of broadband infrastructure and access to the digital economy. The chapter draws upon practical examples from a wide range of countries to describe current information and communication technology (ICT) investment trends and to recommend best practices for regulators wishing to foster and secure new investment opportunities. Although this sampling of case studies is not statistically representative and does not enable significant conclusions to be made, some themes do emerge, and these are summarized in this chapter.

Telecommunication investments in developing markets tend to focus mainly on developing mobile infrastructure, with the aim of increasing voice, data and broadband service penetration. In contrast, mobile operators in developed markets are more likely to invest in Long-Term Evolution (LTE) networks to reverse declining revenues by offering high-speed mobile data services and applications. Meanwhile, new-entrant, fixed operators in developed markets are investing in gigabit broadband networks, since consumer demand for bandwidth-hungry content is expected to increase.

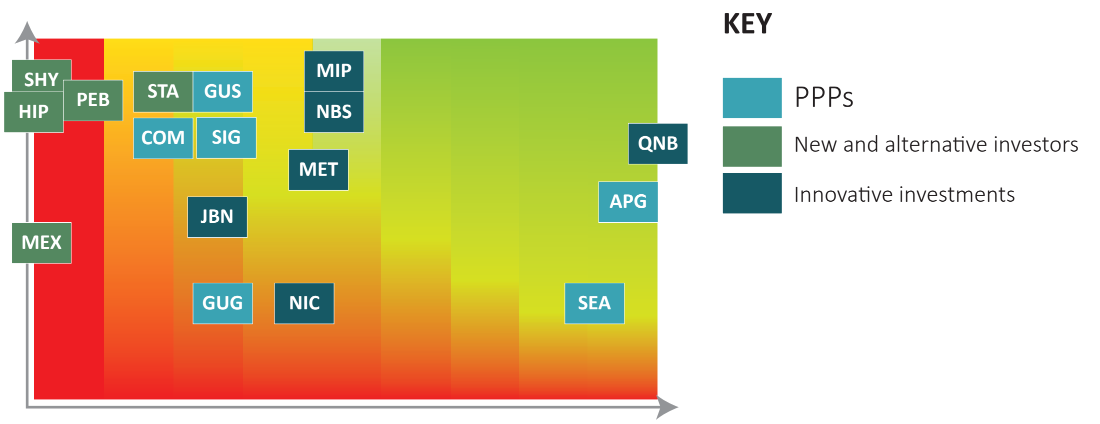
Industry consolidation, in the forms of network sharing or mergers and acquisitions, also is driving investment in both fixed and mobile networks. The improved efficiencies and cost-savings realized through consolidation often prompt operators to fund increased network investment. Governments and policy-makers can encourage investment in networks and services by creating and supporting "tech clusters," which have the added benefit of creating jobs and growth in digital industries.

It is still common for governments to fund broadband networks using public-private partnerships (PPPs) in areas where it is not commercially viable for operators themselves to invest in broadband infrastructure. There is a distinction, though, between how PPP projects are implemented in developing markets and how they are completed in developed markets. PPPs in developing markets are more likely to focus on building national, core networks and metro rings, while PPP projects in developed markets tend to focus on increasing last-mile broadband coverage and achieving very high download speeds.

Regulators can play a key role in PPP projects by encouraging infrastructure sharing and spectrum pooling, and by issuing licences with coverage and performance obligations. Regulators should provide operators maps showing existing network coverage and passive infrastructure to aid their network planning. Regulators can also ensure that operators offer effective, non-discriminatory and transparent access to dominant or government-funded networks. (Detailed analysis will be required, however, to ensure that existing operators are not dissuaded from further investment by such regulations.) Subject to local constraints, regulators should also consider allowing incumbent operators to sell assets, such as copper networks, which can be used to offset the costs of future investment in broadband networks.

New market entrants such as Google, Microsoft and Facebook have invested in broadband networks and emerging technologies. They are motivated to generate downstream revenues by leveraging demand for their content into greater use of widespread broadband networks. Regulators can play an important role in attracting such new market entrants by providing clarity on passive infrastructure-sharing rights, working with local and national governments to promote technology pilots, and supporting community broadband initiatives. They can also help new entrants by expediting licence applications and easing civil planning and construction restrictions. Governments and regulators can proactively champion pilot projects that explore disruptive technologies, such as using broadcasting (i.e "TV white-space") spectrum to promote broadband services in rural areas not considered to be

Figure 1.1: Summary of investment trends



Abbreviations

MIP	Mobile Infrastructure Project
NBS	National Boradband Scheme
NIC	national ICT Backbone (NICTBB)
JBN	Johannesburg National Broadband Project
MLi	Metroweb
QNR	Qatar NRN
GUS	Google US
GUG	Google Uganda
COM	Community broadband
SIG	SIGFOX
APG	Facebook Asian-Pacific Gateway
SEA	Seacom
SHY	Shyp
HIP	Hipcom
MEX	meXBT
STA	Star Citizen
PEB	Pebble

Source: Analysys Mason, 2015. Note figures are not abailable for MGTS

commercially reachable with more traditional network approaches.

The case studies cited in this chapter provide an interesting insight in investment trends, particularly when the value of the investment is plotted against the economic maturity of the region where the investment was made (see in Figure 1.1).

New market entrants and alternative investors (technology innovators, not-for-profit investors and financial institutions such as private-equity or hedge funds) tend to make higher-value (and therefore higher-risk) investments than do PPPs. Moreover, investors are equally likely to invest in both developed and developing markets.

Innovative investments using crowdfunding, digital currencies, pensions and charities largely involve higher-layer services and developed markets. This is partly due to the maturity of the Internet ecosystems in those developed markets, which foster technical innovation. Most of these investments have initially attracted low amounts of funding – with the exception of crowdfunding – and would therefore be unsuitable for investment in significant broadband infrastructure projects. There is generally less government regulatory involvement in attracting this form of investment. This chapter argues, however, that governments and regulators still should be responsible for attracting inward investment and for stimulating the demand for broadband services that will drive investment in higher-layer services and connectivity. Any financial regulations being considered in growth markets should safeguard investors and consumers and enable innovation without restricting business growth.

Chapter 2: Accelerating Broadband Deployment Through Network Sharing and Co-investment

Most governments have a policy objective to increase the availability of affordable broadband services. This often requires deploying new mobile and fixed broadband networks, but these are expensive to build and entail high construction and demand risks. Accelerating broadband deployment, particularly outside the main urban areas, is challenging and requires innovative solutions.

This chapter examines the potential solutions of network sharing and co-investment by multiple operators and other players, including governments, in building new broadband infrastructure. Governments often favour sharing arrangements to promote broadband deployment, and this chapter examines why and how they encourage network sharing and co-investment, as well as the benefits to consumers. It also examines why, in some cases, governments have *not* promoted network sharing. Commercially driven network sharing has been prevalent, for example, in the mobile sector-- particularly in countries with competitive mobile service markets-- but it remains relatively rare in the fixed-service sector.

In examining options for encouraging and incentivizing sharing, it is clear that sharing arrangements are complex and difficult for operators to set up – a reality reflected in the fact that many have not survived for very long. This chapter considers some reasons why, despite the cost- and risk-sharing benefits to operators, there have not been more enduring sharing arrangements.

With this in mind, the chapter looks at some ways governments can encourage and provide incentives for sharing. One favoured approach is for governments to contribute assets and infrastructure, potentially through public utilities, in co-ventures with private operators. There is also real benefit in governments' providing a high degree of up-front certainty about regulatory treatment of sharing arrangements for new network build-outs.

Network sharing and co-investment have a compelling logic if they can be made to work. This chapter concludes by looking at some new ways in which network sharing may arise in the future, including through the emergence of so-called *smart cities*.

Chapter 3: Regulation and the Internet of Things

This chapter examines the implications of the *Internet of Things* (IoT) for individuals, businesses and societies. In particular, it examines the issues that telecommunication and other regulators need to consider as IoT systems proliferate in developed and developing economies alike.

Broadly speaking, IoT refers to the inclusion of communication and sensing capabilities into a very wide range of physical objects. In the next decade, technology companies and consulting firms expect tens of billions of IoT devices to be deployed, driven by an ongoing and rapid reduction in the cost of sensors, processing and networking technologies.[1] Consumers will encounter IoT in everything from parking meters, thermostats, cardiac monitors, tires, roads and car components, to supermarket shelves and many other types of physical objects and appliances. IoT-enabled objects and devices can share data directly using protocols such as Wi-Fi and Bluetooth, via mobile phone networks and specialized radio networks, or over the global Internet.

Device manufacturers, network operators, application platform architects and software developers are forming a broad ecosystem that is even now developing IoT services. Data analytics services, often cloud-based, are also important components of the new environment. IoT systems support a broad range of applications, including monitoring and managing individual health and wellbeing, improving energy efficiency, increasing industrial process quality and reliability, and reducing traffic congestion. They will empower the development of new products and services – especially ones based on pay-per-use charging.

IoT devices will have the biggest societal impact where they are used together in larger, inter-connected, systems. At the macro-level, two of the areas of greatest IoT development and investment are:

(1) "Smart cities" – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities; and

(2) Smart power and water grids – which will see improved efficiency in the transmission of power and the monitoring and maintenance of delivery systems.

Individual consumers increasingly will see "connected vehicles" with hundreds of separate sensors, making them safer, more reliable, and better able to participate in sophisticated congestion management systems. As populations grow – and in many cases grow older – governments can meet health and wellbeing challenges by helping to put IoT systems in the hands of individuals, care-givers, doctors and hospitals. Connected devices such as insulin pumps and blood-pressure cuffs can monitor patients and report warning signs of conditions such as diabetes and heart disease.

Both the public and private sectors are continuing to fund significant levels of IoT research and development in areas such as modularity, reliability, flexibility, robustness and scalability. But the basic capabilities needed for many applications are already well understood and becoming available through smart phones and other standard platforms. These devices also will address some of the cost issues that have held back growth in the past, although cost and reliability remain issues for large-scale systems, as dœs connectivity. One significant opportunity is the greater use of open data and Application Programming Interfaces (APIs), which can enable a higher level of innovation in IoT systems.

As IoT systems grow, two types of issues become more urgent: connectivity issues (i.e., between machines and between machines and humans) and addressing issues (i.e., ensuring sufficient addressing resources are available to accommodate the millions of connected devices). Enabling peer-to-peer connections between devices can increase the reliability of communications, compared with requiring a large and complex global network. But when devices must be globally reachable – most commonly, via the Internet – a large address space is required to individually identify each device. The need to meet this requirement underlines the benefit of globally adopting the next version of the Internet Protocol, IPv6.

The purpose of this chapter is to raise awareness among the ICT regulatory community of the changes prompted by the advent of IoT. It will examine the current and future challenges and opportunities in an effort to understand how IoT is impacting consumers, businesses, governments and society at large. There are particular regulatory implications for licensing and spectrum management, switching and roaming, addressing and numbering, competition, security and privacy. Some of these issues are familiar to telecommunication regulators and others may be areas in which different regulators typically take the lead.

The Internet of Things

What Is It?

"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" (ITU-T)

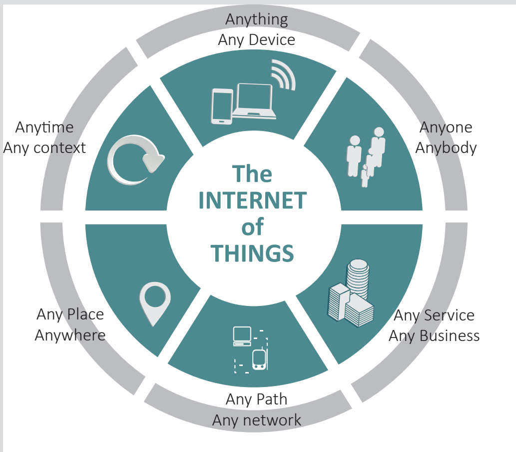
Who Makes It?

Device manufacturers, network operators, application platforms, software developers and (cloud-based) data analytics services providers

How Is It Accessed?

Connection of IoT devices via Wi-Fi, Bluetooth, mobile phone networks, specialized radio networks, global Internet

Figure 3.1: The Internet of Things, in a nutshell



Main current areas of investment

- Smart cities
- Smart metering & grids
- Connected vehicles
- Healthcare

Main Impacts

- Monetary/economic impact: trillions of dollars annually within a decade
- Societal impact: Smart cities – infrastructure, transport and buildings – by improving efficiency and sustainability of a whole range of urban activities; smart power and water grids (smart meters)
- Individual impact: e.g. transport safety through "connected vehicles"; population health and wellbeing can be enhanced, enabling e.g. care at home

Challenges

- Cost needs to fall, reliability needs to improve
- Issues of connectivity, user interfaces and addressing
- Regulatory implications for licensing and spectrum management (access required to 300 MHz-3GHz but also NFC at 13 MHz or EHF bands, AM/FM bands in VHF range, Wi-Fi and 4G mobile networks), standards (interoperability e.g. ITU-T's initiative IoT-GSI), competition (e.g. impact on competitiveness of different markets, customer lock-in due to fixed SIMs in each device etc...), security and privacy ("by design" approach desirable)

Chapter 4: Interoperability in the digital ecosystem

At the most basic level, *interoperability* (or "interop") is the ability to transfer and use data and information across different systems, applications, or components. Interop is invisible, and yet crucial, to many parts of a highly interconnected, modern society. The fact that someone can make a seamless international telephone call without thinking about things like signaling standards or transoceanic cables is a tribute to interop. So is the fact that one can send and receive the same e-mail on a mobile phone or in a browser, regardless of device manufacturer or Internet service provider. Importantly, the Internet of Things relies on interop. For that reason, it is critical to develop a shared understanding of how interop functions, the potential costs and benefits of increased levels of interop, and the variety of approaches for encouraging interop.

This chapter begins by offering a framework for understanding interop as a concept. Figure 4.0 provides an overview of the concept of interop, its benefits, potential risks and approaches.

In theoretical terms, interoperability functions across four broad layers of complex systems: technological, data, human and institutional. When many people think of interop, they think of the exchange of data through technological means. But it turns out that the human and institutional aspects of interoperability are often just as important – and sometimes even more important – than the technological aspects.

This chapter offers examples of some of the many benefits and drawbacks of higher levels of interop. The benefits include innovation, competition, choice and access. Drawbacks can include security and privacy risks; an increase in homogeneity; a decrease in reliability, accountability and accessibility; and a threat to certain existing business models.

The chapter then offers a taxonomy of the various approaches for managing and optimizing the level of interop. These approaches can be deployed either in a unilateral fashion or in more collaborative ways. Moreover, some approaches can be deployed by the private sector, while regulators and other state actors utilize others. The chapter also considers in depth the unique role that governments and regulators can play in shaping the interop landscape. Finally, the chapter concludes by identifying some of the biggest questions and challenges for interoperability among future technologies.

Chapter 5: M-services and applications: Perspectives on regulatory measures to foster diffusion and access

Mobile services and applications are playing a prominent role within the broader digital ecosystem to unlock economic opportunities and provide critical services to citizens. As consumer demands are placed on them, disruptive technologies and innovation are bringing about new possibilities for the future. Governments, regulators, consumers and indeed the world are only beginning to understand the true development potential of mobile services and applications. A few truths are emerging.

First, the old telecommunication "rules of engagement" may not stand the test of time, and some aspects of regulations may need to be re-written to address the changing environment. There is a need to depart from rigid rules and to adopt a "light-touch" approach in order for the regulatory framework to be more responsive to the innovative ecosystem of m-services and apps. The regulatory scope of competition, universal service, resource allocation, interoperability and standards (among others) needs to be reviewed.

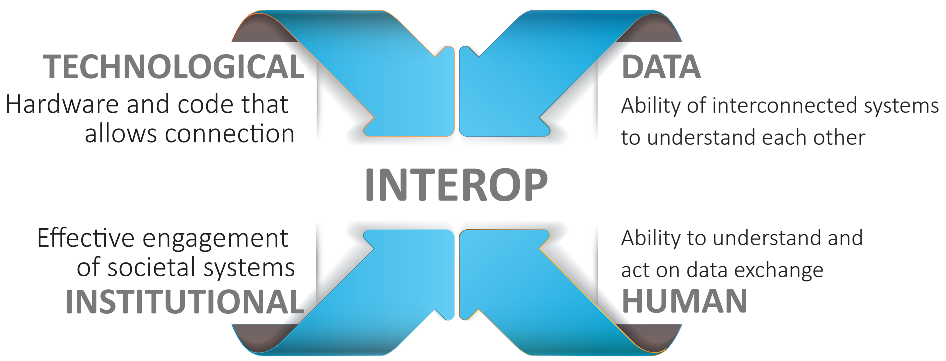
Second, sector regulators have been thrust into a multi- sectoral space, due to the cross-cutting nature of disruptive innovation. This has broadened their domain and capacity to influence regulation and policy across sectors. But regulators must reach out and collaborate proactively, not just reactively, going forward. In addition, the multi-sectoral entry has brought in new stakeholders, which the sector regulator needs to identify and engage in order to leverage for mutual benefit.

Third, a flexible, transparent approach that promotes competition will allow innovation to thrive and provide incentives for investment and, ultimately, consumer benefit. Greater consideration is, therefore, required in the development of regulatory frameworks that will govern the growth of the digital ecosystem in order to ensure that it continues to surprise the world and stretch the imagination with new ideas and innovations.

For this to happen, the regulator needs to adopt a delicate balance. It has long been recognized that regulation can have an impact on innovation, both positively and negatively. Regulators need an awareness to foster the inter-dependencies necessary to enable the digital ecosystem to evolve into a healthy environment. But they also have to deter and punish discordant players for rule violations. This balance requires a resolute approach and stakeholder support. Otherwise, innovation can tend to take a backseat when straddled by complex issues and uncertain rules.

This chapter seeks to explore regulatory perspectives that can be considered in facilitating

Figure 4.0: Overview Diagram of interop



Source: ITU

use and access and, in so doing, reviewing regulatory constructs that have become barriers over time. It suggests that efforts must be made to place the consumer at the center of the digital ecosystem by installing consumer safeguards. This would entail a deliberate focus on consumers with disabilities, to ensure inclusion at all levels.

The chapter encourages regulatory approaches that will ensure there is a balanced, proportionate and robust mechanism for players in the digital economy to flourish, so that development goals can be realized. In this way, m-services and apps can leverage the phenomenal growth of mobile services. This powerful technology is available in most rural and remote areas, empowering development in areas such as healthcare, education, agriculture, commerce, banking and so on.

Chapter 6: Conclusion

This chapter brings together the topical issues discussed through the chapters of this edition of Trends by reflecting on the last steps to the digital economy, from building the foundation through connectivity, to connectedness, in higher layers, to a digitally connected ecosystem. The role of governments is key exploring regulatory incentives to achieve digital opportunities.

Endnotes

1 Cisco Systems, *Internet of Things Connections Counter*, at http://blogs.cisco.com/news/cisco-connections-counter

1 Investment strategies for broadband deployment and access to the digital economy

Iqbal Singh Bedi, Nuno Afonso and Dr Matt Yardley, Analysys Mason

1.1 Introduction

This chapter identifies strategies that private and public investors have implemented to support deployments of broadband infrastructure and greater access to the digital economy. Based on a review of investment cases from around the world, this chapter identifies best-practice investment strategies and variations from different regions and service markets. It also identifies key lessons for governments, regulators and investors to stimulate investment in broadband networks.

The purpose of the chapter is not to focus on any single investment approach or example, but rather to provide an overall view of the best practices used to encourage investment in the digital economy.

The chapter highlights global investment trends and considers regional and industry variations. It also examines public-private partnership (PPP) investments and alternative, innovative approaches to funding.

The chapter has been prepared using secondary research based on publicly available information. Unfamiliar investment cases have been selected deliberately to provide a fresh perspective, and familiar examples that have already been researched extensively have not been used. The investment cases provided do not represent an exhaustive list of examples, but they have been selected carefully to present a wide a range of cases from around the world, allowing investment trends to be identified.

Table 1.1: Case studies covered in the chapter by type of investment strategy and region

Types of investment/activity	Developing regions	Developed regions
Public-private partnerships (PPPs)	• National ICT Broadband Backbone (NICTBB), Tanzania • Johannesburg Broadband Network Project (JBNP), South Africa	• Mobile Infrastructure Project (MIP), UK • National Broadband Scheme (NBS), Ireland • Metroweb, Italy • Qatar National Broadband Network (QNBN), Qatar
Alternative approaches	• Google Fiber, Uganda • Seacom, Africa • Asia-Pacific Gateway, Asia	• MGTS, Russia • Google Fiber, USA • SIGFOX, France • Community broadband, Germany
Financial innovations	• mexBT, Mexico • Aentropico, Colombia	• Star Citizen, USA • Pebble, USA • Shyp, USA • Hipcom, UK

The remainder of the chapter will unfold as follows:

- Section 1.2 provides an overview of telecommunication and ICT infrastructure investment trends worldwide.
- Sections 1.3 and 1.4 examine investment and implementation approaches for PPP projects.
- Section 1.5 investigates alternative funding approaches that can be used to facilitate the roll-out of broadband infrastructure.
- Section 1.6 provides an overview of financial innovations for funding investments, mostly in higher-layer services and applications.
- Section 1.7 summarizes some conclusions regarding the investment trends explored in the chapter.
- Sub-section 1.7.2 provides a summary of best-practice regulatory considerations.

1.2 Global investment trends

The global telecommunication marketplace is vast, and each market varies depending on its own unique set of macro-environmental characteristics. Fixed and wireless telecommunication operators and higher-layer service providers – whether in developed or developing markets – have had to adapt to local conditions. Consequently, they have developed a range of different strategies to remain competitive and to invest in broadband infrastructure. This section provides a summary of the investment trends being exhibited by operators investing in fixed and wireless broadband networks and higher-layer services.

1.2.1 Investment: driving telecommunication revenue growth

Operator investment in fixed and wireless networks is driving revenue growth in both developing and developed markets. The global telecommunication services market[1] will be worth an estimated USD 1.79 trillion in 2019, up from an estimated USD 1.68 trillion in 2014 (Figure 1.2).

In developing markets, current service availability and penetration rates for mobile broadband remain low: for example, there is a 19 per cent penetration rate in in Africa and 23 per cent in the Asia and Pacific region. Penetration rates are even lower for fixed broadband services, with a 0.4 per cent rate in Africa, 3 per cent in the Arab States and 7.7 per cent in the Asia and Pacific region[2]. But an increase in investment in 3G and (in time) LTE mobile infrastructure is expected to drive growth and increase service penetration, leading to the higher revenues depicted in Figure 2.2. Aided by increasing gross domestic produce (GDP) per capita, economies such as China, Brazil and India are expected to see increased revenue growth – driven mainly by investment in mobile infrastructure and mobile broadband services.

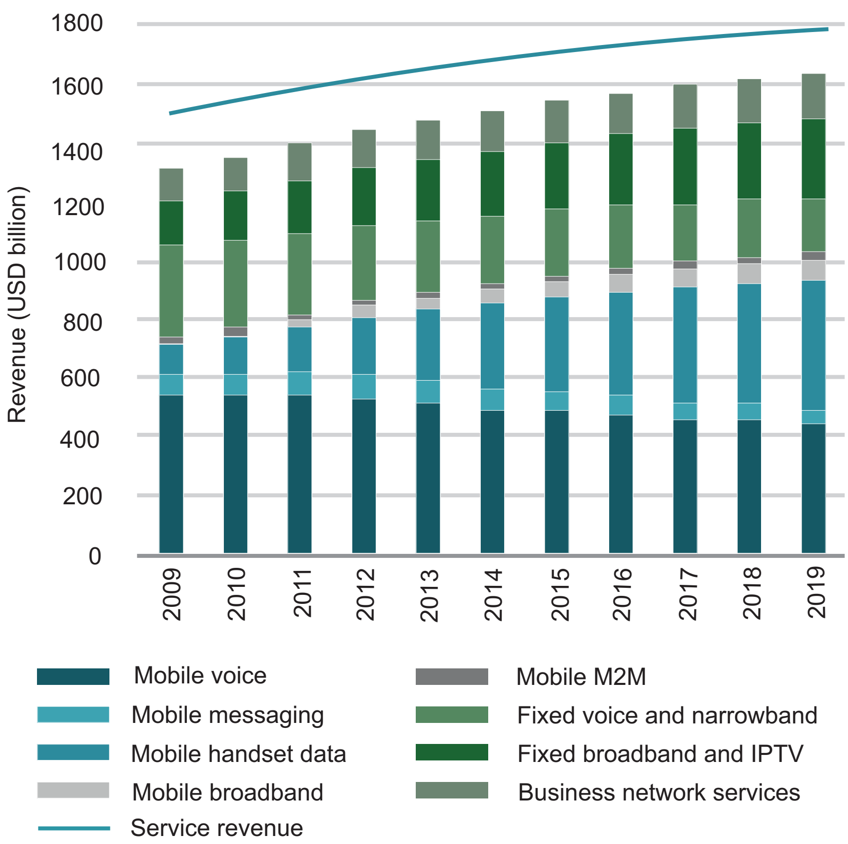
In developed markets, current service availability and penetration rates remain high for mobile data – 64 per cent in Europe, for example. In addition, nearly 79 per cent of all fixed broadband connections globally are in Europe and in the developed markets in Asia. Mobile operators have been making significant investments in LTE networks and offering attractive mobile data services and applications. As a result, revenue growth will come from higher consumer spending. Growth will be particularly high in Japan, Korea (Rep. of) and the United States (which are the world leaders in terms of LTE take-up and data usage), but also in some European markets (as LTE gains traction). Incumbent and alternative fixed operators in developed markets also have been investing in fibre networks to create ultra-fast broadband networks capable of speeds of up to 1 gigabit per second (Gbit/s).

The sections below discuss the fixed and wireless investment trends in further detail.

1.2.2 Fixed network investment trends

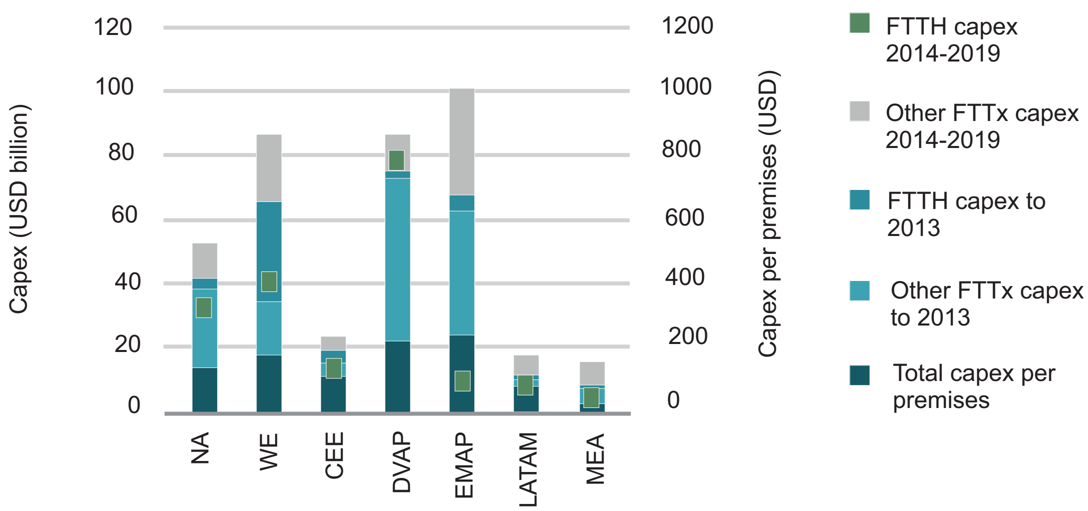
Operators' investment choices will vary in terms of different fibre technologies. Capital expenditures on fibre infrastructure (expressed as "fibre to the x" or "FTTx," with x standing for "home" or "premises") are expected to total USD 144.2 billion between 2014 and 2019. USD 52.5 billion of that will be in Western Europe and USD 55.1 billion will be in developing markets (see Figure 1.3)[3 4].

Figure 1.2: Telecommunication retail revenues by service type and total service revenue, worldwide



Source: Analysys Mason global telecoms market: interim forecast update 2014–2019

Figure 1.3: FTTx capex by region to 2019



Source: Analysys Mason FTTx roll-out and capex worldwide: forecasts and analysis 2014–2019

Note: (NA = North America, WE = Western Europe, CEE = Central and Eastern Europe, DVAP = Developed Asia-Pacific, EMAP = Emerging Asia-Pacific, LATAM = Latin America, MEA = Middle and East Africa)

Some USD 92.7 billion of this forescast total will be spent on fibre to the home (FTTH)[5], of which USD 46.2 billion will be spent in developing markets.

Fibre networks appear to be favoured over copper networks by fixed network operators in developing markets. Also, the low availability and poor quality of copper networks in developing markets can make them unsuitable for investment.

Fixed incumbent operators in developed markets, meanwhile, are more likely to adopt a gradualist investment approach in order to leverage their copper network assets and introduce a mix of FTTx access approaches, including FTTH. In contrast to incumbent operators, new market entrants are deploying gigabit fibre networks in cities, as they are not restricted by legacy investments in copper networks. This is the case with Gigaclear and CityFibre in the UK, and Google Fibre in the United States and Africa.

1.2.3 Wireless network investment trends

Mobile operators in developing and developed markets are expected to make significant investments in 3G LTE networks to leverage the growth in mobile data services. Mobile broadband penetration in developing markets is still quite low, however, with a penetration level of 21 per cent in 2014. But mobile broadband is growing fast in these regions – in fact, growth rates are twice as high as in developed regions[6]. Figure 1.4 shows that 308 operators have launched or are planning various LTE deployments worldwide; 138 of these operators are in developing markets, which form a significant proportion of the global operator base.

Mobile operators in developed markets – where mobile data coverage and penetration are high – are investing in high-speed LTE-Advanced (LTE-A)[7] networks, based on higher smartphone penetration and the take-up of high-speed streaming services. Figure 1.5 shows that 40 operators have launched or are planning various LTE-A deployments worldwide; 35 of these operators are in developed markets. The Republic of Korea has one of the highest LTE penetration rates worldwide (at 66 per cent of connections in 2014, and an expected 89 per cent by 2019)[8].

Other wireless network operators are investing in public small cells, public Wi-Fi networks and in low Earth orbit (LEO) satellites. Operators in developed markets use public small-cell deployments to address 3G and 4G network coverage and capacity deficits, particularly in city business districts where the demand for data-hungry applications can be extremely high. By 2020, the Asia-Pacific region and North America will together account for 78 per cent of the investment in public small cells[9].

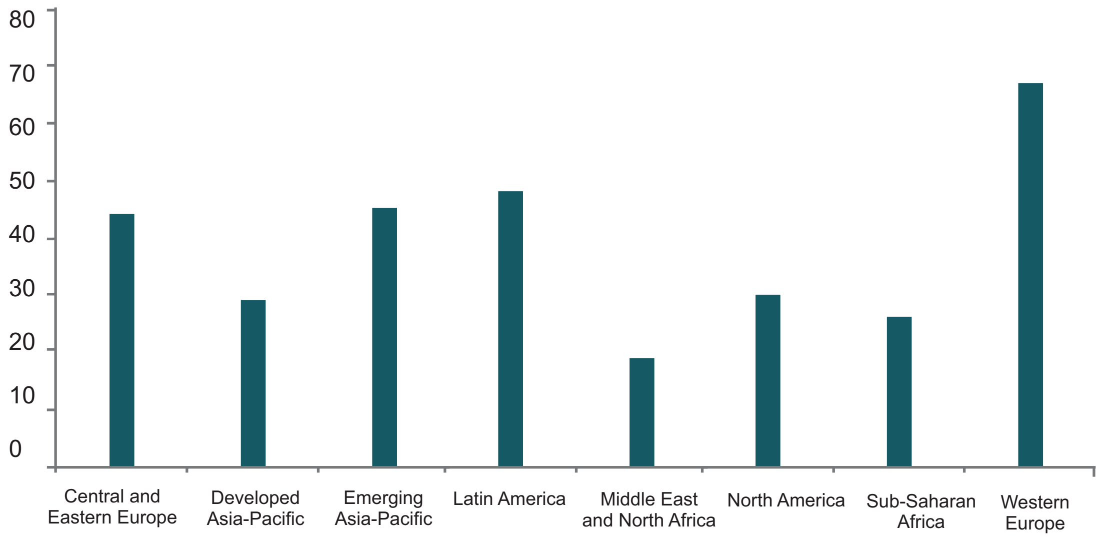
Mobile players in the Arab States also have been deploying small cells since 2010 to help alleviate the strain on their networks and reduce traffic congestion. In the United Arab Emirates, EITC (du) has used a combination of small cells and Wi-Fi to address peaks in data demand levels at the site of the Burj Khalifa skyscraper, which attracts thousands of visitors daily. Etisalat first used femtocells in 2010 and is committed to deploying more 3G cells in public areas around the country to improve capacity. In 2010, Kuwait's Zain launched its Cell Access Point, a consumer-grade cell, to improve signal coverage indoors. The end user device, which can support up to four voice calls at once, was given free to subscribers. In Bahrain, Batelco has deployed a combination of femtocells, microcells and a cell-coordinated network (HetNet) to boost capacity, eliminating the need for 30-50 per cent more macrocells to achieve the same capacity.

Investing in 4G networks and small cells, however, does not remove the need for public Wi-Fi[10] infrastructure. In fact, the rise in consumer data consumption may drive the need for *further* Wi-Fi investment. Mobile operators consider public Wi-Fi a necessary service, although it risks cannibalizing their mobile data revenues. The upside comes with service differentiation and increased customer retention. In fact, consumer behaviour studies have shown that people like using Wi-Fi and prefer it to mobile data in some cases.

When implemented adequately, public Wi-Fi can effectively supplement mobile network capacity, particularly in dense urban areas such as business districts and shopping areas – a phenomenon known as "Wi-Fi offloading". Usually, however, the volume of traffic offloaded onto public Wi-Fi is low even in developed markets. China is exceptional in terms of Wi-Fi usage – public Wi-Fi data traffic far exceeds that of mobile network data, but investment in LTE is reversing this trend (see Figure 1.6).

Meanwhile, satellite operators Iridium and Globalstar have recently raised funds to launch a second generation of low Earth Orbit (LEO) constellations to provide broadband and voice services. In addition, SpaceX, LeoSat and others have plans to invest a total of around USD 13 billion

Figure 1.4: The number of operators by region that have launched or are planning LTE deployments



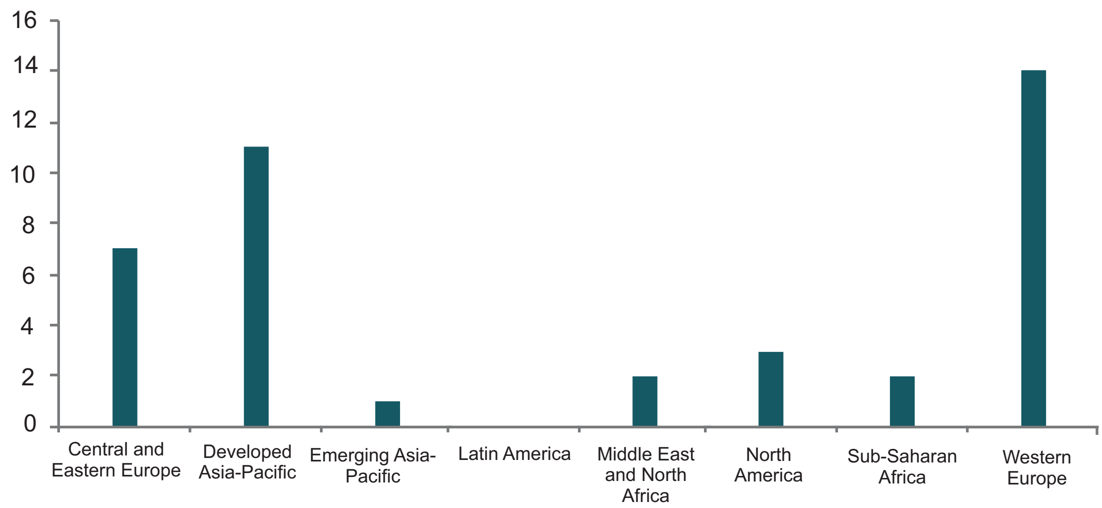
Source: Analysys Mason wireless networks tracker, 2015

to USD 18 billion in new LEO constellations designed to provide global broadband connectivity[11]. Their plans seem commercially feasible given the lower cost of satellites and the development of the broadband market.

1.2.4 Market consolidation

Operators use consolidation and network-sharing strategies, mainly in developed markets, to generate efficiency gains and cost savings to fund further network investments and to develop innovative services. Mobile network operators (MNOs) need scale to compete for 4G licences, invest in mobile network infrastructure and develop services that rival their competitors'. Take BT's USD 19 billion acquisition of mobile operator EE in the United Kingdom, for example. At first glance, the deal seems designed to expand BT's market share and service portfolio by offering a "quadruple play" package. But there may be additional benefits to both BT and EE from synergies in subscriber acquisition costs (SAC) and lower customer churn, as evidence from quadruple play offerings in other European markets shows. On the negative side, however, "in-market" mergers and acquisitions can be expensive and time consuming, and success is uncertain.

Figure 1.5: The number of operators by region that have launched or are planning LTE-A deployments



Source: Analysys Mason Wireless networks tracker, 2015

Operators in developed markets are under increasing pressure to reduce costs as revenue levels decline. When network coverage becomes less of a competitive differentiator, operators may need to consolidate networks (through network sharing) as a means of moving away from infrastructure investment and toward developing innovative services. In France, Bouygues Telecom and SFR concluded a network-sharing agreement in February 2014, enabling them to reduce cell sites by about 40 per cent. This has generated savings of about EUR 100 million per year for Bouygues Telecom and EUR 200 million per year for SFR[12].

Moreover, network sharing is not limited to developed markets. For example, eight major mobile operators in the Arab States and Africa announced plans in March 2014 to work together on a new network-sharing initiative to reduce costs and to improve rural broadband coverage[13].

1.2.5 Tech clusters

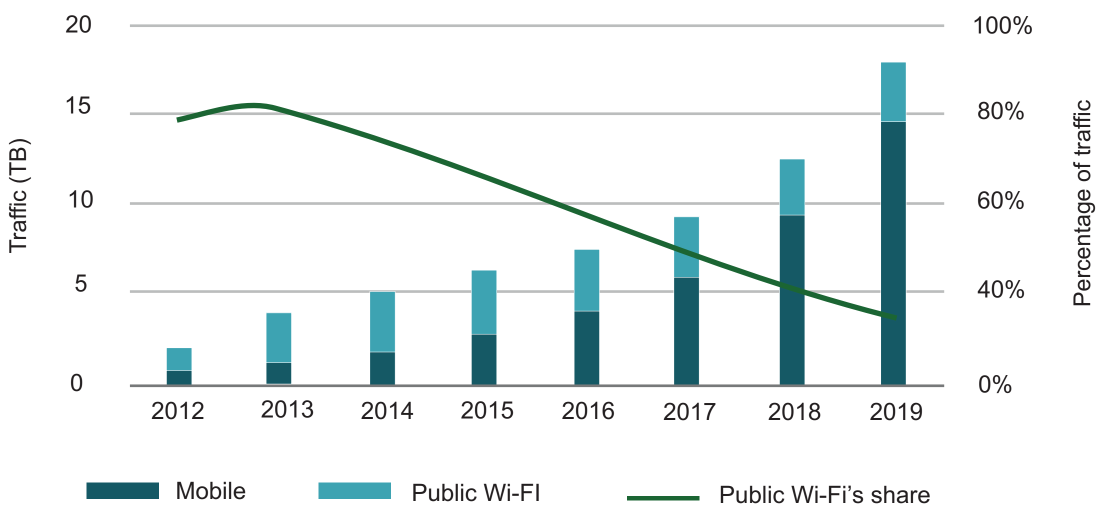
Interesting examples of how to encourage broadband investment can be found in the "Tech City" initiative and through global finance technology intiatives. Tech City is a cluster of technology companies and support-service firms based in East London and endorsed by the UK government and the Mayor of London[14]. It is designed to attract investment in technology firms, creating jobs and economic growth[15]. In the last three years, Tech City has attracted investment from global markets, including the United States, Europe and Asia, and from investors such as Rekoo, Facebook, Google, Twitter, Amazon, Cisco, Intel, Microsoft, FourSquare and Pinterest[16]. As a result, UK operators Openreach and Virgin Media have made announcements to invest in affordable, high-speed broadband infrastructure and services in the area[17] [18].

Another noteworthy trend is investment in the financial tech field (or "fintech"), an industry that develops technology solutions for the finance sector. Global fintech investment tripled to USD 12.2 billion from 2013 to 2014, creating mobile payment solutions, providing easy access to financing, and reducing fraud and identity theft. These solutions and processes are all factors in the development of a mature Internet ecosystem[19]. Silicon Valley is the world leader in attracting fintech funding, with over USD 2 billion in investments in 2014 alone. European investment totalled USD 1.48 billion with the UK (mainly in London's Tech City) accounting for 42 per cent of European FinTech deals in 2014.

1.3 PPP investment strategies in broadband infrastructure

Telecommunication operators make routine investments in core, backhaul and access networks by utilizing cash stockpiles, raising private financing, or, as previously mentioned, through consolidation. These "business-as-usual" investments are well rehearsed and require little

Figure 1.6: Wireless data traffic by type and public Wi-Fi share of that traffic, China, 2012–2019



Source: Analysys Mason, 2015

regulatory or government intervention (and are therefore not extensively discussed in this report). But operators can be reluctant to invest in areas where commercial returns are uncertain. In these cases, governments have intervened, entering into public-private partnerships (PPPs) to invest in broadband infrastructure. This section describes these PPP investment strategies, using case studies to illustrate the key characteristics of each approach.

1.3.1 Overview of PPPs

A European Commission and an ITU study have broadly defined PPPs[20] and identified investment models commonly used for broadband PPP projects[21] [22]. Most PPP projects in broadband infrastructure tend to fall into one of the following funding model categories:

- **Private design, build and operate (DBO)** – where a private operator retains ownership and control of the broadband network. The private operator may benefit from receiving state funds to invest in broadband infrastructure in commercially unviable areas.
- **Public outsourcing –** where a private operator is responsible for running a network under a government-funded contract. The government normally retains ownership of the network after the contract expires.
- **Joint venture (JV)** – where a special-purpose vehicle (SPV) or separate legal entitiy is created by the private operator and the government to invest in broadband infrastructure in commercially unviable areas. The private operator and the government share the funding, network ownership and day-to-day management responsibility.
- **Public DBO** – where the government has full funding responsibility and full ownership of the network assets. Elements of the day-to-day management may be allocated to private contractors.

The EC and ITU reports also identified common funding sources for broadband projects. These included government grants, universal service funding and external funding from non-governmental organizations (NGOs) and international development banks. Note that the "bottom-up" model has been excluded from the list of the most common investment models. This approach involves community-driven investment, and it is described in more detail in Section 1.5, where alternative investment approaches are discussed.

The four above-mentioned models involve variations of public- and private-sector intervention. Each model's approach varies based on three main characteristics:

- the funding source for the roll-out and operation of the infrastructure;
- responsibility for deploying infrastructure and running operations; and
- ownership of the infrastructure (see Table 1.2).

The most suitable investment approach for a particular project can depend on a range of variables, including the market structure, the level of Internet maturity and the political landscape. The government's experience in funding, owning and running broadband networks is also an important consideration when deciding which investment approach should be taken. The key advantages and disadvantages of the investment approaches are summarized in Table 1.2. The following sections provide as least one case study or example for each type of PPP investment approach. They also discusss the role of the regulator in attracting broadband infrastructure investment and list key lessons to be taken from each project.

1.3.2 Private DBOs

In this investment model, the private sector (usually a network operator) designs, builds and operates the broadband infrastructure on behalf of the government. The infrastructure typically is made available to other service providers and Internet service providers (ISPs) on a wholesale and open-access basis. It should be noted, however, that the infrastructure remains under the network operator's ownership, which does not transfer to the government.

In this approach, government intervention is limited to funding. The private operator retains control over the design of the network and retains the network assets. The government has limited responsibility and does not have to manage the infrastructure, minimizing its exposure to risk. The private company, meanwhile, benefits from owning the infrastructure with only minimal government interference. This approach can also be seen as the simplest of the PPP models, as it does not require creating overly complex PPP business structures.

There are disadvantages to this approach, though. Governments have little influence or control over the network design and roll-out strategy, despite funding the network build. The social benefit of the infrastructure may be limited, because private operators may focus more on financial returns than on social investment.

To make the investment case more appealing for operators in commercially unviable areas, the government may provide a grant to partially subsidize the cost of building the infrastructure. In return for the subsidy, the government would expect a significant financial contribution from the network operator. The government might also apply strict controls, including setting roll-out deadlines and network quality and take-up targets. In Europe, mandated "claw-back" rules for state aid prevent the network operator from making excessive profits.

Setting controls and requirements ensures that the network operator has a strong financial incentive to construct the network to the required technical standards. In addition, network operators strive to achieve the take-up targets by stimulating demand and setting reasonable wholesale prices. Much of the operational risk, therefore, lies with the network operator.

This approach assumes that the operator is able to build a high-speed broadband network and is prepared to operate it on a wholesale basis, with open and non-discriminatory access. Even with no direct ownership, governments must monitor and oversee operations in order to achieve an effective outcome from this approach. A private DBO is unlikely to make use of state assets in preference to using and building its own assets.

Two examples of private DBOs are set out in greater detail below.

Case study: Mobile Infrastructure Project (MIP), UK

This case study was chosen because it approached the problem of mobile "not-spots" from a very unique perspective: funding the build-out of passive mobile infrastructure in a very tightly regulated UK market. The UK Government initiated the MIP in 2011 in order to improve mobile coverage in remote and rural areas with little or no mobile coverage. In some areas of the UK, it may not be cost-effective for mobile operators to provide coverage, as the low subscriber numbers and density do not justify investment in mobile infrastructure. These areas, referred to as "not-spots," are the primary focus for MIP.

Table 1.2: Key characteristics of investment approaches

Investment approach	Funding source	Deployment and operations of infrastructure	Ownership of infrastructure	Case study
Private DBO	Public and private sectors	Private sector	Private sector	•Mobile Infrastructure Project (MIP), UK •National Broadband Scheme (NBS), Ireland
Public outsourcing	Public sector	Private sector	Public sector	•National ICT Broadband Backbone (NICTBB), Tanzania •Johannesburg Broadband Network Project (JBNP), South Africa
Joint Venture	Public and private sectors	Public and private sectors	Public and private sectors	•Metroweb, Italy
Public DBO	Public sector	Public and private sectors	Public sector	• Qatar National Broadband Network (QNBN), Qatar

Source: Analysys Mason, 2015

Table 1.3: Selected examples of private DBOs

Name of private DBO	Description
Mobile Infrastructure Project (MIP) (UK)[23]	UK government programme that aims to improve mobile coverage in remote areas by 2016 (See case study below).
Superfast Cornwall (UK)[24]	Project that leverages the resources and expertise of an established operator (BT) to deliver a large and complex project.
NGB Wales (Wales)[25]	Grant-funded government intervention has been used to increase the availability of next-generation access (NGA) broadband coverage in rural areas across Wales.
InfraCo (Nigeria)[26]	The core tasks of InfraCo will be to build, operate and maintain the fibre-optic communication network, and to lease fibre-optic connections to operators and other companies, as well as to the public.
National Broadband Initiative (Malaysia)[27]	This initiative is rolling out high-speed broadband infrastructure through a PPP agreement with Telekom Malaysia Berhad (TM).
Telebras (Brazil)[28]	Telebras, the previously dormant incumbent operator, was re-established in 2007 in order to provide wholesale services to service providers over its backbone network.
Rural Broadband Initiative (New Zealand)[29]	This JV between Vodafone and Telecom New Zealand for rural network roll-out is subsidized through a government grant.
Mobile network sharing (Sweden)[30]	Mobile operators have entered into a network-sharing agreement to reduce their costs and to help achieve the regulator's coverage obligations.

Source: Analysys Mason, 2015

Broadband Delivery UK (BDUK) implemented the project itself, with the following objectives:

- To improve the coverage and quality of mobile network services for the 5-10 per cent of consumers and businesses that live and work in areas where mobile network coverage was poor or non-existent; and
- To extend coverage to 99 per cent of the UK population.
- A GBP 150 million capital fund was set aside by the UK government to construct new masts (passive infrastructure only)[31]. These masts, which would be made available to all mobile operators on a wholesale, open-access basis, would allow operators to install their own active equipment and offer 2G, 3G or 4G connectivity to end users. The operators would be reponsible for funding their own operations.

MIP was funded through a private DBO arrangement. Arqiva, a UK infrastructure provider, won the contract to design, build and operate the masts following a competitive procurement. As a result, much of the design and planning responsibility was left to the private sector. But because MIP was government funded, it had to gain clearance in December 2012 from the European Commission, which confirmed that the project was compatible with the rules of the single market.

MIP was expected to connect an additional 60 000 premises out of 80 000 known "not-spots" by the end of 2013 and was slated to conclude in 2015. However, the project encountered delays and its conclusion was pushed back to March 2016. The first site went live in September 2013, with little progress made in 2014[32]. By December of that year, only two out of several hundred potential

Box 1.1: Key lessons from the Mobile Infrastructure Project (MIP)

- The UK regulator Ofcom played an important role in identifying the location of not-spots and continued to support the government in delivering MIP.
- The award of state funds to develop broadband infrastructure should require operators to share their network infrastructure on a wholesale basis to promote competition and reduce costs.
- Government interventions should aim to fund the construction of passive infrastructure in areas where there is no competing infrastructure.
- Amendments to legislation and regulation involving the deployment of networks can reduce "red tape" and speed up delivery.
- Stakeholder communications are vital in ensuring all industry players are familiar with the design plans for the project, allowing MNOs to coordinate their own radio planning and service delivery plans.
- Private operators should work closely with the industry and key stakeholders to anticipate and overcome the technical challenges of providing power and communications before they become an issue.
- A competitive tender process will ensure that the government achieves a solution that both meets its technical requirements and represents value for money for its citizens.
- A single, coordinated, national roll-out (as opposed to a patchwork of broadband networks) can create implementation synergies, thus reducing the government's overall funding requirement.

sites reportedly had gone live. The delays could be blamed on several reasons:

- It was alleged that Arqiva had not provided detailed roll-out plans or timescales for the development of the mast sites.
- Some of the sites had to undergo lengthy consultation processes to get the necessary planning approvals for the mast construction.
- There were technical challenges in getting an adequate power supply (3-phase electricity) to some of the most remote sites.
- It was challenging to secure backhaul circuits to connect some of the most remote sites.

The UK's telecommunication regulator, Ofcom, played an important role in identifying the location of not-spots and continued to support the government in delivering MIP[33]. It is too early to tell whether MIP has been successful in eradicating not-spots, but it is clear that a project of this scale is challenging and requires detailed upfront planning, coordination and stakeholder management. The key lessons and take-aways have been summarized below.

Case study: National Broadband Scheme (NBS), Ireland

This PPP project was chosen for this chapter because it was one of the earliest schemes to use private a DBO model to improve basic broadband connectivity in rural areas. The fact that it has been fully implemented provides many useful lessons. The project also awarded a contract to a mobile provider rather than a fixed provider, providing useful insights to regulators and governments in developing markets, where mobile services are more popular than fixed services.

Box 1.2: Key lessons from the National Broadband Scheme (NBS)

- Three was required to offer a wholesale service to other operators on a non-discriminatory basis, at an appropriate tariff, to ensure compliance with EU state-aid rules.
- Once-off state funding is useful to get infrastructure and services into areas that are not economically feasible.
- Time-limited interventions can ensure that the retail market has an opportunity to participate in competitive service provision once the intervention period has expired.
- More than one intervention scheme may be required to achieve 100 per cent broadband coverage aspirations.
- The definition of a coverage area by the number of premises and by region can assist operators in understanding the scope and scale of the intervention.

Ireland's Department of Communications, Energy and Natural Resources (DCENR) designed the NBS to address the country's digital divide. In 2007, an estimated 10 per cent of the population resided in areas where it was not economically feasible for providers to offer services. The NBS was launched in 2008 to improve the delivery of basic, affordable broadband in a target areas categorized as the "NBS Coverage Area." Any fixed residential or business customer located within the designated NBS Coverage Area – a total of about 234 000 customers – was eligible to apply for broadband services under the programme[34].

The project cost EUR 223 million,[35] of which the Irish Government made a contribution of EUR 80 million. A competitive tendering process resulted in the award of a contract to Three (a Hutchison Whampoa company), to design, build and operate the NBS. Three was required to provide basic broadband services to residents and businesses, both retail and wholesale, within the NBS Coverage Area for five years. The NBS scheme ended in August 2014 following a 68-month operational period, which was limited in duration to ensure compliance with EU state-aid rules.

In order to facilitate competition, Three was also required to provide wholesale access to all other authorized operators who wished to serve customers in the NBS Coverage Area. Following the end of the project, Three was no longer required to make the NBS retail and wholesale services available under the NBS contract, although broadband coverage will continue to be available on a commercial basis.

In 2010, the government announced that it had met the EU target for broadband availability two years ahead of schedule, making broadband available to 235 000 premises in 1 028 areas (99 per cent of premises) across the country. A separate Rural Broadband Scheme was launched to target the remaining 1 per cent of premises.

A study of the NBS showed that the spin-off benefits of widespread broadband access could be significant in regional areas. The study estimated that the NBS would yield EUR 25 million for the local economy in Donegal, EUR 53 million in Galway, EUR 40 million in Kerry and EUR 26.9 million in Mayo[36].

The NBS seems to have been a success in Ireland. In 2007, only 31.2 per cent of households had a broadband connection – a percentage below the EU average of 42.4 per cent. In 2014, 79.5 per cent of households in Ireland had a broadband connection – surpassing the EU average of 78.3 per cent that year. It is clear that the NBS allowed Ireland to boost the percentage of mobile broadband connections above that of the European Union average[37].

1.3.3 Public outsourcing

This approach allows a government to award a contract to a private firm to construct and operate a broadband network on its behalf. The government typically funds the entire network and the infrastructure remains in government ownership.

The private company normally gets a contract (after a competitive tender) for a wholesale, open-access network. It may also be required to market the wholesale services to other Internet Service Providers (ISPs), and in some cases to offer retail broadband services as well. Contracts typically last between 10 and 15 years, after which a competitively procured contractor may be appointed to operate the network.

Most, if not all, funding for this approach needs to come from the public sector. Unlike the private DBO and JV investment models, the private sector does not make any financial investment in a public outsourcing deal. Instead, the private sector constructs the broadband infrastructure and operates the broadband network on behalf of the government, in return for payments at pre-agreed milestones.

Although the government is fully responsible for financing and financial risk, this approach does give it a greater responsibility and control over the design of the network and the technical- and service-performance criteria. Typically, the government defines clear performance milestones for the private operator (such as network roll-out timescales, take-up and service levels) as part of the contract. Failure to meet these terms may result in fines or other penalties.

Two examples of private DBOs are set out in greater detail below.

Table 1.4: Selected examples of public outsourcing

Name of private DBO	Description
National ICT Broadband Backbone (NICTBB), Tanzania[38]	National core fibre network built across Tanzania. (See case study below)
City of Johannesburg Broadband Network Project (South Africa)[39]	Fibre network operated across Johannesburg by the government. However, in a recent development the city cancelled the contract and is proposing to convert it into a public DBO. (See case study below)
Auvergne (France)[40]	This model leverages the expertise of the private sector, while ownership remains in the public sector. The private operator receives an income to run the network for ten years.
Metropolitan Area Networks (Ireland)[41]	Sells open-access, active and passive, wholesale services to operators in areas that do not have adequate private-sector broadband provision.
Shetland SHEFA 2 Interconnect Project (Scotland)[42]	This project aims to provide an adequate backhaul network in the Shetland Islands in areas where such infrastructure is currently unavailable.
South Yorkshire (UK)[43]	Local authorities invested in an FTTC network, with a partnership arrangement for network management. (However, this initiative is no longer running and has reverted to a private DBO.)
DORSAL (France)[44]	A collection of local authorities invested in network backbone, DSL and WiMAX services.
Project Isizwe municipal Wi-Fi (South Africa)[45]	The private-firm Project Isizwe is being contracted by several municipalities to deploy Wi-Fi hotspots in public buildings and schools.
Western Cape Government broadband (South Africa)[46]	The Western Cape Government has outsourced the deployment and management of a network connecting all provincial government buildings to Neotel.

Source: Analysys Mason, 2015

Case study: National ICT Broadband Backbone (NICTBB), Tanzania

This case study will be of interest to regulators and governments that currently are constructing national fibre backbone networks to facilitate the roll-out of broadband connectivity and wider e-Enabling initiatives.

The Government of Tanzania is building a fibre network under the NICTBB project in order to enhance the usage of ICT applications and promote the development of e-government, e-learning, e-health and e-commerce. The NICTBB is broadly intended to:

- provide international connectivity to all landlocked neighbouring countries;
- establish points of presence (PoPs) across all of Tanzania's administrative districts;
- provide all licensed operators equal access to the fibre network to stimulate competition;
- enable the provision of affordable Internet to Tanzanians;
- increase the usage of ICTs; and
- facilitate the implementation of e-government initiatives.

The NICTBB is managed and operated by the incumbent fixed operator, Tanzania Telecommunications Company Limited (TTCL) on behalf of the government. It should be noted that the NICTBB network is completely independent from TTCL's network. The USD 200 million project is funded by the International Telecommunication Construction Corporation (CITCC) of China at the cost of USD 170 million – mainly thanks to a soft loan from the Chinese Exim Bank[47] and USD 30 million from the Tanzanian Government. The Tanzanian Government deployed a fibre cable on the rail, electricity and gas networks in 2010 and pooled this fibre into a single SPV, the NICTBB.

The NICTBB provides high-capacity, long-distance wholesale capacity to fixed and mobile operators and ISPs, as well as access to international submarine fibre connectivity. The establishment of PoPs across Tanzania allows operators to connect their last-mile networks to a national backhaul network. NICTBB's network connects major towns and cities across Tanzania, extending to the borders of all neighbouring countries. The NICTBB has also been connected to the two East Coast submarine cables (EASSY and SEACOM) landing at Dar es Salaam. Most of the NICTBB equipment has been accommodated in TTCL buildings so that operators can access carrier-class hosting and bandwidth services.

The NICTBB has been implemented in phases, with 31 PoPs currently operational. By the end of 2014, NICTBB spanned 7 560 km across 24 regions. It has reached all border points and even garnered a USD 6.7 million contract to provide bandwidth to Rwanda over the next 10 years. Third-party research has found improvements in provision of e-commerce, m-commerce, e-banking, e-education and e-government since the NICTCBB commenced operations[48]. These improvements have enabled digitally excluded Tanzanians to become proficient in using e-services, accelerating Tanzania's economic development.

Even so, fixed broadband penetration remains very low in Tanzania, standing at only 0.1 per cent of the population as of June 2014. This stems from the limited coverage of fixed broadband metro and access networks. Improved coverage, especially in rural areas, has helped to make mobile services more accessible, but mobile penetration also remains relatively low in Tanzania, standing at 60.1 per cent at the end of June 2014, leaving room for continued growth[49]. The government awarded contracts to TTCL, in February 2014, and Vodacom, in April 2014, to expand coverage to under-served areas, and it supported the operators with the universal access fund. The telecommunication regulator has also helped improve the affordability of mobile services by introducing mobile termination rate (MTR) cuts in March 2013.

Case study: Johannesburg Broadband Network Project (JBNP), South Africa

This case study provides useful insights into a public outsourcing project that has – for a number of reasons – become a public DBO project. The Johannesburg municipal government took control of the project when contracts with private contractors were terminated.

The City of Johannesburg (CoJ) municipal government began the JBNP in 2006 in order to address digital exclusion issues and to improve digital connectivity among Johannesburg's citizens and businesses. The JBNP's vision was to become a "Smart City," and the JBNP was expected to develop economic growth by creating business opportunities, providing access to public services and increasing employment opportunities for youths.

To realize its vision, the CoJ awarded a contract to Ericsson – which then transferred it to CitiConnect Communications – to build a fibre network that would extend coverage across the city's business and residential premises. The network was estimated to be 900 km in length[50]. The goal was to provide broadband and ICT services at a lower cost by enabling service providers to access wholesale capacity from the JBNP on an open-access basis. This, in turn, would allow service providers to provide lower retail prices to end users. The CoJ would also act as an anchor client, connecting its buildings to the JBNP (this would only account, however, for a small percentage of network capacity).

The investment was estimated at about USD 100 million in capital, with management costs expected to be around USD 24 million annually. The contract was constructed along the lines of a public outsourcing model. After 12 years, Ericsson would return responsibility for operating the network back to CoJ[51].

The network build was expected to go live in 2013, but in 2014 the CoJ terminated the contract with CitiConnect Communications, saying that the company had breached the agreement, a claim CitiConnect disputed. The CoJ paid USD 93 million to Ericsson for the infrastructure that had been built to date and in February 2015,[52] the CoJ took responsibility to complete the network build. It is now a public DBO project, meaning that the infrastructure is fully owned and operated by the municipality.

The project has come under scrutiny from independent analysts and officials, who have questioned the need for a municipally owned fibre network. Questions have also been raised about the ability of CoJ to compete with commercial service providers to generate profitable returns. There have been calls for the CoJ to sell the network to private service providers.

1.3.4 Joint ventures (JVs)

A joint venture assumes that ownership is split between the private sector (typically one or more network operators) and the government. The network operator takes responsibility

Box 1.3: Key lessons: National ICT Broadband Backbone (NICTBB)

- NICTBB is operated and managed by TTCL on a transparent and open-access basis and is separate from the rest of TTCL's business. This is essential in ensuring that service providers are not adversely affected by government intervention in infrastructure.
- Other regulatory measures, such as cuts in MTR rates in conjunction with broadband interventions, may be necessary to stimulate growth in mobile services.
- Infrastructure intervention, backed by a strong business case and development agenda, can attract significant development funding or loans.
- National backbone networks are not an end in themselves. Further investment in metro networks and access networks will still be required to deliver last-mile connectivity.
- The lack of specific and defined outcomes makes it difficult to measure the true success of an intervention or investment.
- Allocating universal service funds to competing operators can stimulate competition in the development of rural broadband networks.

Box 1.4 – Key lessons: Johannesburg Broadband Network Project (JBNP)

- Governments should carry out an extensive market assessment before undertaking a broadband intervention to ensure there is a clear market failure that justifies the intervention. In this case a number of alternative fibre networks are already available in Johannesburg, which has called into question the need for the project.
- Contractual obligations upon the public and private sectors should be clear at the outset to ensure there is no dispute if either party defaults or reneges on the contractual agreements.
- Public DBOs should be limited to offering wholesale services on a non-discriminatory and open-access basis to ensure competition is not adversely affected.

for the design, building and operation of the infrastructure, which is typically made available to other service providers and ISPs on a wholesale, open-access basis. The infrastructure remains part-owned by the network operator and the government.

Public-sector funding is required for a JV, but funding is shared with private-sector partners. Much of the initial financial contribution typically comes from the government, to make it attractive to the private sector. The costs of deploying the network, associated systems and processes and the ongoing administration of the JV are shared. The exact amount of private and public sector capital investment has to be agreed beforehand, based on how rewards and risks are to be shared.

With this approach, the government takes on greater financial risk, but it is able to control the initial stages of the network design and construction. Meanwhile the private sector takes on greater responsibility once the project becomes self-financing. Depending on the terms agreed for the JV, the government may retain its ownership in the venture or it may divest its shareholding in order to recoup some of its early investment. In fact, JVs can vary widely, since they need to take account of local tax considerations and the extent to which the government wants to hold shares and voting rights. Examples of JVs are very limited, possibly because they are complicated to set up.

Table 1.5: Selected examples of JVs

Name of private DBO	Description
Metroweb (Italy)[53]	Ownership of the network is split between the public and private sectors by setting up an SPV. (See case study below)
Banda Ultralarga in Lombardia (Italy)[54]	A JV approach enables the government to secure expertise and financing while maintaining public control over the scope of the project.
Eastern Corridor (Ghana)[55]	The Ghana Ministry of Communications, in partnership with Alcatel-Lucent, has planned a 800 km fibre-optic network in the Eastern Corridor.
Kenya LTE[56]	This PPP has been proposed to deliver a national broadband LTE network in Kenya.

Source: Analysys Mason, 2015

An example of a JV is described in greater detail in the following case study.

Case study: Metroweb, Italy

This case study has been detailed in previous ITU reports; nevertheless, it was selected because it represented an instance in which an infrastructure fund manager acquired a controlling stake in a project. Metroweb also has become the subject of a takeover battle between leading operators in Italy, attracting significant private-sector interest.

Italian Prime Minister Matteo Renzi has begun an ambitious plan to bring super-fast broadband to 85 per cent of Italy's consumers by 2020. Fixed broadband take-up in Italy is 23 per cent compared to an EU average of 31 per cent. The percentage of customers with fixed broadband download speeds greater than 30Mbit/s is just 2 per cent – significantly below the EU average of 23 per cent[57]. Mr. Renzi sees Metroweb, which generates sales of just USD 74 million, as a good vehicle to achieve his ambitious plans.

Metroweb is an example of an SPV in which ownership of the network is split between the public and private sectors. It was conceived as a result of Telecom Italia's perceived lack of investment in fibre infrastructure. It is an arrangement between a gas and electricity utility company, A2A, and e.Biscom, a new telecommunication service provider, to accelerate the roll-out of a large fibre-optic network in the major metro areas.

Metroweb currently owns a 3 200-km fibre network extending throughout much of northern Italy, including the municipality of Milan, as well as Turin and Bologna[58]. It is a passive infrastructure operator and leases point-to-point, dark-fibre service to its customers, including its separate retail affiliate, Fastweb. Metroweb also serves Telecom Italia, Wind, Vodafone and other service providers in Milan. Funded by a EUR 100 million loan from two Italian banks, Metroweb has planned to expand to two additional metro areas chosen from a shortlist that includes Florence, Parma, Verona, Brescia and Monza[59].

Although Metroweb is central to the government's broadband aspirations, it has not garnered any state-aid approved funding. However, local municipalities (such as the one in Bologna) have played a key role in creating favourable conditions to attract investment in Metroweb by:

- creating a register of all current network infrastructure in the City; and
- speeding up the process of getting the necessary planning permits to carry out civil work.

An Italian infrastructure fund known as F2i acquired a 53.8 per cent stake in Metroweb in 2011, expecting a growing demand for high-capacity broadband and services. Several years later, however, it began looking to divest all or part of its holding. Consequently, Telecom Italia and Vodafone became interested in acquiring a controlling stake in Metroweb, which was valued at approximately EUR 400 million[60].

1.3.5 Public DBOs

The public DBO investment model is an extension of the public outsourcing model. It requires the greatest level of involvement and financial contribution from the government and minimizes private-sector involvement and investment. This model often is used to intervene when it is not possible to attract any investment interest from the private sector. The government typically funds the entire network construction and the infrastructure remains government-owned.

Public DBO projects work in much the same way as public outsourcing. A private-sector contractor is awarded a contract to design and build the network infrastructure on behalf of the government. However, the government creates a separate, publicly owned company, which then manages and operates the broadband network. The main difference from the public outsourcing model lies in the public-sector operation of the network, rather than its construction. The publicly owned company takes full responsibility for making the wholesale open-access network available to other service providers on a competitive and open-access basis.

In the public DBO model, then, the government is fully responsible for financing the broadband infrastructure and therefore takes on much of the financial risk – and the operational risks. In return, the government retains greater control over the design of the network and the technical and service-performance criteria. Having ownership control may allow the government to re-use assets from SOCs, providing they are fit for purpose. It should be noted that the publicly owned company has to meet the performance milestones itself, a job left to the private sector operator under the private DBO model.

Table 1.6: Selected examples of public DBOs

Name of public DBO	Description
Qatar National Broadband Network (QNBN) (Qatar)[61]	A company owned by the government of Qatar with responsibility to roll out passive fibre infrastructure across the country. (See case study below)
NBNCo (Australia)[62]	An SPV (NBNCo) was created to leverage Telstra's infrastructure to address rural and urban needs.
Asturcon (Spain)[63]	A 100 per cent public-owned and public-run network in an area requiring economic regeneration, Asturcon has attracted a national operator (Orange).
Stokab (Sweden)[64]	A municipality-owned, city-based dark-fibre meshed network.
Midtsoenderjylland (Denmark)[65]	A municipality-owned investment in fibre connectivity between city halls to provide FTTH, in partnership with the local electricity company.
Piemonte (Italy)[66]	Piemonte is managed by a public ICT administration organization investing in multiple infrastructures to stimulate private investment.
Alto Adige (Italy)[67]	Alto Adige is managed by a local council to provide wireless connections to homes and fibre connections to the public sector and businesses.
RAIN (Lithuania)[68]	RAIN is managed by a non-profit public enterprise investing in a nationwide backhaul/core network.

Source: Analysys Mason, 2015

Case study: Qatar National Broadband Network (QNBN), Qatar

This case study is a recent example of how a government-funded private company can be used to facilitate the roll-out of passive fibre infrastructure and work with the private sector to reduce infrastructure costs.

Box 1.5 – Key lessons: Metroweb

- It is possible to create a public–private SPV without direct funding from the government or State-aid or public funds.
- Municipalities can play a key role in attracting private-sector investment by reducing bureaucracy and making relevant data available.
- A network operator can operate a separate retail arm, enabling it simultaneously to offer wholesale services to other service providers. This approach also allows the SPV to generate income from more than one service provider, helping to meet immediate cash-flow requirements.
- SPVs can access commercial financing to fund network expansion, just like any other commercial operator.
- Public–private SPVs can be acquired by private investment funds. This arrangement has likely attracted further interest in Metroweb from private operators.

Qatar has among the highest broadband penetration rates in the world, but it lags significantly behind leading nations in download speeds, with current maximum speeds of only 8 Mbit/s. In 2011, the Qatari government established the QNBN with a mandate to roll out a nationwide, open-access, high-speed broadband FTTH network. QNBN won a 25-year licence from the Telecom Regulatory Authority to carry out Qatar's ambitious digital plans, which were summarized under the Qatar ICT Strategy 2015 and further articulated through the Qatar National Vision 2030. The aim was to become one of the most well-connected countries on Earth.

The plan called for the wholesale QNBN network to have nationwide fibre coverage. In 2012, Ericsson was selected by QNBN to deploy the network, with the government retaining ownership and responsibility for managing and running it – thus making QNBN a public DBO. The network was expected to cover 95 per cent of the households in Qatar, as well as 100 per cent of the business establishments in Doha, by 2015, equating to approximately 260 000 connections[69]. QNBN was to focus solely on the deployment of a passive network, leveraging existing and new infrastructure in Qatar to maximize efficiency and cost-effectiveness.

According to QNBN, typical investors would not be attracted to passive infrastructure because the return on investment is not that high. As a result, the government invested some USD 500 million in capital to overcome this expected bottleneck.

In 2011, QNBN signed an Infrastructure Access Agreement (IAA) with service provider Qtel to reduce its civil infrastructure building costs. Under the agreement, Qtel would supply QNBN with access to ducts and other passive infrastructure over the next 20 years[70]. However, Ooredoo, which dominates the fixed broadband market, appeared to be aggressively laying fibre in an effort to compete with QNBN's fibre roll-out. In addition, Ooredoo seemed to not be giving QNBN access to its fibre, despite the regulator's attempts to force Ooredoo to do so. Ooredoo's lack of cooperation and roll-out delays hindered the government's plans for nationwide fibre coverage by 2015.

QNBN began to roll out fibre infrastructure in Barwa City and the Barwa Commercial Avenue area in August 2012. But it was not until 2013 that it announced the opening of two central offices to serve 30 000 businesses and residences in the West Bay area (the business district) of Doha. The delay was partly caused by operational complexities in the network roll-out – in particular when re-using Ooredoo's civil infrastructure.

In 2012 QNBN signed an interim wholesale agreement enabling Vodafone Qatar[71] to use the QNBN network to deliver its retail services. Vodafone Qatar has deployed very limited fixed infrastructure to date, and it relied on QNBN's network outside its original local market. QNBN's slow growth, however, affected Vodafone, giving it a choice of whether to take further potential action such as lobbying the regulator to force Ooredoo to give access to passive infrastructure. In the meantime, QNBN connected a number of government ministries through point-to-point fibre connectivity, enabling the ministries to benefit from secure high-speed broadband networks.

In 2014, Vodafone Qatar reached a non-binding agreement to buy 100 per cent of QNBN for QAR 210 million (USD 58 million)[72].[73]However, this deal was scrapped following a due-diligence and negotiation process and QNBN has continued with its build-out strategy.

1.4 PPP implementation strategies

Operators and governments (and, in some cases, regulators) still use the PPP investment strategies and models descibed in the previous section to finance investment in broadband networks, particularly where government intervention is required. In implementing national broadband PPP projects that include open-access initiatives, however, governments need to take into account several considerations (see Table 1.7).

Table 1.7: Requirements for governments to foster and secure investment

• Consider local market conditions such as the level of Internet maturity, operator ownership structures and the regulatory and market structure.
• Have realistic and well-defined broadband objectives with speed and coverage targets.

- Introduce non-discriminatory, wholesale open access to broadband infrastructure.
- Implement transparent procurement processes.

Each of these elements is described in more detail in the following sections.

1.4.1 Consideration of local market conditions

Managing authorities generally accept the investment approaches and funding sources described in this chapter. As a result, managing authorities increasingly are focusing on how their broadband vision (as defined in their national broadband plans) can be implemented and adapted to local conditions. National broadband plans set out a vision for broadband connectivity and development of ICTs, detailing broadband coverage and speed targets and the actions needed to help achieve them. Local conditions and factors that are likely to affect these considerations include:

- **The development of the digital economy and Internet maturity**: Internet maturity includes factors such as Internet take-up, availability of compelling local content, and development of e-government initiatives to connect schools, government offices and hospitals. It also includes implementing and enforcing cybersecurity regulations and improving ICT literacy. Economies that can demonstrate greater Internet maturity – or those that show they have plans in place to develop the Internet ecosystem – will drive Internet traffic growth. This, in turn, will encourage competitive investment in broadband infrastructure.

- **Political landscape and ownership structures**: Managing authorities that retain whole or part ownership of incumbent operators are likely to be politicians' favored recipients of

Box 1.6: Key lessons: Qatar National Broadband Network (QNBN)

- QNBN was granted a licence to offer wholesale services on an open, equal and non-discriminatory basis, along with a mandate to set appropriate national wholesale prices to enable downstream (retail) competition.
- Government funding of fibre networks can be used to reduce the investment required from private operators, therefore attracting private sector interest in the network.
- Re-using existing passive infrastructure may reduce civil infrastructure build costs, but dominant operators should be required to provide open access to their networks.
- By continuing to roll out FTTH aggressively, alternative operators (in this case Ooredoo) might contribute to fulfilling the broadband vision in a different way than initially expected – in this case independently of QNBN.
- This may mean putting the government intervention at risk and creating two separate fibre networks. This risk should be taken into account prior to initiating an intervention project.
- Operators should be consulted in advance to understand their roll-out plans; doing so may avert the risk of duplicating fibre networks.
- National broadband networks can be considered for sale to the private sector subject to regulatory approval and commercial due diligence. However, in this case, Vodafone's proposed deal might have run counter to the original remit of QNBN (which was to rent wholesale fibre capacity to both Vodafone Qatar and its rival Ooredoo) limiting competition.

funding even if they are not necessarily the best-equipped commercial operators. This may dissuade private-sector investment in broadband infrastructure.

- **Market structure and regulatory effectiveness**: A market where a dominant operator is not required to provide wholesale, non-discriminatory open access to its network may see delayed broadband development or unnecessary duplication of broadband infrastructure.

Governments and regulators should consider these aspects in the implementation and design of their national broadband plans.

1.4.2 Development of broadband targets

Another factor that often influences the implementation of broadband projects relates to how governments and regulators develop their broadband targets and their understanding of the costs and funding requirements to support those investments. Many managing authorities, particularly in developing markets, have developed broadband targets that are simply too aggressive, given current levels of network investment and the relatively low levels of Internet maturity in those economies.

Well-defined and realistic broadband targets will enable a better understanding of the range of technologies required to meet those targets and a more accurate prediction of deployment costs. Knowing the costs then allows managing authorities to establish the funding needs and operators can then set their investment requirements. In some cases, this can be an iterative process, in which targets are revised until an optimum balance is achieved between optimal speed and coverage targets and the availability of funding.

Governments, therefore, can adopt the following principles in defining their broadband targets:

- Targets should be defined progressively to increase in accordance with market trends for the next ten years. The targets should define the broadband speed and coverage (by number of business and residential premises) targets over that period.

- Targets need to distinguish between rural and urban areas. It is more likely that urban areas will require higher-speed services than rural areas, but greater funding will be required in rural areas.

- Targets need to be realistic and achievable rather than being over-optimistic and over-ambitious. Otherwise, authorities will not be able to gauge the real success of the broadband project.

Coverage targets can be included in mobile spectrum licences or in fixed network licences, so investors need to undertake a detailed assessment of the targets in order to determine the cost of acheiving them. Investors also need to assess whether coverage targets are even achievable so they don't commit to a project that cannot be delivered successfully.

1.4.3 Open access networks

Open access networks are another vital aspect of implementing broadband projects, particularly in promoting competiveness and fairness and, ultimately, in reducing duplicative infrastructure. The mandate to open access to networks can ensure that operators have effective, non-discriminatory and transparent access to wholesale networks.

The concept of "open access" has two dimensions: an operational one and a technical one. At the operational level, access must be:

- **Effective –** it should provide the access services requested without undue burdens such as onerous processes or overheads;

- **Transparent –** it should be clear how to use the access services, and they must be provided efficiently; and

- **Non-discriminatory –** It should be possible to demonstrate – possibily through some level of separate management between wholesale and retail operations – that services are provided in a non-discriminatory way. There also should be a mechanism for recourse if non-price discrimination is suspected.

At the technical level, open access services can be provided at:

- layer 0: civil infrastructure (ducts, poles, towers);
- layer 1: transmission media (fibres, copper);
- layer 2: transmission point-to-point connections; and
- layer 3: Internet Protocol.

Open access at one level typically allows competition at higher levels. The principle of open access can be applied to a number of investment models. Managing authorities will need to decide when (and at what levels) to avoid network duplication and when competition – including potential infrastructure "over-building" – can be encouraged. These decisions should take place well in advance, based on analysis and modelling.

In terms of wireless networks, there is insufficient international experience to suggest what may constitute best practices in wholesale, open-access, wireless networks. Emerging projects may yet develop best practices, but such networks face significant organizational and strategic challenges.

1.4.4 Procurement

Due to the nature of PPP projects, which involve public funding, they are conducted normally as public network procurements. Whether financed through a universal service fund or by other means, such projects should be undertaken according to best practice principles, ensuring they are fair, equitable, transparent, competitive and cost-effective. Privately funded broadband projects, however, are not bound by these principles, although many of the best practice principles still apply. These principles are described in more detail in Annex 1.

1.5 Alternative approaches to funding broadband networks

The previous sections in this report have looked at strategies governments and operators can use to invest in publicly subsidized broadband projects – often PPP projects. The methods privately owned operators use to raise funds are relatively well known and, therefore, not discussed in this report. However, increasing numbers of existing operators, new entrants and financiers have developed alternative funding approaches for broadband network investments. To examine such alternative approaches, we have selected examples from four investor categories, as set out in Table 1.8.

Moreover, we have provided a detailed case study for of each of these investor categories. Each case study provides the motivation for the financing approach, the role of the regulator in attracting investment, and an overview of potential barriers to investment.

1.5.1 Existing market players

Operators traditionally have invested in broadband infrastructure in commercially viable areas using their own capital investment funds. In some cases, operators have generated funds by selling de-commissioned network assets (e.g. copper

Table 1.8: An overview of investor categories and corresponding case studies

Investor category	Case study	Existing parties
Existing market players	MGTS, Russia	MGTS
New market entrants	Google Fiber, USA Google Fiber, Uganda	Google Fiber Google Fiber
New financiers	SIGFOX, France Seacom, Africa Asia–Pacific Gateway, Asia	Elliot Management Convergence Partners Facebook
Not-for-profit investors	Community broadband, Germany	Various Communities

Source: Analysys Mason, 2015

networks) and old active equipment[73]. For example, eBezeq, a fixed and mobile operator in Israel, generated cumulative profits of ILS 214 million (USD 60.8 million)[74] between 2009 and 2013 by de-commissioning its copper network. Another operator exploring this approach is MGTS, a fixed-line operator in Russia.

Case study: MGTS, Russia

This case study illustrates how MGTS, the fixed-line incumbent in the Moscow region, is funding its fibre network roll-out by decommissioning its legacy network. MGTS is aggressively rolling out a gigabit optical passive network (GPON), fibre-to-the-home (FTTH) network. MGTS' existing telephone network consisted of 4.994 million lines at the end of 2012, and MGTS passed 2.6 million homes with FTTH at the end of 2013. The company's ultimate objective was to pass 4.4 million homes with FTTH by 2015[75].

In 2013, the operator agreed to sell its 49 per cent stake of CJSC Business Nedvizhimost, the owner of telephone exchanges in Moscow, to Russian investment company Sistema, retaining a portfolio of buildings in Moscow with a total capacity of about 1 million square metres. The value of the transactions was RUB 6.3 billion (USD 194 million), and the proceeds were to be reinvested to help fund the GPON roll-out, which MGTS estimated to cost about USD 2 billion or about USD 360 per home passed. The sale effectively would cover the costs of passing about 12.7 per cent of the total 4.4 million homes to be covered[76].

MGTS noted that it could generate even more revenue from exchange sales, and it expected to divest further assets. The first tranche of exchange sales was relatively profitable for MGTS, reflecting the high value of property in the Moscow region, Russia's richest area. The operator also intended to generate revenue from selling copper and was working on removal of its copper lines – a project slated to begin in earnest in 2016.

MGTS made good progress in transferring customers to its GPON network. At the end of 2012, 20 per cent of homes passed with FTTH were subscribing to a GPON voice service, a figure that increased to 30.4 per cent at the end of 2013. This transition allowed the company to improve its average revenue per user (ARPU); at the end of 2013, customers migrating to GPON had a 55 per cent higher ARPU than previously[77].

Box 1.7: Key lessons: MGTS

- MGTS commited to a GPON FTTH deployment strategy funded through divestment of key telecom assets, helping to improve the company's competitive position for the medium to long term.
- MGTS demonstrated that investment in fibre can generate higher ARPUs through offering higher-layer services such as IPTV and video on demand.
- De-commissioning the copper network can also result in losing voice-only customers who do not want to migrate to the new network. MGTS acknowledged that it would lose voice-only customers, but the company bet that its ARPU gains would outweigh those losses.
- The regulator allowed MGTS to de-commission its copper network and divest the assets. The implementation of this approach may depend on whether there is local loop unbundling (LLU) or just bitstream services.
- There is no LLU in Russia, so the process of de-commissioning an older copper network may be much faster and easier to achieve in such countries, where the local loop infrastructure is not shared with other operators.

1.5.2 New market entrants

New market entrants typically try to address gaps in the existing market. For example, ISPs will focus on generating connectivity-based revenues, while organizations operating higher up in the Internet value chain (traditionally not ISPs) can benefit from a strong Internet ecosystem that allows their Internet services to be more widely used.

The approach taken by new entrants can vary based on the market context. In established economies, the opportunity is likely to stem from existing broadband providers' lack of motivation to invest in their legacy networks. In this scenario, the new entrants may be required to compete head-to-head with the established players, pushing those incumbents to improve their service offerings. In developing markets, however, the issue is more a lack of infrastructure, and even the established providers may not have the funding to roll out and maintain the comprehensive network. In this case, the new entrant may partner with one or more existing providers, or even the government, to share the infrastructure costs. In the case of Google Fiber in Uganda (see below), Google may have funded the entire project.

Case study: Google Fiber, USA

Governments and regulators need to create the right environment to attract investment from new entrants. This case study describes how Google, a global player whose traditional core business is to provide services over the Internet, decided to invest in broadband network infrastructure and offer broadband services to ISPs and end users.

Google Fiber's initiative was driven by its ambition to "help make Internet access better and faster for everyone." In 2010, Google saw an opportunity to offer end users high-speed connectivity in a handful of cities where operators did not offer high-speed broadband services. Its motivation for investing in fibre networks has been to provide more opportunities for Google to generate revenues from advertising and content in addition to broadband subscriptions.

In December 2012, Google Fiber started offering fixed broadband and TV services over its fibre-to-the-premises (FTTP) network in Kansas City. That city was chosen for its good economic infrastructure and a business-friendly environment – for example, the presence of utility conduits avoided the need for digging up streets.[78] Analysts estimated that it would cost close to USD 84 million to pass 149 000 households in Kansas City, resulting in a cost per household of USD 564. The cost to acquire and connect a broadband customer, meanwhile, was estimated to be USD 464[79].

A key differentiator of Google Fiber's value proposition was its high-speed broadband service, which offered speeds of up to 1 000 Mbit/s. The reaction from other broadband providers was nearly immediate; in August 2014, Comcast and Time Warner announced that they would increase their Internet access speeds to customers in Kansas City[80]. And in February 2015, AT&T announced that it would match Google Fiber's price and speed in the city, as well[81].

In its "Google Fiber City checklist,"[82] the company listed the requirements that applicant cities needed to meet to be considered as candidates for future network expansion. An attractive environment for Google Fiber to expand would offer:

- transparency about existing infrastructure;
- clear rules about gaining access to that infrastructure; and
- facilitation of permitting and construction licences.

Currently, Google Fiber covers three cities, and there are expansion plans for five more across the United States.

Case study: Google Fiber, Uganda

Google Fiber's investment in Uganda, meanwhile, demonstrates that the approach Google took in the United States can also be replicated in developing markets. In this case, Google Fiber did not compete with broadband service providers. Rather, it chose to sell them wholesale services.

The lack of adequate infrastructure in Uganda has been a barrier to high-speed broadband availability and Internet maturity. For Google, this situation has hindered its ability to grow revenues in that market from online advertising, its core business. According to the ICT Association of Uganda, there are only a limited number of local players with the knowledge and resources to invest in broadband infrastructure. Even those few potential players may have been deterred from investing by a fear of assisting their competitors.

In November 2013, Google Fiber announced the deployment of a fibre backbone network in Kampala, enabling local mobile operators and ISPs to increase their data speeds up to 100 times faster than elsewhere in the city. The amount invested by Google Fiber has not been disclosed. However, as an indication, in 2006 the Ugandan government tried to implement a similar broadband infrastructure project at a cost of USD 100 million.

Google Fiber emphasizes the importance of local governments in creating the right environment to attract new entrants. According to Google, "[l]ocal government can actually play a large role in reducing the complexity of fibre networks just by giving new entrants access to maps of infrastructure, including maps of gas and water mains and things like expedited construction permits".[83] Making infrastructure available to new entrants is key to promoting network coverage expansion.

1.5.3 New financiers

Investment in broadband infrastructure may also come from more unlikely institutions such as hedge funds or corporate organizations that do not traditionally invest in broadband infrastructure. These organizations normally are driven by the opportunity to recoup their investment through public listing, when a company is sold, or through downstream revenues (that is, developing the broadband capacity allows other products and services to be sold).

The investments that can deliver the high levels of return sought by hedge funds normally carry a reasonable level of risk, often due to the sheer scale of the project or the uncertainty around the deployment of a new technology. As a result, these investments tend to involve multiple investors to spread the investment risk.

Box 1.8: Key lessons: Google Fiber (USA)

- Having easy access to economic infrastructure and utility ducts was a key reason for Google to select Kansas City, as it reduced the need for street digs. This, in turn, reduced investment costs and the time taken to offer services to the market. Governments and regulators should consider how they can increase the attractiveness of the investment environment to make the business case for new entrant investment commercially viable. This can be achieved through undertaking consulting services to understand investors' concerns.

- Government capital investment needs may be reduced by creating the correct investment conditions for private-sector investment and by working closely with operators. The favourable investment environment in Kansas City, which attracted Google, also benefited the local government, as it was not required to make an investment that it would otherwise have been unable to source. According to the Mayor of Kansas City, they would not have been able pass a bond issue for the investment required.

- The Federal Communications Commission (FCC) played no role in the network roll-out of Google Fiber in Kansas City. The main facilitator was the local government, which expedited the permit process, giving rights of way for little or no cost and allowing Google Fiber to build in desired areas.

- Heavy regulation can create a barrier to new entrants. One of the lessons Google Fiber took from deploying in Kansas City was that investment often flows into areas that are less affected by regulation.

Box 1.9: Key lessons: Google Fiber (Uganda)

- Local operators may be deterred from investing in broadband infrastructure by fear of assisting their competitors – particularly if required to offer parts of their network on a wholesale, open access basis.
- This concern can be reduced if regulators offer incentives such as a limited period of exclusivity, allowing the operator to recuperate their intial deployment investment before offering the network for wholesale access.
- Local governments in developing markets have a central role in attracting new providers. As in the previous case study, it is very important for new entrants to be clear about which infrastructure (e.g., ducts, poles) is available to them and where it is located.
- Google Fiber succeeded in installing the network in Kampala when the Ugandan government failed to do so in 2006. This indicates that a service provider motivated by end-user revenues can be more successful than a government-funded deployment project using a third party.

One example is Gigaclear, a new UK-based fibre broadband network operator that focuses on rolling out fibre networks across rural areas in England. It has been able to fund its business expansion with the support of equity funds. In February 2015, the company secured GBP 6.5 million from investors such as CF Woodford Equity Income Fund and Forward Private Equity[84].

Providers of Internet services such as Google and Facebook have also been involved in large-scale investments in broadband infrastructure. Both companies' business growth depends on people having adequate Internet access. The yearly revenue growth generated by these types of companies allows them to bear the risk of participating in large-scale investments.

Case study: SIGFOX, France

This case study demonstrates how a hedge fund might invest in a start-up global cellular technology developer, as opposed to investing in broadband infrastructure. Elliot Management is a hedge fund founded in 1977 in the United States. The company invests in debt and equity securities, with a focus on companies undergoing restructuring.

In 2015, Elliot Management participated in SIGFOX's Series D funding round[85]. SIGFOX is a French start-up that has developed a cellular connectivity technology for the "Internet of Things". It pioneered a very low-power, long-range, low-message-size RF protocol that operates in the bands below 1 gigahertz (GHz). This could enable a number of smart intiatives, but the technology is new and the applications are still evolving.

Elliot Management signaled its intention to support the expansion of the SIGFOX network in the United States, based on its belief that SIGFOX could provide a high return on investment in future years. The Series D investment round raised USD 115 million[86] from several investors, including Elliot Management, which was the only financial institution involved. Other investors included leading mobile operators (Telefonica, SK Telecom and NTT DOCOMO) and industrial partners (GDF SUEZ, Air Liquide and Eutelsat). The funding was earmarked for accelerating SIGFOX's worldwide network roll-out programme in Europe, Asia and the Americas, in association with international telecommunication operators.

The investors collectively stood to benefit from the development of "smart" applications in energy management, energy efficiency, sustainable cities, Internet-of-Things and machine-to-machine technologies. SIGFOX has signed a contract with TDF, continental Europe's biggest owner of broadcast and telecommunication masts, to expand TDF's national coverage. In 2014, SIGFOX partned with broadcast tower provider Arqiva to build a UK network dedicated to the Internet of Things. A year later, SIGFOX announced that it was

Box 1.10: Key lessons: SIGFOX

- Investing in more unfamiliar technology fields can raise the risk for investors but can offer an upside with high potential. Investing in new technologies is not Elliot Management's typical type of investment, but if SIGFOX succeeds as the prevailing technology to enable the Internet-of-Things market, the return on investment could be significant.

- Other fixed and wireless operators could consider investment from hedge funds, particularly for the expansion of fixed broadband networks. However, the lack of notable examples suggests that some hedge funds may be hesitant to invest in long-term infrastructure projects.

- It is interesting to note that the Series D funding was not made in isolation by a hedge fund alone, but in collaboration with a number of high-profile global partners, which stand to benefit from the success of the technology as it evolves. These "expert" investors can provide financial investors with a higher degree of certainty and reduce the risk. Technology companies looking for alternative sources of investment should consider a combination approach.

- Neither the telecommunication regulator nor the government had any direct investment in SIGFOX. However, regulators do still have overall responsibility for ensuring that the market environment is competitive and attractive for investment. In this instance, regulators will also have responsibility for making spectrum available for low-power wireless networks.

collaborating with Texas Instruments to integrate SIGFOX's technology into TI's chipsets.

Case study: Seacom, Africa

This case study was chosen to demonstrate that financial institutions (particularly those that focus on and understand the technology sector) also invest in broadband infrastructure projects.

In 2007, a venture dubbed Seacom was established to launch the first submarine cable system along East Africa, linking South Africa, Tanzania, Uganda, Kenya and Mozambique to major Internet connection hubs in Europe and Asia. Seacom's aim was to bring affordable and high-quality broadband to southern and eastern Africa as an alternative to expensive satellite technology, which was limited in service capability.

Since 2009, Seacom has been an open access undersea cable system supporting high-bandwidth connectivity. Seacom provides open access points of presence in various countries, and its global partners provide end-to-end wholesale connectivity for African operators. The resulting broad take-up of broadband across East Africa has largely been attributed to Seacom, which is 100 per cent privately funded.

Convergence Partners is a South African investment management company focused on the telcommunication sector in Africa. Its investments typically target ICT infrastructure development. Convergence invested USD 37.5 million of the total Seacom project cost of USD 650 million,[87] giving Convergence an equity share of 12.5 per cent of the cable system. Other investors in Seacom included Nedbank (offering long-term commercial loans), and various African economic development funds.

Convergence Partners made the investment in Seacom because it expected significant growth in data traffic following the exploding growth of mobile services in Africa. Results have been mixed since Seacom went live in July 2009. According to Remgro, a listed investment fund with a 25 per cent share of Seacom, the cable infrastructure company had lost money from 2011 through 2013. In 2014, though, Seacom's headline earnings were ZAR 40 million (USD 3.34 million[88]), compared with a loss of ZAR 32 million (USD 2.67 million) in the previous year[89].

Box 1.11: Key lessons: Seacom, Africa

- The role for regulators in this case was limited. There would need to be a case for regulatory intervention, which is currently unclear, particularly as the cable has brought about significant economic benefits and is available on an open access basis. In addition, coordinating regulatory efforts across a range of countries can be complex to implement. Regulators would need to undertake a comprehensive regulatory analysis and consider whether there is a case for intervention.

- Funding was not made in isolation but rather in collaboration with some high-profile global investors, which reduced the risk. In this instance, however, there was no investment by operators that could benefit from the infrastructure directly. This may be a contributing factor to the early losses.

- Investors should be fully aware of the demand characteristics behind their investments. Investment in large infrastructure projects carries high risk due to the high amounts required. For example, the infrastructure may be made available too soon, and there may not be enough demand to make the project commercially feasible in the short term. A reason for Seacom's poor financial performance is that the demand for data is not high enough.

- High prices for terrestrial broadband, lack of broadband penetration and low usage of high bandwidth services and applications are some reasons why the demand for data is not high enough. Regulators and governments can take actions to improve broadband take-up and the availability of broadband services to improve the market attractiveness for investors.

The financial performance of Seacom indicates the high level of risk that large infrastructure projects involve. Over time, it is likely that terrestrial connectivity prices will decrease, and the demand for Seacom's service is likely to increase. But its future earnings potential remains uncertain.

Case study: Facebook Asia–Pacific Gateway

This case study demonstrates an example of an established corporate organization investing in a relatively new market in the expectation of generating downstream revenues. The Asia–Pacific Gateway (APG) is a 10 000 km undersea cable project designed to improve Internet speeds for citizens and businesses in Asia. The fibre-optic cable will run directly from Malaysia to Korea (Rep. of) and Japan, with links branching off to other countries. It is designed to provide higher transmission speeds and reduce the current dependence on Singapore as the main regional gateway for Internet traffic. APG also is expected to minimize the number of Internet traffic hops, reducing latency and improving the user experience. Meanwhile, APG also will provide redundancy for existing cables, which have suffered from several breaks. In April 2015, for example, Internet users in Vietnam faced connectivity issues on the Asia-America Gateway cable that were expected to last three weeks[90].

Facebook saw these infrastructure problems as a hindrance to its users. With Southeast Asia becoming one of its fastest-growing markets, Facebook wanted to shore up the underlying infrastructure in the region. Facebook's motivation, therefore, was similar to that of Google and other software companies in wanting to support infrastructure in its high-growth markets. Facebook saw the APG as a chance to improve its users' experience in India, Indonesia, Malaysia, the Philippines, Hong Kong China and Singapore[91]. So in 2012, Facebook joined a consortium of investors supporting the APG roll-out, a move that boosted prospects for the project, which had been struggling with funding issues for three years. In addition to Facebook, the consortium included China Mobile, China Telecom, China Unicom, Chunghwa Telecom, KT Corp, LG Uplus, NTT Communications, StarHub,

Box 1.12: Key lessons: Facebook/Asia–Pacific Gateway (APG)

- Facebook's investment was the key enabler from a financing perspective. Notably, a number of high-profile global operators (and co-investors) will use the undersea cable and, as a result, are likely to direct international traffic onto it, contributing to its growth.

- The APG will use an open-access model to ensure all end users are able to utilize the asset without discrimination. This will be difficult to regulate, due to the multiple jurisdictions that the cable will run through. Success of the "self-regulated" system will depend on cooperation among the operators themselves.

- Although governments and regulators in Asian countries did not play a prominent role in the formation of the APG, they will still play an essential role within countries to extend broadband penetration and to drive user demand.

Time dotCom (Global Transit), Viettel, and Vietnam Posts and Telecommunications Group (VNPT). The total investment from the 12 members of the consortium was USD 450 million (Facebook's investment amount has not been disclosed).

The APG cable is expected to be completed in 2016[92]. The intervention of regulators is unlikely, but consortium members likely will have equal access to broadband capacity.

1.5.4 Not-for-profit investors

In this context, the term *not-for-profit investors* refers to socially responsible entities (for example, a cooperative) that invest in the construction and operation of broadband networks that are – for the most part – separate from the networks of commercial service providers.

Commercial operators are more likely to require greater returns on their investment. By contrast, a not-for-profit investor is more likely to invest its profits (clearly depending on the agreement of the legal entity) back into the construction and operation of the broadband network. For this reason, not-for-profit broadband investments can be more commercially feasible in areas where the returns are too low (or too slow) for commercial operators.

Community broadband networks, for example, tend to be "self-build" projects located in remote geographical areas, where there is typically a lower commercial incentive for operators to roll out their networks. Project funding can be mortgaged to make it more affordable. Another alternative is to use crowdfunding (discussed in more detail in Section 6) to raise funds. This approach is more common in markets with high disposable incomes. According to a report published by the Plunkett Foundation,[93] the cost of rolling out fibre can be GBP 2 000 (USD 3 138) per property, using overhead cables, and higher if it requires digging trenches.

Self-build community broadband networks normally are based on FTTH technology. Communities can build these networks at a much lower cost than commercial operators can, as they do not charge commercial rates for undertaking the work or may offer to do it free of charge. Depending on the size of the community, a self-build network can be small in scale, and it may need to overcome a couple of challenges:

- it may be run by volunteers, creating an unsustainable situation in the long term; or

- it may not be vertically integrated and therefore may not be able to offer consumers the choice of services that larger commercial operators may be able to offer.

Some governments have supported these community initiatives. The Scottish government's Community Broadband Scotland (CBS) scheme, for example, provides financial support to communities for this purpose[94]. So far, the CBS has invested in at least nine projects in rural Scottish communities. Eligible communities can receive different kinds of grants during different stages of their projects, including:

- an initial scoping and feasibility assessment grant ranging from GBP 2 000 to GBP 5 000 (USD 3 138 to USD 7 845);
- a detailed project planning grant from GBP 7 500 to GBP 15 000 (USD 11 767 to USD 23 538); or
- capital investment in the broadband project, up to a maximum of 89 per cent of capital infrastructure costs.

Case study: Community broadband in Germany

Communities in rural Germany have joined their efforts successfully to finance the construction of a high-speed broadband network. The investors have included a mix of local governments, businesses and individuals. These communities are located in the German provinces of Nordrhein-Westfalen and Schleswig-Holstein, where they previously did not have access to adequate broadband services because of lack of commercial attractiveness for service providers. The government only provided funding for broadband connections with speeds up to 2 Mbit/s.

These communities used crowdfunding to pay for new broadband infrastructure, which then was rented to service providers, defraying the investment cost[95]. A minimum investment of EUR 10 000 (USD 11 392) could provide investors an annual interest return of between 3 and 5 per cent[96]. For the investment to go ahead, a minimum of 70 per cent of households in that community needed to sign up for a connection.

This approach proved successful. The largest such community consortium took shape in the province of Schleswig-Holstein, drawing a total investment of EUR 70 million. It started in 2010 and came to involve 50 communities[97].

Box 1.13: Key lessons: Community broadband

- Community broadband networks can be successful in deploying fibre networks in areas that are commercially unviable for operators. However, they are relatively new and still in the early phases of deployment, so it is not clear how commercially sustainable they will be in the long term.
- Community broadband networks will often require external financing to get started. Investments can be made by private crowdfunding , by government grants or a mix of the two. Governments offering grants should vet every stage of the grant award process to ensure the project is fully compliant with its investment criteria.
- Regulators may wish to ensure that communities receiving government grants offer the infrastructure on an open-access basis. However, this may reduce the returns to the community broadband network and so the community should consider the impact of this in its early business-planning stages.
- Communities should consider how the service portfolio might evolve over time as consumers increasingly demand over-the-top and streaming services, which require highly reliable networks. In addition, communities might find it difficult to negotiate the same competitive content deals that commercial operators are able to offer.
- Innovative business approaches can make it feasible for communities to invest in broadband infrastructure. In this case study, the investors retain ownership of the infrastructure and are entitled to a return on investment.
- This return could be used to offset possible borrowing needed for the project.

1.5.5 Investments in disruptive technologies

The term *disruptive technologies* refers to technical innovations that are being developed – but not yet in full deployment – that may offer an alternative to current technical solutions for the provision of broadband services. Investing in disruptive technologies can be high-risk, as it may be difficult for new technologies to challenge well-established ones that have been tried and tested. Disruptive technologies may also face implementation barriers due to regulatory concerns or from market players that feel their business model is threatened. Therefore, the financial backers of disruptive technologies tend to be non-traditional operators looking for alternative, low-cost means to address specific connectivity issues (e.g., in remote areas).

One such technology that is gaining prominence is the transmission of data using "white space" in the UHF spectrum range. The term *TV white spaces* usually refers to unoccupied portions of spectrum in the VHF/UHF terrestrial television frequency bands in some geographical areas. This approach can address issues such as the lack of available spectrum, because it is licence-exempt[98]. It also benefits from the strong propagation characteristics allowed by the UHF spectrum, meaning fewer base stations are required to cover a given area.

The interest in white-space technology is not confined to any particular region. Pilot projects have been launched across the world for different types of applications, such as connecting remote health units in Bhutan and providing Internet access on a ferry boat in Scotland[99]. Some countries have staged trials of TV white-spaces operations. Other countries – such as the US and UK – are developing TV white-space regulations[100].

1.6 Financial innovations in funding services and applications

So far, this chapter has looked at funding strategies used by investors and governments to finance broadband networks. But the digital ecosystem has evolved so that there is a very tight and direct relationship between the development of broadband infrastructure and the evolution of higher-layer services and applications. For example, the demand for broadband infrastructure is being driven by an increase in take-up and usage of higher-layer services and applications. Without broadband, it would not be possible to run the higher-layer services and applications. Given this tight relationship, and in the context of investment strategies, this section reviews what financial innovations are being used to fund investments in services and applications that depend on broadband connectivity.

Table 1.9: Types of financial innovations and related case studies

Financial innovation	Case study	Executing parties
Crowdfunding	Star Citizen, USA Pebble, USA Shyp, USA	Individuals Individuals Private investors
Pension funding	Hipcom, UK	Business owner
Bitcoin currency	mexBT, Mexico	Seedcoin
Charity or non-profit institutions	Aentropico, Colombia	INNPulsa and Fundación Bavaria

Source: Analysys Mason, 2015

These financial innovations are alternatives to other, more common financing sources such as bank loans, angel investment, venture capital or private equity. Those are all well-known means of financing and therefore are not discussed in this report. The section below provides a description of each new funding approach, followed by examples of companies that have benefited from that type of investment. Note that regulators have played a minimal role in deploying higher-layer services and so the role of regulators is not included in this section.

1.6.1 Crowdfunding

Crowdfunding is a significant and recent financial innovation that has lowered investment barriers, making investment more accessible to entrepreneurs. As the name suggests, crowdfunding raises investment from a large number of people over the Internet on a crowdfunding website such as Kickstarter, RocketHub or AngelList. It is also often called "peer-to-peer lending."

Individual investments can be as small as USD 15,[101] making it affordable enough for almost anyone to invest. With a large number of investors, each one incurs little individual risk, making it attractive for semi-professional or first-time investors. Entrepreneurs must submit their projects to a crowdfunding website, define the investment target, set the deadline for funding and list the reward to investors. The amounts raised by crowdfunding can vary from USD thousands to USD millions.

Start-up companies in various sectors (e.g. real estate, consumer products, technology) typically use crowdfunding, but it can also be employed to support investment in broadband infrastructure. Crowdfiber is a crowdfunding platform designed to raise funds to invest in high-speed broadband in communities across the United States. It allows communities to advertise their campaigns and collect funding,[102] and a more advanced version is available to service providers[103].

According to an industry survey report from Massolution,[104] crowdfunding was expected to reach USD 34.4 billion globally in 2015, jumping from USD 16.2 billion in 2014. Of the amount raised in 2014, 59 per cent was in North America, 21 per cent was in Asia and 20 per cent was in Europe.

The risks associated with crowdfunding will vary by the type of platform, the company or project receiving the funds, along with the amount invested. Crowdfunding can be categorized into three types: donation, equity and debt.

- **Donation** crowdfunding carries the risk of committing funds to a project that may not materialize.
- **Equity** crowdfunding investments can face the risk of lack of liquidity, equity dilution or loss of investment if the company defaults.
- **Debt** crowdfunding is subject to risks such as loss of investment and interest payments.

Financial regulation plays a very important role in making crowdfunding accessible. In the United States, the Securities and Exchange Commission (SEC) announced in March 2015 that it will be possible for non-accredited[105] investors to invest using equity crowdfunding.

Investors in donation crowdfunding tend to be driven by personal motivation. They are likely to have a connection to the company, brand or project being financed. In some cases, the reward from donating is just the personal gratification of contributing to a cause or project. In other cases, the investor may have access to privileges such as a discount or free access to a service or product.

In equity crowdfunding, investors receive an equity stake in return for the investment. Entrepreneurs define the amount of equity stake for the target funding, and investors' corresponding equity shares will depend on how much they invest in the project. The crowdfunding platform may actually recommend investment opportunities considered most attractive for that particular investor. This service can help investors decide on opportunities that have already gone through a filtering process.

In debt crowdfunding, the investor lends funds to a company and expects this amount to be returned, plus interest, by a fixed date. "Mini bonds" are a type of debt crowdfunding approach that recently has been made available to potential investors. Typically, more established companies use debt funding, although examples of such financing are still rare. It is possible that as debt crowdfunding matures, companies will use it to develop Internet-based services and applications.

Case study: Star Citizen, USA

This case study shows how donation crowdfunding can successfully attract investment through crowdfunding platforms as well as through a company website. Start Citizen is a video game that can be played online in a multiplayer mode. The game developer (who owned his own company) initially failed to convince private investors to invest in the video game's development. He then turned to crowdfunding, with a goal of raising up to USD 2 million. He hoped that this stake would then demonstrate to private investors that there was demand for the game, convincing them to contribute an additional USD 12 million[106].

The developer used the Kickstarter online platform and his own company's website. The benefit of using the website was an ability to avoid paying fees to crowdfunding platforms. Kickstarter, for example, will charge 5 per cent of total funds raised plus payment processing fees.

Box 1.14: Key lessons: Star Citizen

- Donation crowdfunding is typically exempt from regulation by financial services regulators, and can therefore be relatively straightforward to set up and to attract investors. However, investors should be aware that the lack of financial regulation may introduce risks, and they should be prepared to undertake their own due diligence to assess that risk.

- The Star Citizen project was funded using a combination of crowdfunding from a private platform (Kickstarter) and from the project's own website – thus reducing fees paid to the third party platform. This two-pronged approach can lower the costs for crowdfunding, but the project may lose visibility, particularly if the website is new or not seeing heavy traffic.

- Donation crowdfunding is more likely to be successful in developed markets where investors are also potential end users.

This approach proved to be so successful that the developer no longer needed to source funds from private investors. Since October 2012, the company has raised more than USD 81 million[107]. The vast majority of that amount was crowdfunded from the game's website. Only USD 2 million was raised from Kickstarter between October and November 2012.[108] Overall, the game received funds from almost 900 000 people, each paying an average of USD 90.

With this kind of fundraising, the investment risk is measured by the likelihood that the project will be completed once the target funding is achieved and by how much has been invested. For this project, the investment risk was measured by the following:

- the low minimum investment required (only USD 90); and

- the project founder's strong track record in developing video games.

An added benefit for the individual investors was that they could influence how the game was developed based on how much they invested. In addition, investors also had early and free access to the game,[109] which was due on the market in 2015[110].

Financial services regulators do not typically regulate donation crowdfunding. This model corresponds to something like a charitable donation or a non-monetary reward. As a result, it is not seen by regulators as an investment and is exempt from regulation.

Case study: Pebble, USA

Pebble is a company that develops technology for a range of smart watches that allow users to access apps using connectivity provided by a smartphone. For this value proposition to be feasible there must be good-quality data connectivity.

The company is relatively small and lacks the funds needed for product development. During its most recent fundraising session (April 2015), Pebble raised more than USD 20 million from more than 78 000 backers on Kickstarter. Pebble saw Kickstarter as the easiest and most efficient way to market its latest product to the audience most likely to want it. As a result, the company achieved its fund-raising target within three months.

The minimum required investment in Pebble was USD 159, in return for which the investors received a discounted price on a Pebble watch – the higher the investment, the lower the price. Backers of the project also received the watch before it was made available to the general public.

As mentioned in the previous case study, the intervention of financial services regulators in this type of fund-raising approach is unlikely.

Case study: Shyp, USA

This case study was chosen because the company used equity crowdfunding, which is gaining in popularity and *is* subject to financial regulation.

Shyp provides logistic services using a smartphone app. Shyp is available to download in iOS or Android formats but the service is only available to customers in San Francisco, New York City, Miami and Los Angeles. Shyp has been experiencing 20 per cent month-over-month growth, with online returns representing 15 per cent of its business. A large part of Shyp's business depends on the growth of the e-commerce industry, e.g. delivering packages for online shops and easing online returns for consumers.

As a start-up, Shyp did not have the funding required to launch its business. The entrepreneurs behind Shyp wanted their business to be featured on AngelList, a crowdfunding platform, so they could raise their visibility to potential investors. Shyp succeeded in being featured and raised USD 2.1 million from two syndicated investors. The investment risk for investors was high, as Shyp was a start-up when it initially received funding support, and funding was sought at an early seed stage.

Financial regulators have an important role to play in making equity crowdfunding an attractive alternative funding source. The requirements enforced upon crowdfunding platforms protect the consumer and the market's growth as a result. In February 2015, the Financial Conduct Authority, the UK's financial services regulator, introduced rules to regulate equity-based crowdfunding. These rules were designed to allow investors to assess the risk and to understand who will ultimately borrow the money. In the UK, the rules also applied core consumer-protection requirements to firms operating in this market. For example, client money must be protected and firms must meet minimum capital standards. Finally, firms running these platforms must have resolution plans in place so that if the platform collapses, loan repayments will continue to be collected and lenders will not lose out.

1.6.2 Pension funding

This financing approach allows entrepreneurs to use their own pension funds to secure a loan. The pension manager acts as the "investor" by granting a loan secured by the pension funds or the entrepreneur's business assets. Alternatively, the pension fund manager can also buy an asset from the business and lease it back.

The amount that entrepreneurs can raise depends on their loan collateral and the fund manager's risk aversion. For the pension fund managers, this approach allows them to generate additional revenue from existing assets. Businesses use pension funding at different stages of maturity. Some entrepreneurs use it to fund start-ups, while others use it to fund business expansion.

People dissatisfied with their pension fund's performance and unwilling to give up any ownership shares in their business to outside investors may find this approach appealing. As a preliminary step, entrepreneurs need to transfer part or all their pension savings into a self-invested personal pension or a small, self-administered scheme. These pensions give their owners investment powers such as the ability to invest in their own businesses. Only then can the fund

Box 1.15: Key lessons: Pebble

- Pebble used crowdfunding to finance the product development of its smart watch. The funds raised met the company's target, allowing it to proceed with the development of the new version of the smart watch.
- Using a crowdfunding platform allowed Pebble to target the people most interested in its products. These investors are likely to be "early adopter" consumers that follow the industry closely and are keen to have possession of the latest "must-have" gadget. Attracting early adopters is essential to any start-up company's business, as they wil be the most honest critics and will provide essential product improvement feedback.

Box 1.16: Key lessons: Shyp

- Shyp used equity crowdfunding to raise funds needed to launch the company. Securing a 'featured' position in the crowdfunding platform enhanced Shyp's chances of succeeding in its fundraising.
- The popularity of equity-based crowd-funding means that financial regulators and governments may need to start applying rules to protect consumers and investors in the event the firm collapses.
- The ability of firms to attract funding depends on the growth of digital industries and the e-commerce sector. Governments, therefore, may determine that they have a responsibility to promote the use of e-services to drive take-up and demand.

manager provide the financing. Research shows that this funding approach is currently available only in the UK, although it is possible that other countries could offer it in future.

The investment risk for this approach can be relatively low for the investor. The loan cannot exceed 50 per cent of the pension fund's net asset value and may also be secured against an asset of similar or higher value[111].

Case study: Hipcom, UK

This case study was chosen to show how a government can facilitate the use of financial resources that otherwise would be relatively static or untapped. Hipcom is a cloud communication company whose main business is buying telecommunication licences from providers and upgrading them for resale. This process is lengthy, and for the business to grow it requires additional sums of capital to buy new licences.

Allan Murdoch, Hipcom's former owner, wanted to invest in the company without diluting his equity or losing control of the company. Murdoch decided to use his own pension fund to capitalize his business expansion. The fund manager provided a loan to Hipcom based on Murdoch's pension fund amount. In return, Hipcom agreed to pay an interest rate to the fund manager.

The level of risk for the lender is relatively low in this case. The loan value must not exceed 50 per cent of the pension fund's net asset value and other company assets also can be used as collateral. Murdoch raised GBP 684 000 over three stages (GPB 329 000, GBP 155 000 and GBP 200 000). With this approach, he managed to strengthen Hipcom and retain the same equity stake in the business.

Box 1.17: Key lessons: Hipcom

- Hipcom obtained loans by using its owner's pension fund as collateral, allowing the business to expand and be more competitive.
- For pension fund managers, this funding approach can generate additional revenue from using existing funds as collateral for loans.
- This type of investment approach depends on government policy allowing pension funds to be used for such a purpose. By facilitating the use of resources that otherwise would be static, the government can create an incentive for people to increase their savings and help businesses to find alternative financing sources.

1.6.3 Bitcoin currency

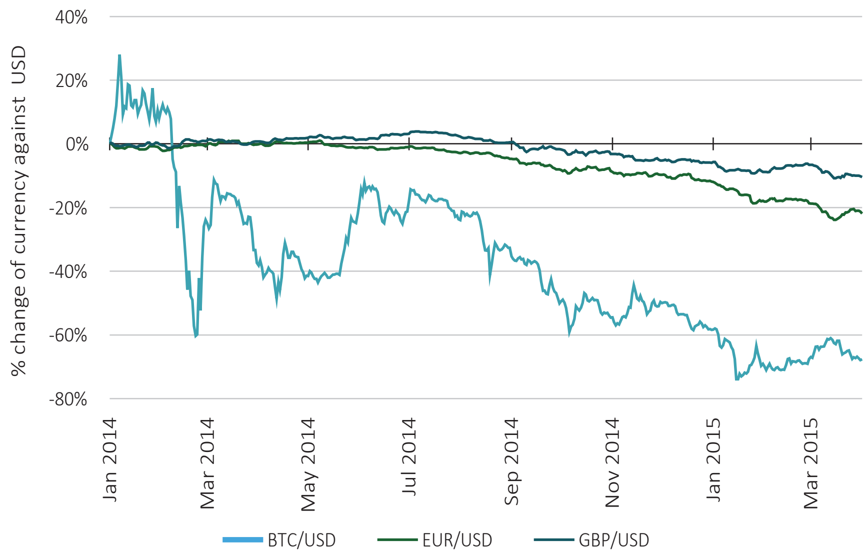
Bitcoin is a digital currency (represented by the currency symbol "BTC") that can be used to finance companies. Seedcoin, a start-up incubator, has invested exclusively in businesses using bitcoin currency, because it focuses on developing the bitcoin currency ecosystem. This financing approach is typically made available to start-ups.

Seedcoin also raises funds in bitcoin currency. This task can carry considerable risk, due to the currency's volatility. Between January 2014 and April 2015, for example, bitcoin lost over 60 per cent of its value against the U.S. dollar. Over the same period, the euro lost 22 per cent and the British pound lost 10 per cent against the U.S. currency (see Figure). This strong value volatility suggests that digital currencies may have a higher level of risk compared to more stable currencies. Entrepreneurs receiving funding in digital currency, therefore, need to consider its volatility as a risk. Another example of the high level of risk is the hacking theft of BTC 750 000 (USD 575 million) from the bitcoin exchange MtGox in 2014[112]. The uncertainty around digital currencies has led countries such as China and Russia to restrict how they can be used in their jurisdictions.

Based on previous funding rounds from Seedcoin, the size of the investment per company has ranged from BTC 100 to BTC 500. At the time of the latest funding round, April 2014, these values would have corresponded to around USD 50 000 and USD 250 000, respectively. The target markets of the start-ups vary by region and can include Africa (TagPesa) and Latin America (mexBT). TagPesa is an exchange and remittance company, based in Kenya, that aims to make it easy and convenient for people to make transactions and transfer money internationally[113]. One of the service's features gives Kenyans the ability to deposit and withdraw money from their M-Pesa (mobile banking) accounts[114]. In 2015, an Australian bitcoin exchange named "igot" acquired TagPesa.

The lack of regulation of digital currencies is a key factor in their associated risk. The uncertainty and distrust around digital currencies can lead to governments being reluctant to regulate them. The impact of regulation on the success of digital currencies was shown in January 2015, when Coinbase was announced as the first regulated bitcoin exchange in the USA. The value of the currency immediately rose to reflect that news, and then immediately fell again when California's state government labelled the announcement false[115].

Figure 1.7: Percentage change of selected currencies against the USD from January 2014 to March 2015



Source: Oanda, 2015

Box 1.18: Key lessons: meXBT, Mexico, 2014

- mexBT received funding in bitcoin from Seedcoin, an incubator, to develop a trading platform. Seedcoin's strong knowledge of bitcoin benefited mexBT. In very nascent markets, it is important to select partners that have a strong market knowledge, as this can determine the success of the start-up.

- Governments can promote the development of the digital currencies market by implementing adequate regulation. This framework should protect consumers and increase their trust and co

Case study: meXBT, Mexico

This case study demonstrates how governments can promote the development of the digital currencies market by implementing adequate regulation. meXBT is a platform for trading digital currencies such as bitcoin and litecoin. One of its objectives is to cater to the remittances market, particularly between Mexico and the United States. The company is based in Mexico and provides services in Latin America. mexBT seeks to help the "un-banked" population move money using mobile phones. The company partners with cash-payment processors to facilitate deposits and withdrawals.

The company required funding to develop its trading platform, so it applied to receive support from Seedcoin, which invested BTC 250 in mexBT in 2014[116]. At the time, this amount corresponded to about USD 150 000 (after bitcoin's precipitate drop in value the next year, that value was closer to USD 62 000)[117]. The equity share Seedcoin received for its investment was not disclosed, but it typically varies between 10 and 20 per cent[118]. meXBT claimed that the support from Seedcoin was very important not only for funding but also from a mentoring perspective, due to the incubator's expert knowledge of the bitcoin market. In November 2014, mexBT launched its trading platform.

The investment risk for Seedcoin was very high, because meXBT was a start-up when it received the funding support. The currency's volatility added to the risk by making the value of the funding amount uncertain. In March 2015, the UK government began regulating bitcoin exchanges to prevent them from being used for money laundering, an initiative applauded by the UK Digital Currency Association as being very important to increase the adoption of digital currencies.

1.6.4 Charity or non-profit institutions

Some charity or non-profit institutions are involved in financing businesses. Their investments normally are related to the mission of the institution, and businesses eligible for this type of financing usually are seen as promoters of economic or social development. Start-up companies are typically the beneficiaries of this type of support.

For entrepreneurs, this funding approach usually means not having to give up equity in their companies to investors. The amounts made available through such funding can vary significantly. Fundación Bavaria in Colombia claims to have financially supported 388 start-ups with a total of USD 8 million[119]. This support represents an average of USD 22 000 per business. In the UK, Nesta, an innovation charity, supports businesses seeking first-phase investments of between GBP 150 000 (USD 235 379) and GBP 1 million[120] (USD 1.57 million).

The investment risk is usually high, because the beneficiaries typically are start-ups, but the goal usually isn't getting a return on investment as much as achieving expected socio-economic gains through the start-ups. Often, this kind of funding involves local non-profits supporting the needs of local entrepreneurs, giving them a foundation to develop and to become attractive to other investors. These funding initiatives may be spurred by financial regulations. For example, a government might provide tax breaks to institutions that support businesses or projects with a positive social or economic impact.

Case study: Aentropico, Colombia

Aentropico is a "big data" company, founded in Colombia in 2012, that provides predictive analytics services to businesses. It aims to make its service easy to use and accessible to a large base of customers. This type of service typically is delivered over a web interface and therefore requires reliable broadband connectivity.

In its first year, Aentropico started its search for funding with a small team and a platform at a very early stage of development. It succeeded raising USD 45 000 from private investors[121]. In 2013, Aentropico raised USD 110 000, of which USD 20 000 was received from INNPulsa, a government-funded incubator,[122] and Fundación Bavaria, an institution that sponsors development-oriented initiatives. Both institutions' missions are to support the growth of Colombia's business sector. The funds were offered to Aentropico as grants; Fundación Bavaria and INNPulsa were not expecting to receive a financial return. For Aentropico, this type of funding meant that it did not have to dilute its equity stake, safeguarding capital for later and attracting investment from other parties.

The grants, together with funding received from investors such as Start-Up Chile and StartupBrasil, allowed Aentropico to keep growing its team and develop the platform. Today the company is selling its products to clients across Latin America.

1.7 Conclusions

Based on the case studies presented in this chapter, this section summarizes the key lessons and best practice approaches to implementing regulatory frameworks and policies in order to attract investment in broadband networks and higher-layer services. This section also summarizes the investment trends across each of the case studies reviewed. Care should be taken, however, in interpreting these trends, because the sampling of case studies needs to be significantly greater to be statistically representative. Therefore, at best the case studies can be considered illustrative, and the trends can be tested further through more analysis and research.

1.7.1 Investment trends

This section summarizes the investment trends discussed in each of the case studies. By plotting the value of the investment of each case study (x axis) and the economic maturity of the region where the investment was made (y axis) it is possible to derive an investment trend for:

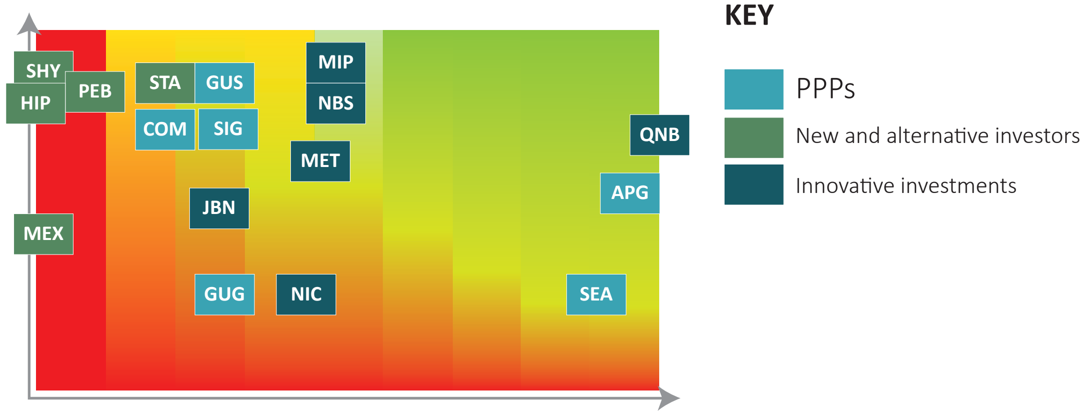
- traditional PPP broadband investments;
- new market entrants and alternative investors; and
- innovative investors financing higher-layer services.

The results are shown in the chart in Figure 2.8. As previously mentioned, however, care should be taken when interpreting these trends,

Box 1.19: Key lessons: Aentropico

- Grant funding from non-profit organizations means that companies do not have to relinquish any of their any equity or ownership, which can be significant in attracting further, private-sector investment.
- Non-profit funding is particularly relevant during the initial stages of a business, when it can be very challenging to attract private investors.
- Governments can foster non-profit initiatives in different ways. A direct approach is to form agencies such as INNPulsa, which help fill in the gaps where there are no private investors. Other, less direct approaches could include rewarding companies that invest in projects of socio-economic importance with fiscal benefits.

Figure 1.8: Summary of investment trends



Abbreviations

MIP	Mobile Infrastructure Project	SIG	SIGFOX
NBS	National Boradband Scheme	APG	Facebook Asian-Pacific Gateway
NIC	national ICT Backbone (NICTBB)	SEA	Seacom
JBN	Johannesburg National Broadband Project	SHY	Shyp
MLi	Metroweb	HIP	Hipcom
QNR	Qatar NRN	MEX	meXBT
GUS	Google US	STA	Star Citizen
GUG	Google Uganda	PEB	Pebble
COM	Community broadband		

Source: Analysys Mason, 2015. Note figures are not abailable for MGTS

as the sample size is small and not statistically representative. Still, several observations and implications for investing in broadband networks seem to emerge:

- PPP investments in developing and developed markets are largely similar in value, e.g., ranging from around USD 100 million to USD 245 million. The exception is Qatar, which has access to significant funds. This would suggest that investments are of a similar scale, although investments made in developing markets are likely to target different outcomes than those in established economies. For example, PPPs in developing markets largely focus on building core national infrastructure, while in developed markets PPPs aim to maximize last-mile broadband coverage to rural areas or to increase transmission speeds.

- In contrast to PPPs, investments by new market entrants and alternative investors tend to have a greater vertical and horizontal spread than traditional PPP investments. The horizontal spread suggests that these investors are prepared to invest in higher-value broadband projects, as well as those of lower value. The vertical spread suggests that the alternative investors are equally likely to invest in developing and developed markets.

- Investment in higher-layer services is predominant in developed markets. This is partly due to the maturity of the Internet ecosystem, which fosters technical innovation and investment. With the exception of crowdfunding, these investments have initially attracted low amounts of funding, suggesting that most of these options would currently be unsuitable for investment in any significant broadband infrastructure project.

1.7.2 Summary of best practice regulatory considerations

Based on a review and critique of the case studies presented in this report, the following considerations can be identified:

- Regulatory frameworks have had a direct impact on government-funded broadband PPP projects in which a national broadband infrastructure was being partly funded by the state or through other public funds. Often, this resulted in the regulator mandating wholesale access to the infrastructure on an equal, open-access basis. Regulators play a key role in ensuring that wholesale networks owned by dominant operators – particularly when funded by public funds – are available on a non-discriminatory basis to help reduce the costs and barriers for new market entrants wishing to invest in broadband infrastructure. Open access can be mandated by the regulator through a licensing process or by ensuring that government fibre deployments are designed on an open-access basis to promote infrastructure competition.

- Rural interventions have largely led to deployment of wireless solutions due to the challenging economics of rural and hard-to-reach areas. Regulators have played an important role in encouraging operators to explore alternative ways of reducing costs for such wireless networks. The interventions vary in their nature, from building shared, passive infrastructure to encouraging active infrastructure sharing and spectrum pooling. Regulators will need to set up processes to monitor the market to ensure that operators are being treated fairly. They will also need to set out guidelines for sharing infrastructure and pooling spectrum if these are being considered.

- Network-sharing deals (particularly for mobile operators) have been subject to much less regulatory and competition oversight than in-market consolidation deals. A wave of network outsourcing deals has convinced regulators that operation of networks and delivery of services are two distinct things. Meanwhile, end users benefit from improved coverage, particularly in rural areas.

- Regulators may play a role in directing investment or offering licences to encourage broadband investment in those areas needing it most. Regulators can also ensure that licensed operators meet performance standards, that interconnection agreements are upheld, and that prices are competitive. In these cases, regulators need to set up processes to gather market information and monitor the market on a regular basis. Other, less direct roles include facilitating information-sharing by providing up-to-date broadband coverage and mapping data, allowing infrastructure investment to be prioritized in those areas where market failure has occurred.

Regulators have also played a key role in attracting new market entrants, leading to innovative approaches to broadband investment. Regulators can:

- Allow operators to decommission and liquidate their copper networks, which can provide an attractive cash source to invest in broadband networks. However, this will only be possible in countries without mandates for wholesale services such as local loop unbundling (LLU) and bitstream services, which may have to be preserved for open-access availability to other providers.

- Ensure that market conditions are conducive to attracting investment from new entrants. For example, it is important for new entrants to be clear about the existing infrastructure (e.g. ducts, telephone poles) they can use and the rules that guide that usage. Other important aspects include having quick access to construction and permission licences.

- Consider authorizing pilot projects to attract market interest, in order to promote investment in new technologies. Regulators' reluctance to facilitate technical trials, particularly with wireless technologies, may dampen investment.

- Play a role in encouraging community broadband networks. In February 2015, the U.S. Federal Communications Commission allowed two community broadband providers in the states of Tennessee and North Carolina to expand the geographical range of their services. The law in these two states had previously prevented such expansion from taking place.

Some of the regulatory factors investors consider particularly important are detailed extensively in the 2009 edition of *Trends in Telecommunications Reform*.[123] These aspects are still valid considerations that regulators and governments should take into account when developing or considering regulatory policy.

Box 1.20: Regulatory factors relevant for investors

- **Design of the legal framework**: Whether the telecommunication law establishes a regulator and defines its role, scope of responsibility, accountability and market objectives.

- **Licensing regime**: The extent to which licence obligations are transparent or come with additional burdens such as administration, reporting and fees.

- **Interconnection regime**: Whether there is a well-designed and implemented interconnection regime that protects investors from below-cost interconnection payments from operators or unreasonable rate mandates from regulators.

- **Regulatory fees and taxation**: Whether there are excessive fees and taxes, which can increase operating costs and discourage innovation and further investment.

- **Universal service funds (USF)**: Whether operators are obliged to contribute to USFs and have the ability to access them to fund investment in cases of market failure.

- **Competition policy**: The regulators' effectiveness in protecting new operators against the abuse of market power from existing dominant operators, and in promoting fair competition through non-discriminatory, wholesale, open access to dominant operator infrastructure.

- **Tariff regulation**: The ability of the regulator to implement tariff regulation in developing regions or in the provision of services where there is ineffective competition.

- **Spectrum management**: Whether scarce spectrum is over-priced and overburdened with coverage obligations, thereby decreasing the operators' available capital to invest in infrastructure.

Endnotes

1 Telecoms services market is defined as retail and wholesale, fixed and mobile voice and data services

2 Source: https://www.itu.int/net/pressoffice/press_releases/2014/23.aspx

3 Includes fibre to the cabinet (FTTC), fibre to the building (FTTB) and fibre to the distribution point (FTTdp)

4 Analysys Mason FTTx roll-out and capex worldwide: forecasts and analysis 2014–2019

5 Includes all deployments in which fibre runs all the way to the subscriber's premises. FTTH includes passive optical network (PON) and point-to-point (PTP) architecture, and includes (despite the acronym) broadband fibre connections to business sites. However, it does not include uncontended dedicated fibre-leased lines.

6 ITU, World Telecommunication/ICT Indicators database and Measuring the Information Society report, 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

7 LTE-A LTE Advanced is a mobile communication standard and a major enhancement of the Long Term Evolution (LTE) standard

8 Source: Analysys Mason Global Telecoms Market Interim Forecast update 2014–2019

9 Source: Analysys Mason public small cells worldwide forecast and analysis 2015 to 2020

10 Public Wi-Fi is Wi-Fi service provided in public areas, such as retail districts, tourist attractions, food chains, coffee shops, business districts, railway stations etc. Private W-Fi is service provided within a home or business intended for use by the home occupants, or by employees of the business.

11 Source: Analysys Mason, 2015

12 See http://www.analysysmason.com/About-Us/News/Insight/France-consolidation-Jun2014/#17%20June%202014

13 See http://www.zdnet.com/article/middle-east-africas-mobile-giants-take-first-steps-on-sharing-networks-to-cut-costs-boost-rural-coverage/

14 See http://www.growthbusiness.co.uk/news-and-market-deals/business-news/2443992/david-cameron-heralds-growth-of-londonand39s-tech-city-on-threeyear-anniversary.thtml

15 See http://www.londonandpartners.com/media-centre/press-releases/2014/12032014-tech-city-launch

16 See http://www.techcityuk.com/investors/#investor-top

17 See http://www.ispreview.co.uk/index.php/2015/01/virgin-media-business-brings-faster-broadband-londons-tech-city.html

18 See http://www.theguardian.com/business/2014/jul/30/bt-trial-broadband-system-london-slow-tech-city

19 See http://techcitynews.com/2015/03/26/uk-accounts-for-42-of-european-fintech-deals-in-2014/

20 It defined PPP as referring to any project where there is a mix of private- and public-sector involvement.

21 See http://ec.europa.eu/regional_policy/sources/docgener/presenta/broadband2011/broadband2011_en.pdf

22 See http://www.analysysmason.com/About-Us/News/Press-releases1/Broadband-PPP-projects-Oct2012/#03%20October%202012

23 See https://www.gov.uk/government/publications/2010-to-2015-government-policy-communications-and-telecomms/2010-to-2015-government-policy-communications-and-telecomms

24 See http://www.superfastcornwall.org/

25 See http://gov.wales/topics/businessandeconomy/broadbandandict/broadband/ngbw/?lang=en

26 See http://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=787:ncc-announces-mainone-ihs-winners-of-infraco-licence&catid=117:editorials&Itemid=5

27 See http://www.skmm.gov.my/Sectors/Broadband/National-Broadband-Initiative.aspx

28 See http://www.senado.gov.br/noticias/Jornal/emdiscussao/banda-larga/telebras.aspx

[29] See http://www.med.govt.nz/sectors-industries/technology-communication/fast-broadband/rural-broadband-initiative

[30] See https://www.itu.int/osg/spu/ni/3G/casestudies/sweden/Sweden_fin3.doc

[31] See http://www.ispreview.co.uk/index.php/2014/12/gbp150m-uk-mobile-infrastructure-upgrade-project-makes-slow-progress.html

[32] See http://www.ispreview.co.uk/index.php/2014/12/gbp150m-uk-mobile-infrastructure-upgrade-project-makes-slow-progress.html

[33] See http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/telecoms-networks/uk-5.20and5.21

[34] See http://www.thejournal.ie/national-broadband-scheme-ending-1609666-Aug2014/

[35] See http://www.thejournal.ie/national-broadband-scheme-ending-1609666-Aug2014/

[36] See “Broadband now available in every district in Ireland”, http://www.dcenr.gov.ie/Press+Releases/2010/Broadband+now+available+in+every+district+in+Ireland.htm

[37] Source: EU Digital Agenda for Europe (DAE) Scoreboard, 2014

[38] See http://www.slideshare.net/CommonwealthTelecommunications/broadband-infrastructure-development-challenges-in-tanzania

[39] See http://www.joburg.org.za/index.php?option=com_content&task=view&id=1223&Itemid=168

[40] See http://www.auvergnetreshautdebit.fr/qui-sommes-nous/

[41] See http://www.dcenr.gov.ie/Communications/Communications+Development/Metropolitan+Area+Networks/

[42] See http://www.shetland.gov.uk/news-advice/ShetlandIslandsCouncil-InformationBulletins-TelecomCableInfrastructure.asp

[43] See http://www.digitalregion.co.uk/

[44] See https://broadbandeurope.wordpress.com/public/

[45] See http://projectisizwe.org/funding-for-free-wifi/

[46] See https://www.westerncape.gov.za/speech/state-province-address-2014

[47] See http://www.balancingact-africa.com/news/en/issue-no-602/top-story/tanzania-government/en

[48] See http://waset.org/publications/9997991/the-impact-of-nictbb-in-facilitating-the-e-services-and-m-services-in-tanzania

[49] See Analysys Mason Tanzania telecoms market report 2015.

[50] See http://www.fin24.com/Tech/News/Joburg-takes-back-control-of-broadband-project-20150219

[51] See http://www.iol.co.za/news/south-africa/gauteng/r1bn-joburg-broadband-project-under-fire-1.1741234#.VV7uLbnbJ_I

[52] See http://www.fin24.com/Tech/News/Joburg-takes-back-control-of-broadband-project-20150219

[53] See http://www.eib.org/epec/resources/epec_broadband_en.pdf

[54] See http://www.reti.regione.lombardia.it/cs/Satellite?c=Redazionale_P&childpagename=DG_Reti%2FDetail&cid=1213693098477&packedargs=NoSlotForSitePlan%3Dtrue%26menu-to-render%3D1213542547392&pagename=DG_RSSWrapper

[55] See http://www.ghana.gov.gh/index.php/news/1293-president-mahama-inaugurates-38-million-fiber-optic-backbone-project

[56] See http://allafrica.com/stories/201305270024.html

57 See EU Scoreboard, based on June 2014 data

58 See http://www.telecompaper.com/news/metroweb-plans-to-expand-network-to-two-more-cities-report--1074238

59 See https://www.telegeography.com/products/commsupdate/articles/2015/04/01/metroweb-looks-at-two-new-fibre-markets/

60 See https://www.telegeography.com/products/commsupdate/articles/2014/11/20/telecom-italia-still-circling-metroweb/

61 See http://www.qnbn.qa

62 See http://www.nbnco.com.au/

63 See http://www.gitpa.es/en/the-asturcon-network.html

64 See http://www.stokab.se/In-english/

65 See https://broadbandeurope.wordpress.com/jv/

66 See http://www.csipiemonte.it/web/en/documentazione/documentation-en/profile-en/592-brochure2014/file

67 See http://www.investintrentino.it/Government/Infrastructures-and-strategic-projects/Telecommunication-infrastructures

68 See http://www.elard.eu/elard/national-leader-networks/en_GB/lithuanian-rural-communities-union

69 See http://qnbn.qa/qnbn_article/delivering-on-the-vision/

70 See http://qnbn.qa/qnbn_article/delivering-on-the-vision/

71 See http://qnbn.qa/qnbn_article/delivering-on-the-vision/

72 See https://www.telegeography.com/products/commsupdate/articles/2014/10/03/vodafone-qatar-agrees-to-buy-qatar-national-broadband-network/

73 See more detail at http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/#28%20October%202014

74 See http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/#28%20October%202014

75 See http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/#28%20October%202014

76 See http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/#28%20October%202014

77 See http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/#28%20October%202014

78 See http://www.forbes.com/sites/eliseackerman/2012/08/04/how-kansas-won-the-google-fiber-jackpot-and-why-california-never-will/

79 See http://www.businessinsider.com/the-cost-of-building-google-fiber-2013-4?IR=T

80 See http://www.techrepublic.com/article/comcast-time-warner-take-on-google-fiber-in-kansas-city-can-the-incumbents-compete/

81 See http://www.theverge.com/2015/2/17/8050935/att-google-fiber-kansas-city-gigapower-internet-price-match

82 See https://fiber.storage.googleapis.com/legal/googlefibercitychecklist2-24-14.pdf

83 See http://telecoms.com/200521/uganda-is-next-stop-for-google-fibre-project/

84 See http://www.gigaclear.com/gigaclear-secures-additional-6-5m-to-accelerate-rollout-of-gigabit-rural-broadband/

85 See http://techcrunch.com/2015/02/11/sigfox-raises-115m-to-take-its-internet-of-things-network-global/

86 See http://techcrunch.com/2015/02/11/sigfox-raises-115m-to-take-its-internet-of-things-network-global/

87 See http://www.convergencepartners.com/wp-content/uploads/SEACOMAnnouncement-ver3.pdf

88 Assumes an exchange rate of USD0.084 per ZAR

89 See http://remgro.com/wp-content/uploads/pdf/2015/Results_31Dec2014.pdf

90 See http://www.thanhniennews.com/tech/intl-connections-in-vietnam-may-fully-recover-in-3-weeks-42574.html

91 See http://www.pcworld.com/article/258844/facebook_buys_a_stake_in_450m_asian_undersea_cable_consortium.html

92 See https://www.time.com.my/aboutus/newsroom_detailed.asp?id=236&ddlYear=2015

93 See http://www.carnegieuktrust.org.uk/getattachment/49d067b8-5836-4906-bfe0-70978c6ca5e9/Rural-Broadband---Reframing-the-Debate.aspx

94 See http://www.hie.co.uk/community-support/community-broadband-scotland/funding/default.html

95 See http://www.governancereport.org/home/governance-innovations/featured-innovations-2014/broadband-crowdfunding-germany/

96 See https://books.google.co.uk/books?id=XlL1AgAAQBAJ&pg=PA86&lpg=PA86&dq=crowdfunding+broadband+germany&source=bl&ots=RvNI8TVdFr&sig=5#v=onepage&q=crowdfunding%20broadband%20germany&f=false

97 See http://www.breitbandnetzgesellschaft.de/die-initiative/ausbauplan/

98 See License-exempt framework refers to devices operating on a non-interference/non-protection basis in compliance with technical specification and/or band rules without the need for an individual device license. See ITU, Trends in Telecommunication Reform- special edition- 4th generation Regulation, Chapter 3 – TV white spaces: managing empty spaces or better managing inefficiencies? www.itu.int/specialtrends

99 See http://www.scotsman.com/news/scotland/top-stories/rural-scotland-to-lead-with-white-space-internet-1-3569913

100 See ITU, GSR14 Discussion paper on new frontier in spectrum licensing, http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Session4_GSR14-DiscussionPaper-SpectrumLicensing.pdf

101 See https://www.crowdcube.com/pg/investing-your-money-1513

102 See http://www.crowdfiber.com/campaigns

103 See http://www.crowdfiber.com/service-provider-edition

104 See http://www.finextra.com/news/fullstory.aspx?newsitemid=27188

105 See the definition of accredited investors by SEC at http://www.sec.gov/answers/accred.htm

106 See http://www.crowdfundinsider.com/2014/11/55071-brief-star-citizen-creator-discusses-crowdfunding-video-games-development-video/

107 See https://robertsspaceindustries.com/funding-goals

108 See http://www.cnbc.com/id/102021804

109 See https://www.kickstarter.com/projects/cig/star-citizen/description

110 See http://www.polygon.com/features/2015/3/2/8131661/star-citizen-chris-roberts-interview

111 See https://www.pensionledfunding.com/press_release/10-things-you-need-to-know-aboutpension-led-business-funding/

[112] See http://www.telegraph.co.uk/finance/currency/10686698/Bitcoin-exchange-MtGox-faced-150000-hack-attacks-every-second.html

[113] See http://www.seedco.in/home/havelock/sf2

[114] See http://www.howwemadeitinafrica.com/bitcoin-exchange-expands-to-kenya-sees-potential-in-using-m-pesa/47442/

[115] See http://www.coindesk.com/california-regulator-coinbase-exchange-regulated-licensed/

[116] See http://www.coindesk.com/seedcoin-gives-btc-sx-500-bitcoins-funding/

[117] See http://www.coindesk.com/seedcoin-gives-btc-sx-500-bitcoins-funding/

[118] See http://www.coindesk.com/bitcoin-startup-incubator-seedcoin-raises-2000-btc-funding-round/

[119] See http://www.marketsgroup.org/news/destapa-futuro-and-angel-investment-in-colombia

[120] See http://business.scotland.gov.uk/view/funding/nesta-venture-investment

[121] See http://lavca.org/2014/01/29/entrepreneur-profile-sebastian-perez-saaibi-ceo-juan-pablo-marin-diaz-cio-aentropico/

[122] See http://lavca.org/2014/01/29/entrepreneur-profile-sebastian-perez-saaibi-ceo-juan-pablo-marin-diaz-cio-aentropico/

[123] See https://www.itu.int/pub/D-REG-TTR.11-2009

Annex 1 – Procurement principles

Fairness and equitability

Fairness and equitability require that a procurement process be procedurally fair and non-discriminatory. The procurement specification and decision-making criteria (i.e., the evaluation criteria) should not favour any particular bidders. Also, the procurement specification should be written in a manner that is technology-neutral. It should define a clear set of output requirements and service quality standards independent of the technology used to achieve these requirements. All participants in the procurement must be given the same information before and during the process, including any clarifications or modifications to the specification or the decision-making criteria.

Transparency

Transparency requires openness throughout the entire procurement process. The process should be undertaken in a transparent manner, in public and not behind closed doors. All information regarding the tender specification and the procurement process must be made available and accessible to all potential bidders before, during and after the process. For example, a pre-tender information notice published on a central website or leading broadsheet newspaper can be used to alert all potential bidders to the intended procurement.

In addition, bidders should be given access to a publicly available, detailed broadband network coverage map to demonstrate where public investment will *not* be targeted – i.e., where broadband networks are already available. This exercise should be conducted as a public, open consultation.

The requirement-specification and decision-making criteria should be made clear and followed throughout the procurement process. Where government aid is involved, selection of a preferred bidder should lead to the publishing of a notice detailing the name of the winning bidder, the amount of aid to be provided, the intensity of aid and the technology chosen.

Competitiveness

Bidders should be selected through a competitive procurement procedure, to minimize the need for public subsidy. Projects involving public subsidy can be particularly complex to procure. In Europe, a competitive dialogue procedure improves communication between the contracting authority (in this case the government) and bidders. This can lead to better designs and innovative solutions. Competitive dialogue can also increase competitive tension and allow better value to be extracted from bidders. However, competitive dialogue can be complex (see Figure A1.1) and costly in terms of time and procurement resources, and therefore other options also should be considered[1].

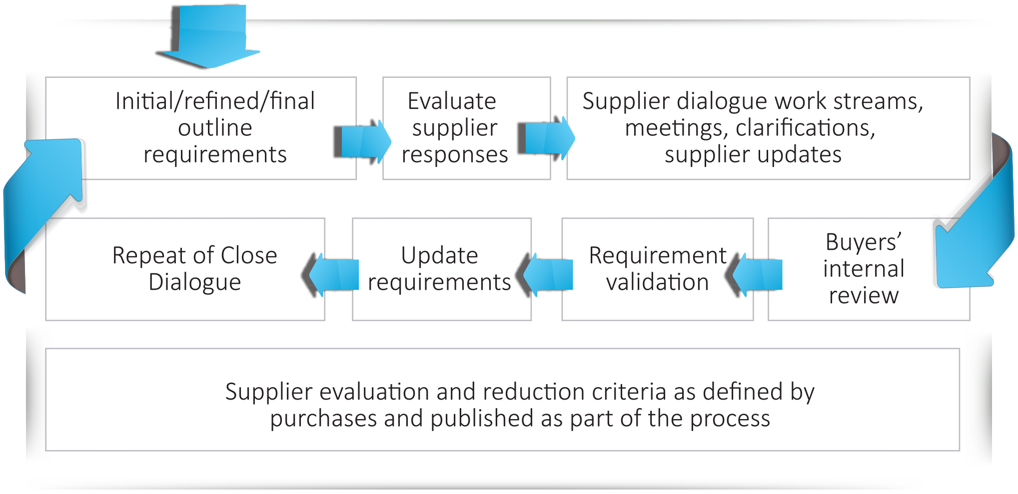
Government award of a subsidy following a competitive procurement may limit market competition, especially if the funding goes to an already-dominant operator or an operator that subsequently becomes dominant. So, public network procurements should enable competing operators or retail service providers to offer competitive and affordable services to end users. The award criteria should favour bids proposing wholesale or passive network models.

Cost-effectiveness

A government entity should try to procure equipment for a broadband network at the lowest possible cost. This can be achieved by selecting a bidder through a competitive procurement procedure (as described above). This approach is different from awarding a contract to the bidder with the lowest cost – a process that does not take non-price-related criteria into account. Consequently, the evaluation of a tender should not exclusively depend on cost alone. The relative weight assigned to price and other criteria will vary, but bidders should be advised of that weighting and evaluation criteria well in advance. Such criteria may include, for example:

- geographical coverage,

Figure A1.1: Overview of competitive dialogue process



Source: Analysys Mason, 2015

- broadband speeds offered,
- competitive wholesale pricing,
- projected initiatives to stimulate broadband take-up,
- sustainability of the technological approach,
- proposed re-use of existing infrastructure, and
- impact of the proposed solution on competition in the market.

Value for money can be achieved in several ways, for example, by:

- Writing procurement specifications in output terms, enabling suppliers to consider and recommend cost-effective solutions that meet the requirements.
- Ensuring that the requirements are met but not exceeded (bidders may propose, for example. building a network in an area that is not considered to be a priority). Making network coverage maps available will be vital as part of this process.
- Introducing longer-term incentives into the contract to ensure continuous cost and quality improvements are made to the broadband network throughout its lifetime.
- Optimizing the cost of delivering the network over a longer-term, such as 15 years or more.

Use of existing infrastructure

Bidders should be encouraged to re-use existing infrastructure (where this is fit for purpose) to avoid infrastructure duplication and reduce the amount of public subsidy required. The government should consider setting up a national database containing information on the availability of existing infrastructure that could be re-used for broadband roll-outs.

Demand and rights of way

All efforts should be made not only to aggregate demand from government, but also to enforce rights of way. Demand aggregation can encourage operators to make broadband infrastructure investments in regions that they may otherwise consider commercially unviable. By demonstrating the demand for broadband services, operators may be convinced that there is a commercial case for investment.

Governments and regulators can also take steps to ensure that operators are not dissuaded from investing in broadband networks because of high costs or lengthy delays for acquiring fibre rights-of-way. For example, the Nigerian Ministry of Communications and Technology announced in June 2013 that, in order to help implement its national broadband plan, it had reduced the time for a rights-of-way application to be processed and reduced the cost per kilometre[2].

Endnotes

1 See EPEC, *Procurement of PPP and the use of Competitive Dialogue in Europe. A review of public sector practices across the EU*, available at http://www.eib.org/epec/resources/epec-procurement-and-cd-public.pdf

2 See http://www.internationallawoffice.com/newsletters/detail.aspx?g=681de6db-6cb0-4064-b8f9-f1f3feb4059e

Annex 2 – Sources

Case study: Mobile Infrastructure Project (MIP), UK, 2011

Sources:

- http://www.ispreview.co.uk/index.php/2014/12/gbp150m-uk-mobile-infrastructure-upgrade-project-makes-slow-progress.html
- https://www.gov.uk/government/policies/making-it-easier-for-the-communications-and-telecoms-industries-to-grow-while-protecting-the-interests-of-citizens/supporting-pages/improving-mobile-coverage

Case study: National Broadband Scheme (NBS), Ireland, 2007

Sources:

- http://ec.europa.eu/competition/state_aid/cases/221646/221646_729738_49_2.pdf
- http://www.thejournal.ie/national-broadband-scheme-ending-1609666-Aug2014/

Case study: National ICT Broadband Backbone (NICTBB), Tanzania, 2010–14

Sources:

- http://www.nictbb.co.tz/news.php
- http://www.telecompaper.com/news/ttcl-to-supply-bandwidth-to-neighbouring-countries–886443

Case study: Qatar National Broadband Network (QNBN), Qatar, 2011

Sources:

- http://www.telecompaper.com/news/qnbn-pledges-to-have-fibre-optic-network-in-qatar-by-2015-901175
- http://www.gulf-times.com/qatar/178/details/374129/ambitious-plan-for-high-speed-broadband
- http://qnbn.qa/qnbn_release/heads-of-agreement-announced-between-qnbn-vodafone-qatar/

Case study: MGTS, Russia, 2013

Source:

- http://www.analysysmason.com/Research/Content/Viewpoints/Copper-decommissioning-costs-Oct2014-RDTW0/

Case study: Google Fiber, USA, 2012

Sources:

- http://www.businessinsider.com/the-cost-of-building-google-fiber-2013-4?IR=T
- http://www.cnet.com/uk/news/google-to-test-ultrafast-broadband-to-the-home/
- http://www.technologyreview.com/news/510176/when-will-the-rest-of-us-get-google-fiber/
- http://www.techrepublic.com/article/comcast-time-warner-take-on-google-fiber-in-kansas-city-can-the-incumbents-compete/
- http://www.theverge.com/2015/2/17/8050935/att-google-fiber-kansas-city-gigapower-internet-price-match
- http://www.fastcompany.com/3036659/elasticity/lessons-from-googles-first-rollout-of-google-fiber

Case study: Google Fiber, Uganda, 2013

Sources:

- http://www.google.com/get/projectlink/
- http://www.iwayafrica.com/iwayafrica-uganda-launches-high-speed-fibre-access-to-sme-customers/
- http://www.ibtimes.com/google-goes-africa-why-western-tech-giant-digging-kampala-uganda-1487814

- http://www.technologyreview.com/news/521801/google-tries-to-turbocharge-internet-service-in-uganda/
- http://www.ibtimes.com/google-goes-africa-why-western-tech-giant-digging-kampala-uganda-1487814
- http://telecoms.com/200521/uganda-is-next-stop-for-google-fibre-project/

Case study: Elliot Management, USA/SIGFOX, France, 2015

Sources:

- http://www.reuters.com/article/2015/02/11/us-sigfox-fundraising-idUSKBN0LF06720150211
- http://www.fiercewireless.com/tech/story/iot-startup-sigfox-launching-902-mhz-network-nationwide-us/2015-03-03

Case study: Convergence Partners, South Africa/Seacom, 2009

Sources:

- https://manypossibilities.net/african-undersea-cables/
- http://www.pidg.org/impact/case-studies/seacom-undersea-cable

Case study: Asia–Pacific Gateway, Malaysia and Japan, 2012

Sources:

- http://www.bbc.co.uk/news/technology-18725728
- http://www.cnet.com/uk/news/intra-asian-submarine-cable-system-going-live-in-2015-as-koreas-kt-hooks-up/
- http://www.pcworld.com/article/258844/facebook_buys_a_stake_in_450m_asian_undersea_cable_consortium.html
- https://www.time.com.my/aboutus/newsroom_detailed.asp?id=236&ddlYear=2015
- http://www.thanhniennews.com/tech/intl-connections-in-vietnam-may-fully-recover-in-3-weeks-42574.html

Case study: Community broadband, Germany, 2008, 2010 and 2012

Sources:

- http://www.governancereport.org/home/governance-innovations/featured-innovations-2014/broadband-crowdfunding-germany/
- https://books.google.co.uk/books?id=XlL1AgAAQBAJ&pg=PA86&lpg=PA86&dq=crowdfunding+broadband+germany&source=bl&ots=RvNI8TVdFr&sig=5
- http://www.breitbandnetzgesellschaft.de/die-initiative/ausbauplan/

Case study: Star Citizen, US, 2012

Sources:

- https://www.kickstarter.com/projects/cig/star-citizen
- https://robertsspaceindustries.com/funding-goals
- http://www.itworld.com/article/2694217/networking/internet-operators-explore-improving-african-interconnections.html
- http://www.crowdfundinsider.com/2014/11/55071-brief-star-citizen-creator-discusses-crowdfunding-video-games-development-video/
- https://ignitiondeck.com/id/crowdfunding-a-video-game/
- https://www.kickstarter.com/help/fees?country=GB
- http://www.cnbc.com/id/102021804

- https://www.kickstarter.com/projects/cig/star-citizen/description
- http://www.polygon.com/features/2015/3/2/8131661/star-citizen-chris-roberts-interview

Case study: Pebble, US, 2015

Source:

- https://www.kickstarter.com/projects/597507018/pebble-time-awesome-smartwatch-no-compromises/description

Case study: Shyp, US, 2013–14

Sources:

- http://blog.angel.co/
- https://medium.com/@kevingibbon/how-we-built-shyp-on-angellist-and-raised-2-1m-1c723714f713
- https://medium.com/@kevingibbon/how-we-built-shyp-on-angellist-and-raised-2-1m-1c723714f713
- http://www.fca.org.uk/static/documents/crowdfunding-review.pdf

Case study: Hipcom, UK, 2015

Source:

- https://www.pensionledfunding.com/case_study/hipcom/
- https://www.pensionledfunding.com/press_release/10-things-you-need-to-know-aboutpension-led-business-funding/

Case study: meXBT, Mexico, 2014

Sources:

- http://www.coindesk.com/seedcoin-gives-btc-sx-500-bitcoins-funding/
- https://www.cryptocoinsnews.com/mexican-bitcoin-exchange-mexbt-launches-trading-platform/
- http://www.coindesk.com/bitcoin-startup-incubator-seedcoin-raises-2000-btc-funding-round/
- https://www.cryptocoinsnews.com/mexican-bitcoin-exchange-mexbt-launches-trading-platform/
- http://eleconomista.com.mx/tecnociencia/2015/04/06/mexbt-quiere-llevar-bitcoins-mundo-reglas-innovacion
- http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-government-to-regulate-cryptocurrency-to-avoid-money-laundering-says-treasury-10117566.html

Case study: Aentropico, Colombia, 2012

Sources:

- http://thenextweb.com/la/2013/12/28/12-latin-american-startups-look-2014/
- http://lavca.org/2014/01/29/entrepreneur-profile-sebastian-perez-saaibi-ceo-juan-pablo-marin-diaz-cio-aentropico/

Abbreviations

ARPU	average revenue per user
DBO	design, build and operate
FCC	Federal Communications Commission
FTTH	fibre to the home
FTTP	fibre to the premises
GPON	gigabit passive optical network
ICT	information and communication technologies
ISPs	Internet service providers
LLU	local loop unbundling
MNOs	mobile network operators
MTR	mobile termination rate
NGOs	non-governmental organizations
POPs	points of presence
PPPs	public–private partnerships
SAQ	subscriber acquisition costs
SPV	special purpose vehicle
WAN	wide-area network

2 Accelerating Broadband Deployment Through Network Sharing and Co-investment

Author: Malcolm Webb, Partner, Webb Henderson

2.1 Introduction: the value of network sharing

Governments around the world recognize that there are substantial societal benefits in deploying new broadband networks and services – for example, 4G wireless networks and fibre transmission lines. And many governments feel that current investment levels are insufficient.

Of course, these governments need to acknowledge that broadband networks are very expensive, particularly if deployed nationwide. Moreover, construction risks can be high and returns on investment are uncertain. So, governments may need to be creative and innovative to find ways to encourage operator investment and reduce the risks that operators face in deploying widespread broadband networks and affordable services.

Governments have tried to address these challenges in several ways. Some have chosen to build broadband networks themselves. Government-built access networks include NBN Co. in Australia and QNBN in Qatar, while backhaul/backbone networks have been constructed in rural areas of India, Argentina and Brazil. But building a nationwide broadband network is beyond the reach of many governments, particularly in the access or "last mile" segment. Backhaul and backbone networks are potentially more affordable – for example, the government of South Africa, a middle income country, has invested in backhaul/backbone through Infraco.

Other governments have chosen to incentivize a single operator to deploy the network, usually with a mandate to provide open access. Examples include the Malaysian government's arrangement for Telekom Malaysia to roll out a high-speed, broadband network and the agreement between the New Zealand government and Chorus to roll out a fibre-to-the home network.

This chapter considers whether governments should try an alternative approach: encouraging or providing incentives for *network sharing* (the term commonly used in the mobile sector) or *co-investment* (the term commonly used in the fixed sector). This approach enlists multiple operators – or even the government itself – as partners in solving the "further and faster" challenge of broadband deployment.

2.2 Advantages to governments of network sharing and co-investment

Governments are likely to view network sharing and co-investment initiatives positively, particularly in areas where there is limited scope for competition among multiple networks. In parts of many countries, there is only limited potential for network-based competition in fixed access and backhaul/backbone market segments beyond the main trunk routes. There is far greater latitude for infrastructure-based competition, however, in the mobile sector. Even then, it may make sense to build only a single mobile network in higher cost, low-ARPU ("Average Revenue Per User") regions.

This chapter differentiates network sharing from a situation in which a single network operator deploys a fixed or mobile network and then is required to provide open access to third parties. Although open access technically involves a sharing of infrastructure, it is not the same business relationship as a joint venture or other arrangement among multiple operators to deploy a new network.

Infrastructure sharing creates a new and different market dynamic. It can change market structures.

It is a shift from granting access to sharing costs and risks. It involves industry cooperation rather than heavy-handed regulatory oversight. It focuses on dynamic efficiency being driven from the active layer and retail competition rather than in the passive layer. And the logic of network sharing and co-investment will only improve over time, as the costs of passive infrastructure deployment (construction materials, labour, land, etc.) increase while the costs of active infrastructure decline.

Governments around the world are encouraging sharing arrangements. For example, as a component of its Digital Agenda, the EU Commission has specifically endorsed fixed network sharing, stating: "To foster the deployment of NGA and to encourage market investment in open and competitive markets, the Commission will adopt a NGA Recommendation based on the principles that co-investments and risk-sharing mechanisms should be promoted"[1].

2.2.1 Network sharing in the mobile sector

In the mobile sector, the main advantages of network sharing to governments are:

- **Provision of services in higher-cost areas**: By reducing costs and sharing demand risks, network sharing encourages mobile operators to provide services in the higher-cost, low-ARPU areas where the business case for building a new network does not stack up.

- **Planning and environmental efficiencies**: Avoiding duplicate infrastructure, through sharing, is often important for planning and environmental reasons. Tall towers are an eyesore, and communities are resisting a proliferation of new, above-ground infrastructure. There may also be limited capacity or planning restrictions on roof-top sites in urban areas.

- **Consumer benefits**: As a result of sharing, there may be lower overall costs for individual operators. Combined with a competitive retail market, this should lead to price reductions and better value for money for consumers.

2.2.2 Network sharing in the fixed sector

In the fixed sector, governments will see some advantages equivalent to those in the mobile market, but there are other attractive features, as well:

- **New sources of investment**: Co-investment arrangements enable or facilitate funding from new sources such as utilities, local governments or infrastructure funds – for example, the sharing between telecommunication companies and utilities in Switzerland. These non-traditional players benefit from partnering with operators (and vice versa). Non-traditional players usually have access to financing, valuable existing infrastructure or other assets they can bring to the table. Operators, for their part, can contribute skills, capabilities, infrastructure and capital.

- **Industry co-operation**: Co-investment is a "big tent" approach, in which industry players negotiate and co-operate in deployment and operation of the shared infrastructure. In the absence of anti-competitive concerns, a consensus-based outcome is usually superior to a regulated outcome.

- **Lessening of market power**: To the extent that an incumbent operator is a party to the co-investment arrangement, it can result in a lessening of market power, with a corresponding reduction in regulatory burdens for the regulator and for industry.

2.2.3 Third party access

Governments will often prefer, and sometimes require, open-access arrangements as part of network sharing or co-investment agreements. However, governments should consider a nuanced approach to this issue. If sharing operators are willing to assume potentially substantial construction risks and demand risks to invest in new broadband infrastructure, then a case can be made for governments to take a broader view of open-access mandates. Section 2.4.3 discusses regulatory certainty as a key prerequisite for encouraging network sharing and co-investment.

2.2.4 Comparison with single operator deployment

It can be debated whether co-investment models are superior to deployment by a single network operator that receives government incentives. If the single network operator is required to provide open access to other operators on a non-discriminatory basis, at cost-oriented prices, then co-investment alternatives may not be materially better. After all, It is likely to be easier to implement a bilateral arrangement between the government and a single network operator (usually the incumbent in the fixed sector), for a speedy network roll-out.

On the other hand, the burden to regulate the incumbent operator will persist and may even intensify with the single operator model. If the single operator participates in the downstream retail market, there will still be an incentive to engage in discriminatory behaviour favouring the operator's retail activities. All of this suggests that a sharing arrangement is more likely to lead to a reduced regulatory burden as compared to a single network operator model.

2.3 The development of network sharing models

This section explains how network-sharing arrangements developed and evolved in both the mobile and fixed-service sectors.

2.3.1 Evolution in the mobile sector

Commercial network-sharing arrangements have been prevalent in the mobile sector, both in developed and emerging markets. These arrangements mainly developed voluntarily between mobile operators, with only fairly light-touch encouragement from governments. Today, approximately 15 per cent of mobile operators engage in some type of network sharing.

Mobile network sharing is commonplace when powerful competitive pressures make it necessary for operators to reduce costs. This usually arises in mobile markets where there are four or more network-based competitors. In these markets, there has been substantial passive sharing and increasingly active sharing, including through the use of third parties such as tower companies or "towercos".

Sweden was one of the earliest countries to take up mobile network sharing and it appears that these arrangements have been enduring (see Box 2.1).

Australia was also one of the earliest countries to adopt mobile sharing arrangements. For various reasons, however, these arrangements did not survive for very long (see Box 2.2).

Most of the cost savings from network sharing (up to two-thirds) can be captured by sharing passive infrastructure. The cost savings from sharing active infrastructure are not as great, but they are still sizeable – delivering approximately 20-30 per cent cost savings for mobile networks. An approximation of cost savings from different types of mobile infrastructure sharing is shown in Figure 2.1.

The pressure to share mobile network infrastructure is heightened by the explosion in consumer and business demand for data. Data is a lower-margin business compared with earlier voice and messaging services. At the same time, the cost of running inefficient legacy networks is greater when dealing with high data volumes. New LTE networks, which are optimized for carrying huge volumes of data, involve major new investments by operators.

"Green-field" situations that require entirely new networks are generally considered to be easier and more suitable for sharing. This is one reason why network-sharing deals are more frequent in emerging markets than in developed ones. Although there is some sharing of existing assets, LTE is a more green-field opportunity, and this boosts the chances of a successful LTE network-sharing deal.

Box 2.1: Mobile Infrastructure Sharing in Sweden

3G mania swept through Sweden in 2000, with the result that TeliaSonera, the incumbent operator, failed to win a 3G licence[2]. It quickly sought an extraordinary network-sharing deal with Tele2, which resulted in Tele2 transferring its 3G licence to a 50/50 joint venture vehicle between the two companies called Svenska UMTS-Nat AB (SUNAB).

As well as owning the spectrum, SUNAB took full ownership of the W-CDMA network, including parts of the core network. The joint venture enabled each sharing operator to launch retail services and otherwise operate independently of the other. Each party bought wholesale capacity from SUNAB, acting essentially as a separate MVNO utilizing the joint network. Capacity charges were the same for both operators.

The Swedish regulatory framework positively supported these sharing arrangements. The 3G licences permitted network-sharing in areas covering up to 70 per cent of the population (the remaining 30 per cent – in practice, the urban areas – was to be covered independently).

At about the same time, in 2001, a 50/50 3G joint venture called 3GIS was created between 3 and Telenor in Sweden. Management and operation of 3GIS has been outsourced to Nokia Siemens Networks[3]. In 2009, Telenor and Tele2 formed a 50/50 joint venture, (dubbed Net4Mobility) to deploy an LTE network[4]. Net4Mobility participated in spectrum auctions and acquired 800 MHz and 1.8 GHz spectrum licences[5]. The same supplier structure used in SUNAB was carried over to Net4Mobility.

Box 2.2: Australia: Going their Separate Ways

Australia's four network operators paired up in two W-CDMA network-sharing joint ventures in 2004. But after three years, each of the operators began building their own 3G networks[6].

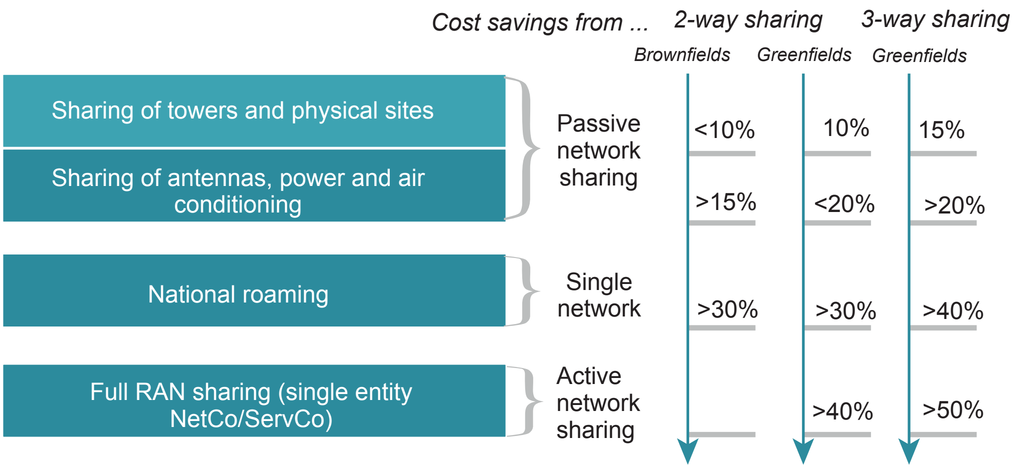
In 2003, prior to its network-sharing venture, Hutchison had a first-mover advantage in the W-CDMA (2.1 GHz) market in Australia's urban centres. But it gave up that advantage by entering into a 50/50 network sharing deal with Telstra in 2004 known as 3GIS Pty Ltd. In exchange for a 50 per cent ownership of the joint venture, Telstra paid AUD 450 million to Hutchison. 3GIS Australia involved a RAN share and a partly shared core, as well as shared frequencies. The venture was intended to last until 2017, when the 3G licences were to expire.

Telstra launched its W-CDMA services over 3GIS in 2005, but shortly after made the strategic decision to deploy a new W-CDMA network of its own (NextG) using 850 MHz spectrum that originally was used in its 2G CDMA network. Telstra launched NextG in 2006, meaning it was actually providing W-CDMA services over two separate networks. With its lower frequencies, NextG had much greater coverage than with 3GIS. Then, without much fanfare, 3GIS was closed down in 2012.

Meanwhile, just weeks after the 3GIS joint venture was launched in 2004, Vodafone and Optus decided to share a new W-CDMA (2.1 GHz) network, which was to be built from scratch. It was a RAN sharing (using MORAN), with each operator using its own spectrum and its own core network, meaning it was not as integrated as the 3GIS Australia joint venture.

Around 2007, both Vodafone and Optus began to build their own 3G networks using both 2.1 GHz spectrum and the 900 MHz bands that had become available for W-CDMA. Vodafone subsequently switched partners, merging with Hutchison to form VHA.

Figure 2.1: A cost-savings comparison of different types of sharing



Source: GSM Association and Vodafone Group

Box 2.3: Fixed Network Co-Investment Examples

Netherlands: In an example of a commercially driven co-investment arrangement, the Dutch incumbent operator KPN co-invested with Reggefiber to deploy FTTH connectivity to 2 million homes. The initial arrangement was for KPN to pay 41 per cent, with Reggefiber funding 59 per cent of the deployment cost[7]. But in November 2014, KPN acquired 100 per cent of Reggefiber, effectively ending the co-investment arrangement[8].

Singapore: Singapore's OpenNet is an example of how a government incentive was used to effectively require a co-investment strategy. Singapore's policy objective was to introduce a structurally separate entity at the passive layer, so it forbade the fixed incumbent from having a controlling stake in that entity[9]. As a post-script, the co-investment arrangements were unwound in 2014, when all of the OpenNet shareholders, including the incumbent, sold their interests to NetLink Trust, which was set up with the incumbent operator as the beneficiary[10].

Portugal: Vodafone Portugal and Optimus entered into a long-term cooperation agreement calling for each operator to build next-generation access networks independently (mainly in the Lisbon and Porto areas). The agreement spelled out conditions granting each operator access to the other's networks[11].

France: In France, the regulator has mandated network sharing for in-building wiring. This has led operators to grant a passive access to other operators at the concentration point[12]. Under the French model, one operator signs a contract with the building owner and becomes the main operator within the building. This operator is in charge of constructing and maintaining the networks and offering passive access to the other operators, either through a dedicated or shared fibre line. Access is granted through a long-term (24- or 30-year) cooperation agreement.

2.3.2 Network sharing in the fixed sector

Co-investment in fixed markets occurs relatively infrequently compared to mobile network sharing. It is especially rare to see co-investment agreements for fixed infrastructure without some pressure or incentive by a government.

The other main example of fixed-service co-investment has been when non-incumbent competitors have agreed to co-invest in a new network without involving the incumbent. These agreements, however, face the risk that the incumbent will cherry-pick prime customers and otherwise compete aggressively wherever the alternative network is being deployed. In fact, the very threat of that strategy being used may deter competitors from co-investing in the first place.

In some markets, regulators have mandated network sharing in fixed networks. Planning and environmental regulations can also drive network sharing/co-investment by reducing the amount of passive infrastructure that can be built. This will increasingly be the case in urban areas for tower structures – but also potentially for underground deployment, as well.

2.4 Obstacles to Network Sharing

Reasons why there is not more network sharing and co-investment

Despite the apparent cost reductions and other benefits of network sharing and co-investment, it's worth considering why they don't happen more often and why many of them don't seem to last. The commercial dynamics of sharing are complex, and governments looking to encourage or provide incentives for sharing arrangements need to keep in mind the various obstacles, which are explored in the following sub-sections.

2.4.1 Loss of independence

By definition, a sharing arrangement means an operator will no longer have full control over network strategy and investment. A fully independent network operator can dictate the direction of its network development, roll-out strategies and vendor choices. Network sharing involves ceding some of this control, in return for the benefits that are available. This sometimes manifests itself in concern that the sharing partner (who is also a competitor) will stymie new competitive developments in the shared network that the other operator wishes to make. For a sharing deal to succeed, the operators must reach agreement on where full independence needs to be maintained, where agreement is required with the sharing partner, and where operational control may be ceded.

Concerns over loss of independence mean that neutral or independent oversight is critically important in network-sharing transactions. This is one reason why parties often create new, separate joint ventures. There also may be benefits to bringing in third-party involvement – for example, either a third investor or an outsourced management company. The success of the towerco model is partly due to the neutrality that an unrelated third-party management company can provide. Neutral or independent governance means that a subset of decisions may be entrusted to the joint venture or independent manager without requiring negotiation between the sharing parties. The need to reach agreement with the other operator over investment and deployment issues is likely to consume time and generate disputes that may threaten the success of the venture.

2.4.2 Partner selection

Having a compatible sharing partner will alleviate some of these concerns. The selection of a compatible partner involves considering whether the prospective partner has the same strategies for network deployment and investment. This is particularly the case with mobile network sharing. When two mobile operators have similar networks, neither party is likely to have a material advantage over the other in entering into the arrangement. If a large operator and a new market entrant are considering a network sharing deal, however, there can be real difficulties in reaching agreement on key issues such as valuation and allocation of benefits.

2.4.3 Difficulty in reaching agreement

It is never easy to reach agreement on a network-sharing deal with a competitor, due to the healthy distrust that each management team has of the other. Shareholder support can be important in getting a sharing deal across the line, including incentives for management to put in place and then implement the arrangement.

A network sharing deal will often involve transferring existing assets into a joint venture structure (or to a third party) and decommissioning some sites. Disagreement over asset valuations in such cases is one of the main reasons why non-green-field network-sharing deals do not proceed. Negotiators also need to resolve transfer pricing issues and service levels for ongoing services, as well as vendor strategy.

This includes the role of third-party vendors – which vendors will perform which functions (e.g., maintenance, repair, field services), etc. Although it will be difficult to exit a network-sharing agreement, exit provisions also need to be agreed.

2.4.4 Incumbent resistance

In the fixed sector, which is devoid of the intense infrastructure-based competition that characterizes the mobile market, incumbents can be reluctant to depart from the status quo or to consider novel co-investment options – particularly options involving any loss of control.

2.5 Ways governments can encourage or incentivise network sharing and co-investment

To date, governments have generally adopted a light touch in encouraging network sharing and co-investment. Some countries have mandated network sharing, but there have been few examples of governments actively incentivizing network sharing or co-investment. This section addresses what governments can do to *actively* promote network sharing and co-investment.

2.5.1 Government co-venturing

Governments can play a significant role in fostering co-investment by co-venturing with private-sector operators. This is one of the most important steps that a government can take to encourage broadband deployment, particularly in green-field network development. Governments have very valuable assets and infrastructure that, if made available, can speed up and potentially reduce the cost of broadband deployment. Governments can contribute assets, access to utility infrastructure or rights-of-way, among other things.

It is not essential for governments to enter into ventures with private sector operators, but it is a key option. An auction could be used to determine private sector participation and the valuation of government contribution could, for example, be set at replacement cost using modern equivalent assets. Alternatively, government assets could be leased to a co-investment entity, rather than the government participating at an equity level.

Governments can pursue participation by public utilities in the roll-out of next-generation access networks. Co-investments are already happening between public utilities and private operators in European countries such as France, Germany and Switzerland. In Switzerland, the co-investment arrangements reportedly have increased competition in the market as well as facilitating deployment of next-generation access networks[13]. Interestingly, in regions of Switzerland where public utilities have not participated, the incumbent operator hasn't shown the same level of investment activity.

Co-investment between a utility and a private-sector operator avoids some of the obstacles referred to in the previous section concerning negotiating agreements between competitors. Loss of independence could still be a concern for private-sector operators, but arrangements with utilities may permit operators a greater level of control over key network decisions than might be the case in a pure sharing arrangement between private operators.

Moreover, utilities may not be the only public-sector entities getting involved in such ventures. Road or railway entities can be key partners

Box 2.4: Utility Participation in a Joint Venture in Ireland

In 2014, the Irish electricity utility ESB entered into a 50/50, incorporated joint venture with Vodafone to build and operate a wholesale-only, open-access, fibre-to-the-building (FTTB) network in certain parts of Ireland. The joint venture entity will deploy fibre to homes and businesses using ESB's existing overhead and underground infrastructure, in return for a fee from the joint venture. In turn, the joint venture will provide a wholesale, *virtual unbundled local access* (VULA) product to retail operators, as well as a higher quality, point-to-point service suitable for mobile backhaul and business customers[14].

for private-sector operators looking to roll out new broadband networks. In emerging markets, where there is often a policy priority to push out electricity, road and rail networks into more rural areas, there can be a particular synergy with telecommunication operators seeking to build out infrastructure in the same areas.

2.5.2 Use of spectrum licensing

The dynamics are different in the mobile sector. Here, a lighter regulatory touch may be all that is required from the government to encourage network sharing. One of the most potent means available to governments is setting 4G spectrum licensing conditions. Spectrum is in high demand and, through licence conditions, governments can facilitate sharing. Licence conditions are not without costs, of course, because they may potentially reduce the governments' proceeds from auctions or other licensing fees.

One approach to promoting sharing is to require each licensee to provide nationwide coverage while allowing network sharing. This can create a strong incentive for licensees to share, particularly in higher-cost, low-ARPU areas. Alternatively, the licence conditions may require each licensee to build a network in its defined geographic licensing area, while allowing sharing or roaming in other areas.

2.5.3 Regulatory certainty

As noted earlier in this chapter, the question of whether co-investment arrangements should be subject to open access by third parties is a subtle one. On the one hand, open-access policies are usually thought to promote competition, but this has been true normally in the case of existing networks with long-sunk costs. When it comes to new investments, threatening to impose stringent open-access requirements may discourage operators from investing at all.

Governments can address this risk by providing regulatory certainty for co-investing entities. Regulators could, for example, clarify that access pricing can take into account the build and demand risks at the time of investment. One of the major concerns of investors in new broadband networks is that, if they build a network and it is a success, they will be forced to provide access on terms that don't recognize those risks. Other possible approaches include:

- providing long-term regulatory commitments, such as the Australian regulator's acceptance of NBN Co.'s 27-year special access undertaking[15], which provided a high degree of certainty for NBN;
- applying a utility-style regulatory asset base approach to the new broadband network, providing a revenue ceiling for the new entity;
- providing the shared network operators with a period of exclusivity before requiring them to offer open access, which may be seen as a fair trade-off for operators' assumption of risk and commitment to invest and deploy the new networks; and
- enabling the shared network operators to access the network at the passive layer, with third parties being entitled to access only at the active layer – but otherwise on a non-discriminatory basis.

Regulators may be more prepared to provide regulatory certainty to a joint venture in which no single operator is dominant rather than to a single owner with a new network. At the very least, governments should review the regulatory environment to ensure there are no unintended roadblocks that may undercut the potential for commercial network sharing and co-investment arrangements.

2.5.4 Mandated network sharing

Some regulators (e.g., Colombia, France and the United States) have mandated mobile network sharing or roaming obligations, often on a temporary basis and usually for the purpose of matching existing coverage rather than increasing coverage. There may be merit in these mandates in brown-field environments, but there are doubts about whether mandated network sharing is likely to be productive in encouraging green-field investment.

Again, this may come down to regulatory certainty. As long as the investing operator building a new network in a green-field environment is certain

Box 2.5: Tower Limits in Indonesia

In Indonesia, the sector Ministry has restricted the construction of new towers in the vicinity of existing towers in order to persuade operators to undertake infrastructure sharing. Under the terms of the regulation, a new tower can be constructed only if, for some reason, the existing tower cannot be shared[16]. The regulation provides a guideline for the construction and development of joint mobile towers. Owners of mobile towers are required to give non-discriminatory access to other telecommunication operators. The tower owners also must give information about their tower's capacity to potential access-seekers in a transparent manner.

about the rules governing mandated network sharing, then there can be little objection as long as they have the choice of whether or not to invest. But regulators should take care not to stymie investment in the first place by instituting overly rigorous requirements for mandated sharing.

2.5.5 Grants and subsidies

There have been some successful examples of government use of modest grants and subsidies to overcome stiff resistance to network sharing, particularly from incumbent fixed-service operators. Box 2.3 showed how Singapore used a financial incentive to promote a co-investment arrangement. In New Zealand, the government used a grant to provide an incentive to deploy an ultra-fast, FTTH network, inducing the fixed incumbent to structurally separate in order to participate in the initiative.

2.6 Potential downsides to network sharing

While there are potential downsides for governments of network sharing and co-investment, they are generally regarded as fairly manageable, in the right circumstances. This section explores those downsides and how to cope with them.

2.6.1 Reduction in competitive intensity

Reduction in competitive intensity can be a concern with network sharing, as competition will be confined to the services layer, rather than to both services and infrastructure layers. The common stance regulators have taken is that, at least for passive network sharing in the mobile sector, there is little competitive benefit in expanding pure coverage, so infrastructure sharing is unlikely to harm competition. Similarly, with most types of active network sharing in the mobile sector, the impact on competition is fairly benign as long as sharing operators have the ability to differentiate their services from one another. However, once a sharing arrangement has achieved integration at the infrastructure layer, it's very difficult to unwind, leading to a potentially permanent reduction in infrastructure competition.

2.6.2 Potential for collusive dealing and information sharing

There is also the potential for collusive dealing between sharing operators. Regulators need to carefully evaluate this issue and engage in ongoing monitoring. Sharing of commercially sensitive information among co-investors is a concern, as well, but it may be an inevitable feature of sharing arrangements. Appropriately structured procedures and protocols can be implemented to reduce the competitive impact of such information sharing.

2.6.3 Reduced options for services-based competitors

A reduction in infrastructure competition may lead to reduced options and more limited capacity being available for service-based competitors such as MVNOs. This may not be such an issue where sharing operators retain their competitive independence – the motivations for entering into MVNO-type arrangements should not change in these cases. Limited capacity can be an issue, but most sharing or co-investment arrangements can be expected to provide sufficient capacity for sharing operators and potential service-based competitors. If this remains a concern for regulators, they could require (and provide upfront regulatory certainty about) provisioning of sufficient capacity for services-based competitors.

2.6.4 Service-Level Agreement (SLA) performance

In the absence of infrastructure competition to drive efficiencies, there will be a requirement for SLA-driven performance to incentivize the shared network to perform. Depending on the effectiveness of the SLA regime, this can be effective in ensuring efficient operation of the network.

Commercial models for sharing

The main commercial models for network sharing and co-investment are joint ventures and long-term co-operation agreements, often known as *IRU access.*

Joint ventures – Joint ventures are a common structure adopted for network sharing (usually incorporated, sometimes unincorporated). Normally, the joint venture owns, operates and maintains the joint network. In these circumstances, sharing operators contribute financial and human resources to the joint venture, although some aspects may be outsourced to third-party vendors. Sometimes it is only an asset-owning joint venture, or the JV may acquire assets from one or both sharing partners to form the basis of the new network.

Indefeasible rights of use (IRUs) – IRUs have been a feature of the telecommunication industry for many years, particularly for long-haul transmission and undersea cables. Legally, IRUs give a party the right to use network infrastructure (such as dark fibre), a certain amount of capacity (including transmission), or a network facility (such as ducts) for most of the life of the asset. IRU arrangements are often valid for about 25-30 years and are normally non-renewable. As well as access to the main infrastructure, an IRU will usually also allow access to ancillary infrastructure, such as manholes and cabinets where duct access is provided, as well as colocation and access to splicing/junction nodes.

An IRU may be seen as a form of co-investment or network sharing. Seen as an up-front guarantee of access, the IRU effectively gives an operator a share of the infrastructure, which it shares with the grantor of the IRU and any other IRU holders. IRUs have been a particular feature of the French FTTH projects. They can also arise in mobile network sharing arrangements.

2.7 Alternatives to Network Sharing

What are the alternatives to network sharing/co-investment? This section explores other ways for governments to promote efficiency in deploying broadband infrastructure.

2.7.1 Geographic splitting

Geographic splitting allows one operator to simply provide wholesale network services to another operator – including national roaming or MVNO services – in return for the same services being provided to it in another geographic region. Operator A would build, own and operate the network in Region A, allowing Operator B to use its network there. In return, Operator A would get the same rights to use Operator B's network in Region B. This sort of arrangement can be applied in relation to fixed networks, as well as mobile ones. In Geneva, Switzerland, for example, the utility SIG operates an access network in the Geneva metro area, while Swisscom operates an access network in the centre city. Both SIG and Swisscom grant each other dark fibre access, allocating the roll-out cost 60 per cent to Swisscom and 40 per cent to SIG[17].

In the fixed network context, there are instances of one partner building the access or "last-mile" segment of a network, with another partner building the backhaul segment. In Switzerland, the utility usually builds the terminating segment (OTO-CP) and Swisscom builds the feeder and backhaul network (CP-ODF), providing collocation. The partners exchange IRUs to access each other's infrastructure[18].

2.7.2 Third-party outsourcing

Another alternative to network sharing is third-party outsourcing, in which the sharing operators pool their assets and outsource the management and operation of their shared network to a third-party manager. This can be an attractive arrangement, as it removes aspects of trust issues that can sometimes complicate joint ventures.

More commonly, arrangements for the management and operation of RAN, core and transmission networks are entered into with individual operators (about 25 per cent of operators have entered into these arrangements). Equipment vendors such as Alcatel-Lucent, Ericsson, Fujitsu, NEC, Nokia, Huawei and KT Corp provide various types of third-party outsourcing products that may be suitable in a network-sharing environment.

The involvement of a third party will reduce the savings available to the sharing parties and may result in SLA-driven control of that third party. Outsourcing to a third party also involves loss of competence within the operator's organization, which can have long-term implications.

2.8 Future applications of sharing and co-investment

This section explores some of the forward-looking applications of the network-sharing and co-investment model, such as for "smart cities" or dynamic spectrum sharing.

2.8.1 Smart city environments

Extensive and ubiquitous high-speed connectivity is a key enabler for the success of so-called smart cities. Telecommunication operators have the opportunity to provide connectivity solutions that will go beyond fixed and mobile broadband. They will include proximity connectivity using WiFi, NFC, Bluetooth, RFID and the like. There will also be a need for other progressive connectivity solutions.

Governments, operators, utilities and private entities will need to share and provide access to key infrastructure needed for the proliferation of smart city solutions, such as access to buildings, cabinets and light poles. Sensors and other smart components may need to be installed in strategic locations that are owned by multiple parties, and it may make sense to make those sensors and components available for use by many players in the smart city ecosystem.

It won't just be access to infrastructure that will need to be shared in smart cities. Data sharing and access will also play critical roles, and clear rules and even regulatory intervention may be needed. For example, in the context of a smart emergency services solution, energy utilities may need to share smart-grid data with emergency services agencies so that they can respond immediately – or even pre-emptively – to power outages or power-related emergencies on the basis of that data.

2.8.2 Virtualization of core network infrastructure

Telecommunication operators can be expected to increasingly use cloud-based infrastructure for their data centre, platform or application requirements. This is a form of sharing, as logical separation through virtualization will make it possible for core network infrastructure and functions to sit on physical infrastructure that is used by other parties, including other operators.

2.8.3 Dynamic spectrum sharing

Spectrum sharing is likely to feature increasingly in RAN and optical fibres (dynamic wavelength allocation). Traditionally, mobile network operators have been reluctant to consider spectrum pooling, or sharing of spectrum between operators, because they seek to maintain maximum flexibility to manage their networks. Also, frequency allocations are often not equal. India, for example, does permit some RAN spectrum sharing, but it is not permitted in many countries.

Up until now – and for the foreseeable future, realistically – governments allocate spectrum mainly on a dedicated basis. This has allowed operators to use higher-power equipment, with resulting wider coverage, while limiting interference. The exception has been unlicensed spectrum, which used by (among other things) Wi-Fi networks.

Dynamic spectrum access (DSA) technologies allow devices to use spectrum where it is not being used in a particular geographic area, or at a particular time. This way, multiple users can "share" access to the spectrum while minimizing interference to others. The best near-term opportunities for deploying spectrum sharing may be in those bands with substantial government uses. Some of these bands may be suitable for mobile broadband, but clearing these government users from the spectrum cannot be done in a reasonable timeframe. In Europe, the 2.3 GHz band is being considered for spectrum sharing between government and commercial users[19]. In the United States, the FCC is considering shared access to the 3.5 GHz band for use by small cells[20].

2.9 Learnings/recommendations

Achieving "further and faster" broadband coverage is a key issue for most governments around the world. One of the options available to governments is to encourage network sharing or co-investment, which will bring a range of benefits for governments. Little or no investment may be required from government to make it happen, and the results could include speedier deployment, cost savings passed on to consumers, and a reduced ongoing regulatory burden.

It is undoubtedly a challenge, however, for operators to create, implement and maintain a successful network sharing or co-investment arrangement. It is often difficult to explain clearly why potential sharing arrangements do not work out, and the parties are commonly loathe to detail in public the problems they encountered. Nevertheless, given all the benefits available to operators, it is somewhat surprising that sharing does not occur more frequently.

It is clearly more difficult to achieve co-investment in fixed networks, where there is less infrastructure competition than in mobile markets. This is an area where government incentives, including in-kind contributions, could bring about breakthroughs. There may be particular merit in governments (including through utilities) co-venturing with telecommunication operators to facilitate the rapid roll-out of fixed broadband networks.

Endnotes

[1] "Draft BEREC report on Co-investment and SMP in GA networks", BoR (11) 69 (BEREC 2011), page 12. Available from berec.europa.eu/files/news/bor11_69_coinvestmentnga.pdf.

[2] GSMA, "Mobile Infrastructure Sharing" (2012), page 41. Available from http://www.gsma.com/publicpolicy/wp-content/uploads/2012/09/Mobile-Infrastructure-sharing.pdf.

[3] Ibid.

[4] Telegeography, "Tele2 and Telenor Sweden launch LTE", 15 November 2010. Available from https://www.telegeography.com/products/commsupdate/articles/2010/11/15/tele2-and-telenor-sweden-launch-lte/index.html.

[5] Telegeography, "Telia, Tele2, Telenor win 1800MHz spectrum, Hi3G misses out", 14 October 2011. Available from https://www.telegeography.com/products/commsupdate/articles/2011/10/14/telia-tele2-telenor-win-1800mhz-spectrum-hi3g-misses-out/index.html.

[6] GSMA, page 43.

[7] KPN, "KPN announces next step in its commitment to Fiber-to-the-Home", 9 November 2011. Available from http://corporate.kpn.com/press/press-releases/kpn-announces-next-steps-in-its-commitment-to-fibertothehome.htm.

[8] Telegeography, "KPN to increase Reggefiber stake to 100%", 18 November 2014. Available from https://www.telegeography.com/products/commsupdate/articles/2014/11/18/kpn-to-increase-reggefiber-stake-to-100/index.html.

[9] ZDNet, "OpenNet wins Singapore NBN bid", September 28, 2008. Available from http://www.zdnet.com/article/opennet-wins-singapore-nbn-bid/.

[10] Rujun Shen, "Singtel wins conditional approval for ownership of fiber network", (Reuters) 21 November 2013. Available from http://www.reuters.com/article/2013/11/21/us-singtel-opennet-acquisition-idUSBRE9AK0O020131121.

[11] Telegeography, "Optimus, Vodafone agree to share fibre network", 20 December 2010. Available from https://www.telegeography.com/products/commsupdate/articles/2010/12/20/optimus-vodafone-agree-to-share-fibre-network/.

[12] Telegeography, "France Telecom-Orange, Bouygues ink deal on fibre development", 17 January 2010. Available from https://www.telegeography.com/products/commsupdate/articles/2012/01/17/france-telecom-orange-bouygues-ink-deal-on-fibre-deployment/.

[13] "Financing of the Roll-Out of Broadband Networks: Note by Switzerland", DAF/COMP/WP2/WD(2014)17 (OECD, 2014). Available from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=daf/comp/wp2/wd%282014%2917&doclanguage=en.

[14] Vodafone Ireland, "ESB and Vodafone to invest €450 million in 100% fibre broadband network across Ireland in European first", 2 July 2014. Available from http://www.vodafone.com/content/index/media/vodafone-group-releases/2014/esb-vodafone-ireland.html.

[15] Special Access Undertaking (NBN

[15] Co, 2013). Available from http://www.nbnco.com.au/sell-nbn-services/special-access-undertaking-sau.html.

[16] MoCI Regulation No.02/PER/M.KOMINFO/3/2008 regarding Guidelines on Construction and Utilization of Sharing Telecommunication Towers.

[17] OECD, page 8.

[18] BEREC, page 22.

[19] "Opinion on Licensed Shared Access", RSPG13-538 (EC RSPG, Brussels, 2013). Available from https://circabc.europa.eu/d/d/workspace/SpacesStore/3958ecef-c25e-4e4f-8e3b-469d1db6bc07/RSPG13-538_RSPG-Opinion-on-LSA%20.pdf; Webb Henderson, "Spectrum Sharing – it's on its way", 5 May 2014. Available from http://webbhenderson.blogspot.co.nz/2014/05/spectrum-sharing-its-on-its-way.html.

[20] John Leibovitz, "Breaking Down Barriers to Innovation in 3.5 GHz Band", *FCC*, 21 April 2015. Available from https://www.fcc.gov/blog/breaking-down-barriers-innovation-35-ghz-band.

3 Regulation and the Internet of Things

Author: Prof. Ian Brown, Oxford Internet Institute, University of Oxford, United Kingdom[1]

3.1 Introduction

Plummeting electronics and communication costs have set the stage for a rapid expansion of the Internet of Things (IoT). The billions of everyday physical items and appliances that now have sensors and network links will increasingly be able to remotely share data about themselves, their users and their environments. In the next decade, technology companies and consulting firms expect tens of billions of IoT devices to be deployed, with a total annual economic impact in the trillions of US dollars[2].

Companies manufacturing IoT devices are only one part of a broader ecosystem of organizations developing the IoT. The data created by interconnected devices can be shared via communication networks, stored on application platforms (including social media sites), and controlled by third-party applications. The information is then accessible from users' smart phones (which themselves contain an increasingly diverse range of sensors)[3].

This chapter examines the concepts, technologies, and societal changes influenced by the IoT and related technical developments. These include convergence, cloud services, data analytics, the proliferation of sensors, and the measuring and monitoring of people, machines and things. Seen as a whole, this constitutes a shift from human-to-human communications to machine-to-machine (M2M) and everything-to-everything communications.

The purpose of the chapter is to raise awareness among the ICT regulatory community of the changes caused by the advent of IoT. It will examine how this huge shift is impacting consumers, businesses, governments and overall society. The most important regulatory implications are in the areas of licensing, spectrum management, standards, competition, security and privacy.

3.2 Internet of Things concepts and deployment

The ITU-T's definition of the IoT calls it "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[4]." This refers to the network of remotely linked tags, sensors and *actuators* (motors and other mechanisms to cause an action within a device) that are increasingly being built into objects throughout the physical world, driven by an ongoing rapid drop in the cost of microchips, sensors and communication capacity.

Collectively (and with slightly different nuances and emphases) these technologies are also termed *ubiquitous/pervasive computing*, *cyber-physical systems*, *smart environments/spaces/cities* (shown in figure 3.2, and discussed in the next section), the *industrial Internet* (focusing on manufacturing processes), and *ambient intelligence*.

The term *Machine-to-Machine* (M2M) communications, meanwhile, is used to refer to communications directly between IoT devices, often via cellular networks. The mobile industry association GSMA predicts between 1 and 2 billion M2M connections by 2020[5]. This has regulatory implications for switching and roaming, as discussed later in the chapter.

In addition to the wide range of terminology, the IoT takes in and enables a very broad range of applications. A short list would describe more efficient agriculture, manufacturing, logistics, counterfeit detection, monitoring of people, stock, vehicles, equipment and infrastructure, along with the improved healthcare and traffic management discussed already in this chapter. Moreover, there are applications for retailing, product development and hydrocarbon exploration – and it doesn't stop there. The IoT also enables new business models, such as car and truck rental clubs, whose members can book and use vehicles parked around their neighbourhood almost on-demand. Or, the IoT can lead to "pay-as-you-drive" insurance based on precise driving patterns, behaviours, and risk factors.

The simplest IoT technology – passive *Radio Frequency Identification* (RFID) tagging – is already widespread in retail, transit ticketing and access control. *Near-Field Communication* (NFC) is now included in newer smart phones, enabling applications such as contactless payments (examples include Visa's payWave and Mastercard's PayPass standards). Specialized sensors and processors in smart phones, watches, bracelets and even clothing can collect, process and share data about individuals and their environments.

RFID and NFC only work at close range. M2M systems, however, can send information over cellular networks. Examples include electricity metre readings sent to energy companies and car airbag deployment notifications sent to emergency services. Literally hundreds of millions of M2M systems are being deployed around the world, as shown in Figure 3.3.

Many M2M devices use standard mobile *Subscriber Identity Modules* (SIMs) for identification and authentication. Unlike mobile phones, though, these devices often are located in diverse, unsupervised locations, where they are subject to wind, rain, large temperature changes, and vibration. To protect the SIMs-- and also to prevent theft – they often are attached permanently and securely to the M2M devices[6].

M2M communications are often periodic and uplink-intensive (especially if video is being streamed from cameras, sometimes in high definition). By contrast, many core and access communication networks currently are configured to support the downlink-heavy communications typical of Internet use[7].

In the ITU-T model, communication network providers are responsible for:

- access and integration of resources provided by other providers;

Figure 3.1: The Internet of Things, in a nutshell

The Internet of Things

What Is It?

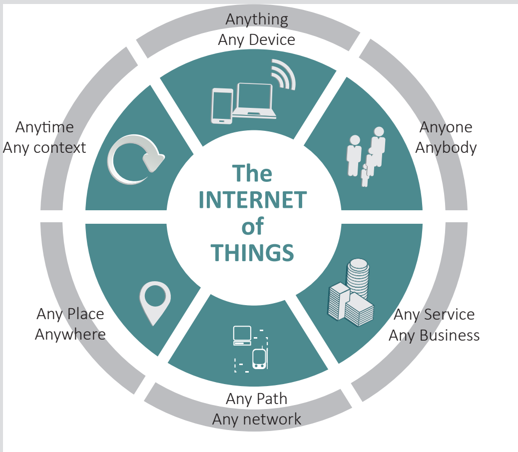
"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication" (ITU-T)

Who Makes It?

Device manufacturers, network operators, application platforms, software developers and (cloud-based) data analytics services providers

How Is It Accessed?

Connection of IoT devices via Wi-Fi, Bluetooth, mobile phone networks, specialized radio networks, global Internet



Main current areas of investment

- Smart cities
- Smart metering & grids
- Connected vehicles
- Healthcare

Main Impacts

- Monetary/economic impact: trillions of dollars annually within a decade
- Societal impact: Smart cities – infrastructure, transport and buildings – by improving efficiency and sustainability of a whole range of urban activities; smart power and water grids (smart meters)
- Individual impact: e.g. transport safety through "connected vehicles"; population health and wellbeing can be enhanced, enabling e.g. care at home

Challenges

- Cost needs to fall, reliability needs to improve
- Issues of connectivity, user interfaces and addressing
- Regulatory implications for licensing and spectrum management (access required to 300 MHz-3GHz but also NFC at 13 MHz or EHF bands, AM/FM bands in VHF range, Wi-Fi and 4G mobile networks), standards (interoperability e.g. ITU-T's initiative IoT-GSI), competition (e.g. impact on competitiveness of different markets, customer lock-in due to fixed SIMs in each device etc...), security and privacy ("by design" approach desirable)

Source: Author

Box 3.1: The Republic of Korea's Master Plan for Building the Internet of Things

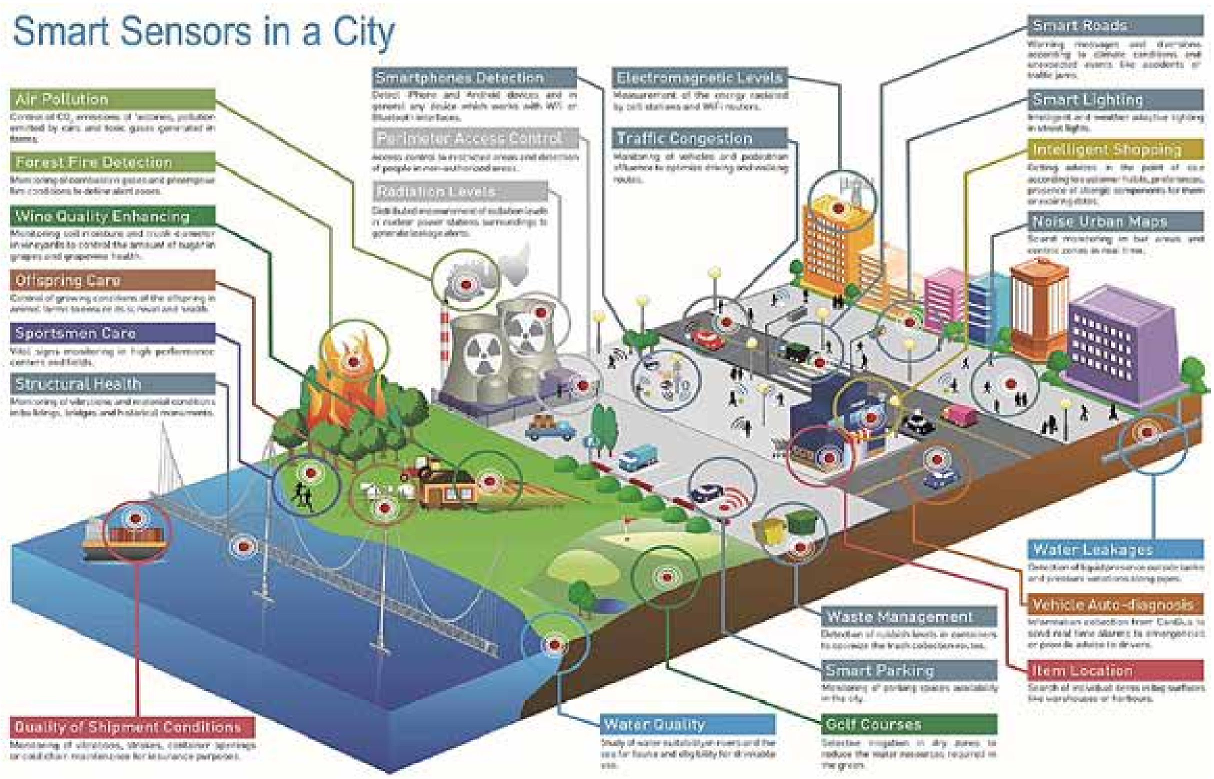
The government of the Republic of Korea has developed a master plan to use IoT to improve public administration, to increase industrial productivity, efficiency and added value, and to improve individuals' safety and quality of life. It sees the country as a potential global leader in IoT products and services, given Korea's top-class ICT infrastructure and manufacturing capacities.

The plan aims to increase the domestic IoT market fourteen-fold by 2020, with a 30 per cent increase in productivity and efficiency in companies adopting IoT. Because of the small domestic market, cooperation with global businesses is an important part of the strategy. Domestically, new software implementation in advanced manufacturing will enable growth of traditional industries and new software companies. The government will promote joint research and demonstration projects with the Trans-Eurasia Information Network, which connects 19 Asian and 34 European countries.

Information-sharing is one key focus of the plan. The government aims to establish an information-sharing and analysis framework with governments in the United States, Japan and the European Union. The country's IoT Innovation Centre will provide a test-bed environment for security functions and promote security and privacy-by-design in IoT systems.

Source: Ministry of Science, ICT and Future Planning, Republic of Korea, 8 May 2014.

Figure 3.2: Smart cities



Source: Libelium.

- support and control of the IoT capabilities infrastructure; and
- offering IoT capabilities, including network capabilities and resources, to other providers[8].

Depending on the requirements of specific applications, there may be some degree of business integration between device, network, platform and application providers.

3.3 Development trends and application areas

The IoT sector has grown, sometimes unevenly, over the last 15 years[9]. Hardware developments have made these technologies available at the low cost, size and energy-consumption necessary. But many applications have been incremental improvements to existing business processes, developed by existing companies that can afford the required investments. At this stage, businesses specializing in IoT services may be needed to spur further growth and market-entry, along with further cost reductions, enabling the radical disruption of existing industries that many technology companies and consulting firms predict[10].

With near-field communication, smart phones can be a universal platform for individuals to interact with IoT objects, removing one of the main cost barriers to growth. Payment, ticketing, vouchers, and customer loyalty applications will become cheaper and easier to manage, allowing much greater sophistication in pricing, marketing, product management and analysis. One company has forecast that approximately USD 36.05 billion in NFC payments will be made worldwide in 2017, although this figure has declined by more than 40 per cent from previous forecasts, due to slower than expected growth[11].

3.3.1 Uses of IoT in manufacturing and logistics

So far, IoT technology has been used mostly in logistics and inventory management. Retailers can track products from the factory, through distribution networks – updating orders and routes in real time – to warehouses and into stores. IoT allows automatic replacement of stock when it is

Figure 3.3: Machine-to-machine (M2M) services

Source: Beecham Research.

taken off the shelves, as well as replacing stolen or damaged products. Customer payment systems can be tied-in automatically, signalling the need to re-stock whenever sales reach a trigger point. Managers can monitor customer flows within each store, allowing changes in store layout.

Manufacturers can embed sensors throughout their production processes, enabling much more precise control and enhancing both efficiency and quality, while significantly lowering waste, energy use, the risk of accidents and product damage[12]. Similar techniques can be used through the whole lifecycle of equipment, vehicles, and the built environment, allowing for just-in-time repairs that minimize downtime and repair costs. And farmers can use IoT systems to monitor soil and crop conditions, precisely adjusting planting and pesticide use to maximize yields and minimize environmental impacts, while enabling better food traceability[13].

Businesses likely will continue to be the biggest users of IoT technologies. One analysis estimated that by 2019, enterprises will be using 40 per cent – 9.1 billion – of all of the deployed inter-connected devices, with the highest-spending industry sectors being manufacturing, transportation and warehousing, and information[14]. Another analysis predicted that by 2020 there will be 2.1 billion machine-to-machine device connections, with two-thirds of these in utilities industries, one-fifth in security applications, and smaller numbers in the automotive and transport sectors, healthcare, government, retail and financial services. Applications will spread from developed to emerging economies, from limited commercial markets to a broad spread of consumer applications[15].

3.3.2 Consumer applications

Many of the IoT applications coming online now have direct consumer impacts. For example, shoppers can take advantage of RFID tags, using smart phones to access online information about products from the manufacturer or the retailer, or from independent reviewers and even friends,

Box 3.2: China's large-scale M2M deployment

China is the world's largest M2M market, with some 50 million connections by 2014. China Mobile, China Telecom and China Unicom are all developing large M2M businesses. They have support from the Chinese government, which has identified IoT as an "emerging strategic industry" and is investing USD 603 billion in the M2M ecosystem in the decade leading up to 2020.

The energy (including smart grid) and transportation (including freight tracking) sectors have been early adopters, with increasing demand in the automotive, smart city, healthcare, education and retail sectors. China Unicom connects BMW cars to the BMW ConnectedDrive service, providing embedded SIMs and hosting call and data centres. China Telecom's Mega Eye business supports 800,000 video cameras in 20 different industry sectors. The growth of 4G networks will further support applications such as video surveillance and in-car multimedia services.

Hundreds of Chinese cities are deploying smart-city technologies. These include intelligent traffic management systems that adjust signals to ease congestion and help drivers find parking spaces, as well as systems to monitor pollution and noise sources. Mobile healthcare and education services are being developed to reach patients and schools in remote areas. And there are enhanced emergency-response and home health-monitoring applications, with Unicom developing smart ambulances that can send patients' data ahead to the destination hospital. China Mobile has developed M2M applications to help farmers remotely manage greenhouses and irrigation systems and to assist forest managers in monitoring fire hazards.

Source: GSMA, How China is set for global M2M Leadership, June 2014.

allowing them to compare prices and reviews among different products and stores.

Customers also can access discounts and advertisements tailored to their known preferences or demographics. Interestingly, some of the information gathered may be on-scene, using camera image analysis and signals from wireless devices such as smart phones. The use of such data gathered about individuals, of course, raises significant questions about privacy, as discussed below.

Figure 3.4 and Table 3.1 show the areas where IoT usage is currently receiving the most attention from key ICT stakeholders, identifying possible future developments. At the macro level, two of the areas of greatest IoT development and investment are:

- smart cities – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities; and
- smart power and water grids – which will provide similar improvements, efficiencies and cost reductions for key utility infrastructures.

Closer to the individual, "connected vehicles" with hundreds of separate sensors will be safer, more reliable, and able to participate in sophisticated congestion-management systems. Health and social services, which increasingly challenge governments around the world as populations grow older, could be significantly enhanced with IoT-based systems used by individuals, care-givers, primary care doctors and hospitals.

3.4 Challenges and opportunities

Governments and the private sector are continuing to fund significant levels of IoT research and development in areas such as modularity, reliability, flexibility, robustness and scalability[33]. But the basic capabilities needed for many applications are already well understood and are becoming available through smart phones and other standard platforms[34]. These devices will also defuse some of the cost issues that have held back growth, although cost and reliability remain issues for large-scale systems, as does connectivity.

IoT technical standards have evolved from a variety of different applications and stakeholders with different aims and requirements, and more work is needed to integrate different standards frameworks. A significant opportunity is the greater use of open data platforms and *Application Programming Interfaces* (APIs), which can enable greater innovation in IoT systems. Table 3.2 provides an overview of the various challenges and opportunities discussed in this section, and identifies best practices looking forward.

3.4.1 Cost and reliability

For IoT to become a truly ubiquitous technology, the costs of tags, sensors and communication systems need to fall to a level where they are a very small fraction of the total costs of the objects to which they are attached, with readers also made easily available. Even the cheapest (printed) tags, known as *Quick Response (QR) codes*, have not yet generated high responses in consumer-targeted marketing campaigns. This is partly because specific software may need to be installed to read the codes – something the users don't want to do-- and users need to position phone cameras so the code is in focus and can be read accurately[36]. In response, companies are developing more aesthetically attractive codes that can include images, such as the "dot-less visual codes" being used by Chinese e-commerce giant Alibaba to combat counterfeits[37].

High reliability levels also become important in large-scale systems that can include thousands of sensors, devices and readers. During trials of the most important RFID standard, EPC Global, retailers Walmart and Tesco had difficulties in detecting tags due to product orientation and the blocking effects of nearby materials[38].

Figure 3.4: Popular IoT uses

	INDIVIDUAL	COMMUNITY	SOCIETY
IoT	Smartphones Wearables	Connected Cars Health devices Smart homes	Smart Cities Smart Grids
Egs.	GPS, Fitbits Visa PayWave Mastercard Paypass Employee passes	Intelligent Transport Systems Event Data Recorders (EDRs) Blood pressure monitors, remote burglar/heating systems	Smart metering Smart water meters Traffic monitoring
Data	Mobile money Fitness data, GPS location-based data	Speed, distance, airbag, crash locations/alerts, Heart rate, blood pressure, Diet, remote heating data	Electricity/water consumption and billing Traffic flow data
Intended Audience	Individual person, Immediate friends/family, banks, employers	GP, health authorities, health and car insurance, police, wider friends social networks	Authorities/regulators Utility companies Other citizens

Source: ITU.

Powered tags (relying on batteries) must minimize energy consumption, a requirement that is prompting further research and development of energy-scavenging, low-energy protocols and algorithms[39]. One example is Bluetooth Low Energy (BLE), which is supported by new smart phones. BLE tags advertise their presence by sending out a message every second, and they can operate for up to one year using a lithium coin cell battery. They currently cost less than USD 5, a price that is likely to drop even further[40]. Another example is EnOcean, an ultra-low-power wireless standard that supports energy-harvesting wireless technology for smart buildings. Such sensors can be powered entirely using motion, light or temperature differences[41].

Table 3.1: Overview of some key applications to-date

Areas of applications	Drivers	Examples	Possible development
Smart cities	• Continued urban growth, which presents quality-of-life & safety issues. By 2023, there are likely to be 30 cities with populations of over 20 million. Over half of these will be in India, China, Russia and Latin America[16]. • Large public and private-sector investments, such as Saudi Arabia's USD 70 billion "economic cities" project[17]; South Africa's USD 7.4 billion smart city in Modderfontein[18]; Masdar in Abu Dhabi; Accra in Ghana; Yachay in Ecuador; plans for over 100 smart cities in India; and a USD 8 billon smart city technology investment fund in China[19].	• Monitoring and maintaining critical infrastructure such as roads, bridges, tunnels, railways, ports, communications, water and power[20]. Doha, São Paulo, and Beijing have used water pipe and pump monitoring sensors to reduce leaks by 40-50 per cent[21]. • Networked traffic signals dynamically manage traffic movement across a city in response to measured and predicted changes in congestion and accidents. • Congestion charging systems reduce vehicle commuting time by 10-20 per cent[22].	• Continued deployment of sensors and metering systems will enable greater city coverage and new applications, as will greater availability of communications capacity & distributed, intelligent network analytics. These will include platforms for small/medium-sized businesses and software developer interaction[23].
Smart meters and grids	• Environmental sustainability – to increase energy efficiency and reduce power consumption, especially at times of peak demand. • To enable consumers to understand and reduce energy usage and switch to suppliers offering tariffs closer to their needs. • To integrate variable renewable and home energy sources into the larger power grid. • Fraud and theft can be remotely detected and meters disabled.	• An estimated 1.1 billion smart meters will be installed by 2022[24]: 80 million in Japan, hundreds of millions in EU, and 150 million in India[25]. • Smart water meters can enable leak detection. Installations in the United States, Malta, India and Canada found an average reduction of water usage of 5-10 per cent[26].	• Could save 33 per cent of the total cost of constructing a grid using traditional methods[27]. • Will reduce downtime and waste through better load balancing and voltage regulation, as well as faster detection and diagnosis of faults.

Table 3.1: Overview of some key applications to-date (end)

Areas of applications	Drivers	Examples	Possible development
Connected vehicles	• Faster and more targeted emergency response to accidents. • To enable drivers to monitor their cars' operational condition and performance, allowing them to improve vehicle reliability and fuel efficiency, as well as keep track of journeys. • Pay-as-you-drive insurance. • Stolen cars can be remotely tracked and disabled. • Autonomous driving.	• Worldwide, the top 14 car manufacturers, which account for 80 per cent of the global market, all have connected vehicle strategies[28]. • The EU is close to agreeing on requirements for all new cars and small trucks to feature an "eCall" system from April 2018[29].	• By 2020, an estimated 90 per cent of cars sold in the United States will have an Internet connection-- an increase of more than 80 per cent over 2013[30]. • Cars will share congestion and road problem data, enabling other cars to avoid traffic snags and to notify repair and emergency services of road maintenance problems. • More efficient insurance markets, particularly for under-served groups such as young adults.
Healthcare	• The need to improve efficiency and care in existing healthcare settings. • The need to enable much greater use of remote tele-medicine services, with greater patient comfort and lower cost. • Letting individuals monitor own health, improving well-being by better managing conditions such as diabetes, encouraging exercise and healthy eating, diagnosing medical conditions more quickly, and encouraging compliance with treatment regimes.	• Patients with chronic conditions can monitor and report warning signs, using devices such as connected insulin pumps and blood-pressure cuffs. • The annual cost of chronic conditions could reach USD 15.5 trillion by 2025, with remote monitoring potentially reducing this figure by 10-20 per cent[31].	• "Quantified self" systems will measure heart rate, breathing, temperature, sleep and brainwaves, and apps will help users record diet and alcohol intake – increasingly collected and linked via users' smart phones or other wireless devices[32]. • Patients will share data to reassure care-givers and relatives, share advice in online patient forums, and volunteer information to medical researchers.

The immature and fragmented state of markets for many IoT services increases development and operational costs. A Korean government review found limited application of IoT e-government pilot projects and a low rate of introduction of IoT services in small and medium-sized enterprises (SMEs). To encourage new businesses to develop and use IoT applications, some governments (including those of Rep. of Korea, China, India and the United Kingdom) are supporting the development of IoT business incubators and innovation centres, which include platforms and testbeds for start-ups and SMEs. These can increase market entry, leading to increased competition and reduced costs[42].

In addition to these issues, there is a coordination challenge. Put simply, IoT infrastructure must be deployed in a given industry sector before applications can be deployed to bring the concrete benefits of IoT to that sector. Large investments may be needed to finance the development of infrastructure and applications, but this creates a risk that speculative investments will not be repaid as quickly as expected[43].

The most ambitious smart city projects, such as India's project to create 100 smart cities, are spending hundreds of millions of dollars to build more liveable and sustainable communities[44]. To

Table 3.2: Overview of challenges and opportunities

What?	Why?	What is done today/best practice	Possible way forward
Cost and reliability	• Most tags and readers are not yet cheap enough to be ubiquitous. • Limited consumer use of QR codes, and perceived negative impact on aesthetics. • Costs can be too high for adoption by SMEs. • Very high reliability requirements in large-scale systems with thousands of tags and devices. • Power sources are challenging for cheap but long-life sensors. • Large investments are needed to take full advantage of "smart city" systems.	• Ongoing development and deployment of cheaper, more efficient and reliable hardware and protocols. • Innovation centres to stimulate market entry and competition. • Public-private partnerships and cooperation between municipalities, businesses and contractors to reduce costs and share resources.	• Standardized functions in smart phones could interact with tags and sensors, including via web browsers. • Greater attention to aesthetics of tags, such as dot-less visual codes[35]. • Further R&D in areas such as energy scavenging, low-energy protocols and algorithms, and high-reliability systems.
Connectivity	• Application-specific networks and components increase costs and reduce the opportunities to improve security and reliability. • Mobile data networks still are adapting to support large M2M systems.	• Data from disparate systems are integrated at hubs, including cloud services. • Many mobile networks have M2M business units and networks with specialized business processes, including charging and system integration to support large systems. • Increased 4G deployment gives high throughput, low latency option for M2M.	• Additional IoT support in next-generation cellular networks. • R&D for more common middleware and APIs, and further standardization of protocols for resource-constrained systems.
Open data and APIs	• IoT data is often held in "silos" that are difficult to integrate without time-consuming data discovery and licensing. • IoT platforms can be industry- and vendor-specific, limiting opportunities for SMEs and start-ups to participate.	• City and country initiatives can provide for sharing of information by individuals and organizations under non-proprietary, open-source licences.	• Further work is needed to encourage cataloguing and contributions to open datasets. National and local government authorities are in a key position to do this and could collaborate through Open Government Partnership.

Table 3.2: Overview of challenges and opportunities (end)

What?	Why?	What is done today/best practice	Possible way forward
Standards (from the ITU and other organisations)	• Technical standards have evolved for different applications and stakeholders, making them less coherent. • Smaller national markets may lack scale to support development of local IoT solutions, unless they are built on international standards. • Specific software often is needed for each system, increasing user load. • Premature standardization can constrain innovation, but partial or late standardization can create industry coordination problems and fragmented technology options.	• ITU has a Global Standards Initiative to develop IoT standards and provide an "umbrella" for other standards organizations. • Wider-focus IoT and application-specific standards groups and frameworks.	• Further cooperation is needed between key standards bodies such as ITU, IEEE, IETF, IoT-specific standards organizations, and industry groups such as GSMA. • Governments can encourage further standardization through participation in standards bodies (already prioritized in China, Korea and India), as well as through R&D funding and procurement policies. • Development of common user interface mechanisms, especially via web browsers.

create the city-wide infrastructure needed for smart cities takes a strong commitment from local governments and other authorities, as well as large investments and strong partnerships between municipalities, businesses and contractors. Laying new fibre-optic cables to increase the communication bandwidth available for smart city applications, for example, can be done more cheaply if contractors take advantage of shared infrastructure (such as road trenches and utility tunnels) coordinated by a local authority.

This can be particularly effective when a smart city is built on a green-field site. The ITU-T focus group on smart, sustainable cities has developed specifications for multi-service infrastructure in such new-development areas. One example it provides is the new Indian city Lavasa, where a single company has been appointed to establish, maintain, and grant rights to assets such as dark fibre, rights-of-way, duct space, and towers on a lease/rent/sale basis[45]. In existing cities, system deployment is likely to be on an incremental basis.

3.4.2 Connectivity

For IoT system designers, there is a choice between centralized, cloud-based functionality and more distributed applications, where some data is stored and processed on or near the sensors. Centralized systems allow a small number of powerful computers to manage large numbers of cheap devices – although those devices must have a network interface that can connect to the Internet or to mobile phone networks. This centralized configuration has advantages when large amounts of sensor data must be processed.

In a more distributed system, devices can send data to smart phones or other, nearby computing devices over a local radio protocol such as Bluetooth. These local devices can process data before sharing it further across a global network. This increases system responsiveness to a local user, and it can provide more data privacy protection – which is especially valuable for sensitive information such as health data[46].

Some radio protocols (such as Ultra-Narrow Band) can provide longer-range coverage, which can be useful for smart city applications such as streetlight management, video surveillance and environmental monitoring. Using application-specific networks, though, can increase costs and reduce the opportunity to improve security and reliability when compared with multi-purpose networks[47]. Where mobile phone network coverage is available, 2G and 3G networks can be used for most IoT applications. The increasing coverage of 4G cellular networks, meanwhile, provides a high-throughput and low-latency option for higher-value IoT applications such as video surveillance.

The development of 5G cellular networks, expected to be deployed in the early 2020s, will provide considerable benefits for IoT applications, especially high-bandwidth ones such as video sharing. It will bring significant improvements in wireless communications, using smart radios and spectrum-sharing with 1,000 times higher spectral efficiency than current standards. 5G will support cooperative relays and femtocells, enabling low-power sensors to communicate farther while reducing the possibility of interference between communicating devices. It will include specific features to support device-to-device communication (such as traffic offloading) and explicit support for IoT/M2M systems[48].

The industry association GSMA identifies sub-1ms latency and greater than 1 gigabit per second (Gbit/s) bandwidth as defining features of 5G. Many of the other 5G goals can be met gradually using existing protocols. Meanwhile, autonomous driving, augmented-reality and virtual-reality systems, and tactile Internet interfaces are the main technologies today that would require such low latency and high throughput. These could be used in gaming, telemedicine and manufacturing[49].

5G likely will also support *Software Defined Networking*, allowing operators to run production and test networks over existing physical networks. These will feature separate IP control and data planes, increasing security while reducing expenditures. And it could provide support for running cloud computing in core networks, moving analytics closer to IoT edge devices[50]. SDN and femtocells are already being deployed in some 4G networks.

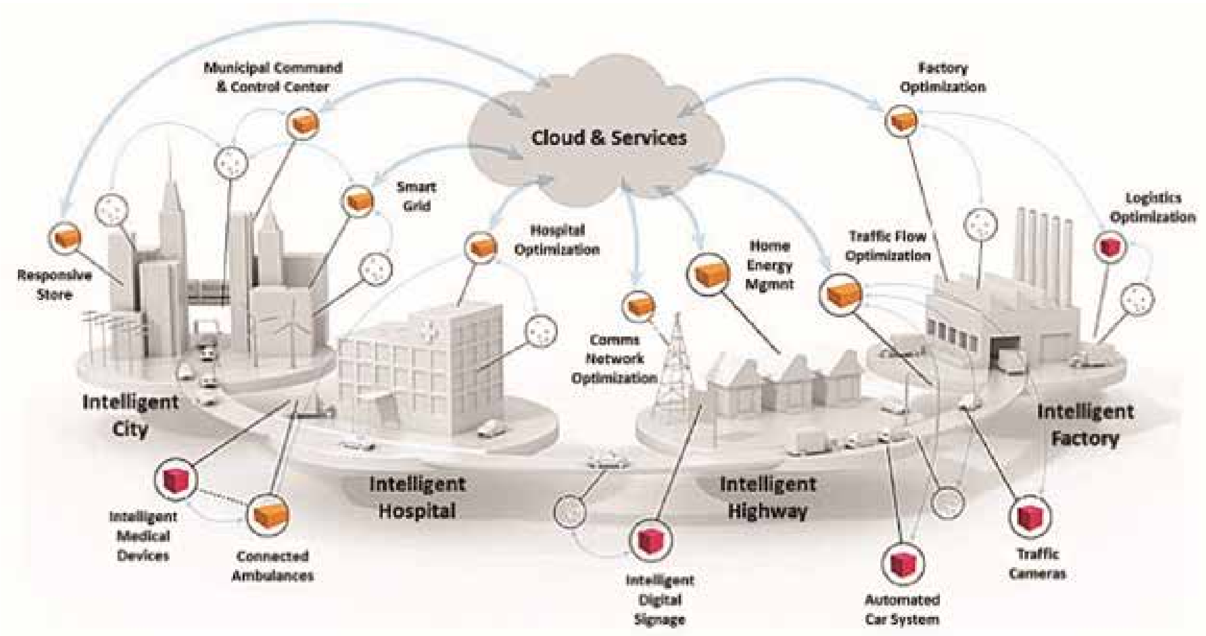
When a company such as a smart meter operator is managing thousands or millions of M2M devices via mobile data networks, they have very different requirements from a typical mobile telephone customer. They need comprehensive network status information to determine whether a non-communicating device or its network connection is faulty. They want a single subscription for the whole system, not on a per-device basis. And in many cases, the intended device lifetime will be much longer than the time during which individuals typically own a mobile phone – perhaps a decade or more. Replacing a device-- or even a communications module within it-- will require either an expensive service visit or a complicated process for customers that may cause faults. Not all mobile network operators can yet cope with these requirements, although many have set up business units specifically to address them[51].

IoT systems are built on fixed and wireless communications standards, but it can still be difficult to connect systems in different industry sectors or to reuse system components. The great heterogeneity in application programming interfaces and middleware (software components) makes it difficult to write applications that will run on different systems. So, users often have to rely on a single set of applications for a single set of IoT components. More standardization would enable more innovation, allowing information to flow between different industry sectors such as consumer electronics and automobiles. There is a need for interoperability, connectivity, access control, service discovery, and privacy services, all built on IoT-optimized protocols where necessary[52]. Greater configurability allows components to be used in a wider variety of systems, but it can increase complexity and price.

Because IoT applications have strongly heterogeneous requirements, there is a need to fit different communications protocols to different applications – for example, using IoT-specific protocols such as the *Constrained Access Protocol* (CoAP) in resource-constrained systems. Most applications will be built around Internet Protocol, except on very constrained devices. M2M devices can connect directly to other machines, but frequently there are gateways connecting IoT devices, which provide added-value services such as protocol conversion, filtering, caching, and back-end hubs – which can run on smart phones, gateways, or in the cloud (for global scale)[53].

Even if integration of infrastructure and networks can prove challenging between organizations – whether public or private-sector – data from

Figure 3.5: Intel's Intelligent Systems Framework



Source: Intel Corporation, Simplifying the Internet of Things: Intel® Intelligent Systems Framework, 2012.

disparate systems can still be integrated at data hubs, including cloud services[54]. Companies are building system frameworks to connect together disparate applications and networks via these cloud services. One example is shown in Figure 3.5:

Much of the value of IoT systems will come from integrating separate, proprietary silos, especially for large organizations with a broad range of partners. This will unfold in the same way that sharing technologies for personal computers (for example, operating systems and processors) enabled much greater levels of distributed innovation and consumer choice in the 1980s. Improved data-sharing also will allow the development of specialized data analysis providers that can increase the value of that data[55]. This does, however, depend on consumer trust in the security and privacy protection of the data (discussed further below).

3.4.3 Standards

To date, IoT technical standards have evolved from a variety of different applications and stakeholders with different aims and requirements[56]. A universal, uniform network of "things" is unlikely to develop in the medium term. Smart meters are unlikely to communicate directly with heart-rate monitors, or recipe planners. Some networks will use public infrastructure, while others will be entirely private. Some applications will have high bandwidth and interactivity requirements (such as video surveillance), while others may focus on transferring short bursts of information (such as smart meters). But with effective standards, these networks can be bridged.

Greater technical standardization can both reduce the barriers to entering IoT markets and increase economies of scale, helping suppliers to compete internationally. Without this, national markets may face the issues identified in a Korean government review, which reported that large businesses are developing IoT platforms but lack leadership in the global market. This, in turn, makes it difficult for local SMEs to enter the market and leaves them dependent on global suppliers[57]. Because of the strategic dimensions of IoT deployment for economic and industrial activities, states may have an incentive to seek more cooperation at the national and regional levels[58].

However, the diversity of IoT systems and users means that there is a limited constituency actively pushing for standardization[59]. Many of these users – for example, in the healthcare sector – do not have much experience working in communications standards bodies. Standards need to be carefully designed so they do not constrain innovation in still-young IoT markets. But partial or delayed standardization can complicate innovation, leading to industry coordination problems and fragmented technology options[60].

In an effort to deal with these issues, ITU-T has created a *Global Standards Initiative on Internet of Things* (IoT-GSI) to "promote. . .a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale," and to "act as an umbrella for IoT standards development worldwide." IoT-GSI works with specific ITU-T IoT groups (i.e., a joint coordination activity and the focus group on a machine-to-machine service layer), and the main ITU-T Study Groups (especially Study Groups 2, 3, 5, 9, 11, 13, 16 and 17)[61].

Other international communication standards bodies have ongoing IoT-related activities. The Institute of Electrical and Electronics Engineers (IEEE) considers IoT-related issues in a range of its communication standards, particularly 802.11 (Wi-Fi), 802.15 (Wireless Personal Area Networks), 802.16 (broadband wireless), 802.3 (Ethernet), and 1901.2 (power line networks). IEEE also is considering applications relating to the smart grid, energy, industrial, agricultural and mining sectors. It has created a draft standard (P2314) on an architectural framework for IoT.

The leading Internet communication standards body, the Internet Engineering Task Force (IETF), has considered IoT issues in the following working groups:

- 6Tish (IPv6 access and meshing over deterministic (scheduled) MAC),
- IPv6 (Internet Protocol version 6),
- 6LoWPAN (IPv6 over Low power WPAN),
- RPL (Routing Over Low power and Lossy networks),
- MPL (Multicast Protocol for Low power and Lossy Networks), and
- CoAP (Constrained Application Protocol)[62].

In addition, there are some IoT-specific standardisation groups. The OneM2M group brings together manufacturers, service providers, end-users, and regional standards bodies from North America, Europe and East Asia[63]. It has developed a suite of standards for M2M and other IoT applications, including a set of security solutions[64].

Another IoT-specific group is the Industrial Internet Consortium, which includes some of the largest companies developing IoT technologies, such as AT&T, Cisco Systems Inc., General Electric, IBM, and Intel. The consortium is developing use cases, reference architectures, and frameworks, and it aims to influence global standards processes[65]. A third example is the AllSeen Alliance, a consortium that is developing the open-source AllJoyn software and services framework. Members include consumer electronics companies such as Canon, Electrolux, LG, Panasonic and Sharp, as well as technology companies such as Microsoft and Qualcomm[66]. And the mobile industry association GSMA works with its members to drive M2M standardisation.

There are also IoT application-specific standards frameworks, such as the M/490 Smart Grid reference architecture, which can be reused in other IoT domains. This was created following a specific mandate from the European Commission to European standards organizations, principally ETSI, CEN and CENELEC. These bodies are able to create standards that can be referenced in EU regulations and directives, allowing policy-makers to incentivize the creation and use of specific technical standards[67]. Another incentive method is for governments to support the development of standards and products through grant funding and by prioritizing the use of such products in government-funded programmes. Without such incentives, large companies may find it more attractive to create their own, proprietary standards, which might act as market-entry barriers to limit competitors[68].

Many IoT systems will require very limited human interaction – for example, an on/off switch or a bus stop sign notifying passengers of the time until the next bus arrival. Requiring a separate smart phone app or other type of software to interact with such systems will be an unnecessary burden for users. One suggestion for standardizing the user interface to these systems is to have them locally broadcast a *Uniform Resource Indicator* (URI), which is currently most commonly used to identify web pages. Other smart devices within range can then list and interact with such devices, via a web browser or more specialized software[69].

3.4.4 Open platforms, data and APIs

One way to encourage much greater analysis and integration of IoT data is for individuals and organizations to share information under non-proprietary, open-source licences. Data becomes available for new applications without the need for time-consuming data discovery and licence negotiation.

One example is Amsterdam's Open Data programme, which has catalogued 438 datasets about the city[70]. Partners contributed to and analysed these datasets. For example, a sensor was designed to enable individuals to monitor and share pollution, noise and light intensity data from their own neighbourhoods. Amsterdam is also one of eight cities participating in a CityService Development Kit (CitySDK) project[71]. This lets programmers write software that can access data and shared IoT services via open APIs, such as services to improve transportation, report problems to the city council, and guide tourists around places of interest[72].

As part of the Amsterdam initiative, several "Living Labs" have been set up in communities to experiment with smart-city initiatives, identifying successful ideas so they can be implemented across the city. An example is in IJburg, where there are "projects like free Wi-Fi and a new fibre network, personalized television and transportation services, and a co-working space [to] allow residents to experiment and test city projects to improve healthcare, environment, and energy programs in the city.[73]"

Another example of the use of open source approaches is in the Korean government's IoT master plan. The government will collaborate with the private sector to develop an open IoT platform, and all ministries will be encouraged to collaborate with businesses across the entire country. This will stimulate an open IoT ecosystem, which is intended to improve interoperability, reduce costs through economies of scale and scope, and enable flexible responses to environmental changes. A test-bed for small- and medium-sized enterprises will reduce development costs and time-to-market, and will support collaboration between businesses in different areas. The ecosystem will prompt start-ups to turn ideas into businesses, using tools that include open-source software and hardware (circuit diagrams, board plans, and specifications required for hardware development) and DIY open labs.

3.5 Policy and regulatory implications and best practices

The deployment of IoT systems, and their potential impact on individuals and businesses, raises regulatory issues. Some are familiar to telecommunication regulators, such as licensing, spectrum management, standards and competition, while others are more often handled by other regulators, such as data-protection, privacy and security.

A 2013 European Commission consultation found diverse views on whether IoT-specific regulation is necessary. Industry respondents argued that state intervention would be unwise in this still-young sector, and that general rules such as the EU's forthcoming *Data Protection Regulation* will suffice. Privacy advocacy groups and academics responded that IoT-specific regulation *is* needed to build public confidence and ensure a competitive market[74].

Meanwhile, a staff report from the U.S. Federal Trade Commission (FTC) suggested that IoT-specific legislation would be "premature." Instead, it encouraged self-regulatory programs for IoT industry sectors to improve privacy and security practices. It also reiterated the FTC's previous call for "strong, flexible, and technology-neutral federal legislation" to strengthen its ability to enforce wider data security standards and require consumer notification following a security breach. The FTC also sought broad-based privacy legislation[75].

This section reviews actions taken by regulatory agencies to enable the development and adoption of IoT systems in a way that maximizes their societal benefit (see Table 3.3).

Box 3.3 describes one notable example: India's programme to develop 100 smart cities and highlights a number of policy and regulatory issues raised by the Telecom regulator, TRAI.

3.5.1 Licensing and spectrum management

Licensing and spectrum management are important issues for ensuring availability and capacity for IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. The protocols include short-range radio protocols such as ZigBee, Bluetooth and Wi-Fi, and mobile phone data networks. In more specialized applications, such as traffic infrastructure, there are longer-range radio protocols such as Ultra-Narrow Band (UNB).

To communicate with remote networks, IoT devices may send data via a gateway with a wired (PSTN, Ethernet, powerline or DSL) or wireless (2G, 3G, 4G/LTE or UNB) connection to the global Internet or a telephony network – or directly over one of these mediums[76]. For consumers, the gateway will often be a smart phone or home wireless router. Businesses will frequently use their existing corporate data networks.

Devices communicating over many kilometres need access to the 300 MHz to 3GHz spectrum range, while centimetre or millimetre, "contactless" transactions may use near-field communications at 13 MHz or in the EHF bands (as shown in Figure 3.6). Some IoT applications may also make use of AM/FM bands in the VHF range. Telecommunication companies are experimenting with "white space" spectrum to make more use of often-unused spectrum bands, while a US presidential commission has recommended the development of shared-space technology that

Table 3.3: Overview of policy and regulatory measures

What?	Why?	What is done today/best practice
Licensing and spectrum management	To ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.	Monitor availability of spectrum for short- and long-range IoT communications and backhaul network capacity, and encourage 4G deployment and use of small-cell technology.
Switching and roaming	Standard mobile telephony network SIMs and accounts are unsuitable for large M2M users, mobile devices, and fixed devices in areas of poor reception.	• Mobile network operators develop M2M-specific business units with appropriate billing and management. • Further development and deployment of embedded, remotely provisioned SIMs in M2M systems.
Addressing and numbering	A very large address space is needed for globally addressable things.	• Deployment of IPv6 by ISPs, public and private-sector organizations. • Use of IMSI for M2M applications.
Competition	• Some market configurations of IoT services could strengthen the positions of large firms and increase potential for consumer lock-in. • Limited user access to raw IoT data reduces ability to switch providers (and to understand privacy implications).	• Ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions. • Provide institutional mecha-nisms for ongoing review of laws and regulations for impact on IoT competitiveness.

Table 3.3: Overview of policy and regulatory measures (end)

What?	Why?	What is done today/best practice
Privacy and security	• Security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles. • Many IoT companies have little Internet security expertise. • IoT device resource and connectivity constraints make security and vulnerability patching more difficult. • Smart city vulnerabilities can be hard to fix and present significant safety issues (e.g. in traffic lights). • Innocuous sensor data can be linked together to create detailed individual profiles and used to infer sensitive personal information, such as medical disorders. This may lead to discrimination in employment, financial and healthcare services.	• Ensuring security and privacy from outset of IoT system design process. • Development of co-regulation by all stakeholders to protect security and privacy. • Further development of privacy and consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.

enables government, licensed commercial users, and unlicensed users to cooperatively make use of a large amount of spectrum[77].

The U.S. Federal Communications Commission's (FCC's) expert IoT working group predicts that IoT will add a significant capacity load to existing Wi-Fi and 4G mobile networks. Regulators will need to give continuing attention to the availability of spectrum for short-range IoT communications and the capacity of backhaul networks that connect IoT gateways to the Internet. They will also need to encourage the roll-out of small-cell network technology such as 5G. If these conditions are met, the working group does not expect that new spectrum will need to be explicitly allocated to IoT communications[78].

The FCC also is reviewing the use of spectrum above 25 GHz for 5G networks, and possibly the IoT[79]. The Korean government plans to secure up to 1 GHz of additional spectrum by 2023, and it will ensure that 5G is commercialised by 2020 to cope with the "exponential growth" it expects in IoT traffic[80].

Studies for the European Commission have suggested that a licence-exempt model is most effective for IoT development, since it avoids the need for contractual negotiations before devices are manufactured and used, allowing the production of large numbers of cheap devices[81]. A Korean government review found an increasing demand for unlicensed, low-power, long-distance communications to connect devices in remote areas[82].

3.5.2 Switching and roaming

Firms operating large networks of M2M devices via mobile telephony networks, with a fixed SIM in each device, may not find it easy to switch networks at the end of a contract. The same difficulty in switching would arise if a device roams into a different network area or, for some time

Box 3.3: India's smart cities programme

India is continuing its rapid pace of urbanization, and it expects urban areas to contribute almost 75 per cent of GDP within 15 years. To improve efficiency, employment opportunities and quality of life, the government has embarked on a programme to create 100 smart, sustainable cities (SSCs). The programme consists of 80 per cent public-private partnership assets and 20 per cent public-funded basic infrastructure.

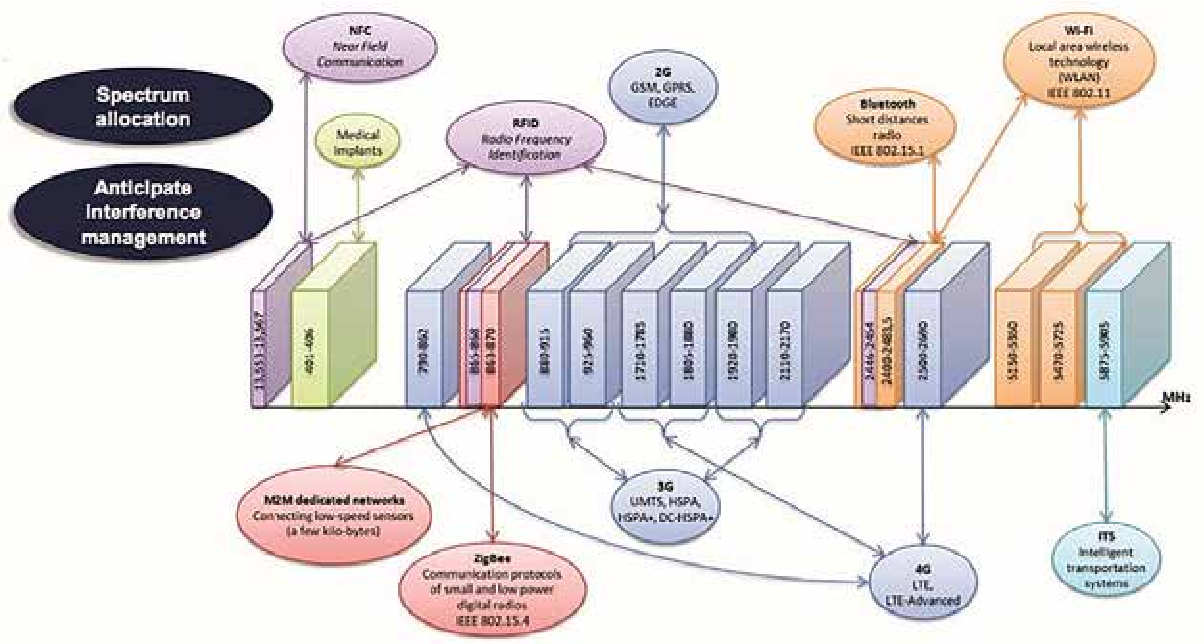
"Smart" services will include transport, building planning, water supply, solid waste management, sewerage and sanitation, electricity, Wi-Fi connectivity, and health care and education elements, with a total investment of USD 113 billion over 20 years. The services will be built around an Internet Protocol core network, a broadband access network, building sensing and analytical capabilities, and e-services websites for citizens. Shared infrastructure will include Wi-Fi in all public places and small-cell deployment for high speed/capacity links.

TRAI, India's telecoms regulator, has identified some policy and regulatory issues with the SSCs. These include how to encourage sharing of common assets and resources; ensuring spectrum availability for reasonable quality of service; avoiding electromagnetic frequency issues with large-scale wireless sensor deployment; identifying and developing open standards (especially to enable interoperability between sectors); data security; a numbering and addressing plan (including customer addresses for M2M devices); and security and lawful interception for M2M devices.

Source: Telecom Regulatory Authority of India, Smart Sustainable Cities- Policy and Regulatory Issues for India, 2015.

period, could get better service from a different provider. This means that roaming capability is important for devices that move between countries, and also for fixed location devices that may be used in an area of short or long periods of service unavailability – often indoors[83].

Figure 3.6: IoT spectrum



Source: Radio Spectrum Policy Group.

Some technical standardization work has been done to enable such roaming services, with some of Apple's latest iPads including SIMs that make it easier for users to switch between mobile networks. A leading SIM supplier, Gemalto, is supplying reprogrammable SIMs for smart watches. The first steps have been taken in this direction in the Netherlands, which in 2014 allowed SIMs to be issued by organizations other than mobile network operators, such as utilities and car companies[84]. The GSMA has developed standards for remote M2M device management. Mobile operators, including China Unicom and Telefónica, are supporting these standards[85].

Greater flexibility and competition would be possible if large IoT operators were able to act like mobile virtual network operators – not least because they could then have wholesale access to mobile networks[86]. The German network regulator, Bundesnetzagentur, consulted on the market for *International Mobile Subscriber Identifier*s (IMSIs) in late 2014[87]. An OECD analyst estimated that if German carmakers were able to issue their own SIMs and rent spare capacity on mobile networks, they could save USD 2.5 billion per year through lower prices and more flexible contracts[88]. The Belgian communications regulator BIPT is also consulting on the national number plan[89].

The European Conference of Postal and Telecommunications Administration's (CEPT's) Electronic Communications Committee has recommended that SIMs whose IMSI can be remotely updated should be implemented as soon as possible, and that CEPT countries consider greater flexibility in assigning *Mobile Network Codes* (MNCs) to IoT service providers. It has also encouraged the ITU-T to consider updating Recommendation E.212 to explicitly allow this flexibility, as well as to plan for the future use of MNCs to support a broader range of services[90]. These changes have been under consideration in ITU-T Study Group 2.

3.5.3 Addressing and numbering

IoT devices may have globally unique and routable communications addresses (requiring a very large protocol address space, such as that of IPv6). Or, they could have an address assigned by a gateway that allows limited inter-network connectivity. Or, they could make use of local networks only, to share data with-- and receive instructions from-- a nearby controller, such as a personal computer, smart phone, or specialized management device. In that case, a globally-unique address is not required.

Enabling peer-to-peer connections between devices can increase the reliability of communications, compared with requiring a large and complex global network. Peer-to-peer also matches the common use case of an individual discovering and interacting with nearby devices. But where devices must be globally reachable – most likely, via the Internet – a large address space is required to individually identify each device.

The number of unallocated addresses for the current version of the Internet Protocol (IPv4) is extremely limited, but the new version (IPv6) being rolled out by ISPs around the world has enough addresses for almost any conceivable number of devices[91]. The transition from IPv4 to IPv6 has taken longer than expected, and policy-makers may need to continue encouraging the transition in the medium term. The U.S. government, for example, has set up a Federal IPv6 Task Force to move all federal agencies from IPv4 to IPv6, also prompting the private sector to do the same. Many other countries have also set up IPv6 task forces to encourage national transitions.

For any IoT identification scheme, there will be trade-offs between performance, scalability, interoperability, efficiency, privacy, ease of authentication, reliability, flexibility, extendibility, and mobility support. Along with IPv6 addresses, the other main identification standards being developed are from the International Organization for Standards (ISO) and GS1, as well as ITU-T Recommendation E.212 for the use of IMSI for machine-to-machine communications[92]. The latter has the advantage of a well-developed authentication, payment and global roaming framework, operated by mobile telephony providers, with hardware security based on SIMs.

IoT applications using public networks, particularly mobile networks, will require ITU-T Recommendation E.164 (on telephone numbering plans) in the short-to-medium term and will provide a bridge to an all-IP solution in the longer term. The relevance of the E.164 telephone numbering plan for IoT applications was further noted by the European Communications Office in the context of M2M, where there is continued demand for telephone numbering resources for vending machines, smart meters, and in vehicle communications modules.

3.5.4 Competition

IoT technologies likely will have a range of impacts on the competitiveness of different markets. In the short term, firms adopting IoT systems will have better information on their business processes, enabling an increase in efficiency and more flexible responses to supply, processing and demand shocks. This could strengthen the market position of larger firms that have greater access to capital (to build their own IoT infrastructures) or brand loyalty. Some products will have network effects – i.e., the purchase of a product will increase its value to all other purchasers. A good example of this is telephone service, where a new customer can call and be called by all existing customers. With network effects, greater sales volumes can increase the likelihood of consumers being locked in to existing suppliers – especially if the supplier uses non-standard interfaces and sells complementary services[93].[94]

Over time, if IoT technology is adopted in ways that require high capital spending, increase firms' pricing power, or strengthen network effects, then early adopters can drive out competitors. Market structure will also be affected if large companies can build their own IoT systems but smaller companies have to subscribe to them or connect to networks operated by larger firms. If a "core" of large businesses adopts IoT, this could increase competition between them while reducing competition between core and peripheral firms. This could benefit consumers by turning quality-based competition into price competition. But if firms feel they have to adopt IoT simply because competitors have, this could lead to over-investment by incumbent firms and reduced market entry by firms not willing to make this investment[94].

The terms on which IoT service providers can access customers through the public Internet will have a significant impact on their ability to enter new markets. Baseline access could be protected by "network neutrality" rules that have been implemented by communications regulators in the United States, the EU, and elsewhere. IoT users with very high bandwidth or reliability requirements may be affected by neutrality rules that limit the ability of telecommunication companies to discriminate between Internet data from different sources. Such rules usually still allow telecommunication providers to offer such customers "specialized services" with specific speed or reliability guarantees[95]. The terms attached to such services, however, will be a key area of review for competition regulators[96].

In the longer term, an important factor affecting competitiveness of IoT systems is the extent to which end users can gain access to the raw data gathered and stored by components. Systems usually process sensor data extensively to make it more useful to users. While this makes systems more user-friendly, it reduces the users' ability to transfer data to different providers if a better service is offered (or to understand what inferences could be drawn about them from the data)[97]. It also makes it more difficult for end-users to combine systems from different providers. This could become a competition issue if a provider becomes dominant in one area and tries to extend that dominance into other areas by blocking interoperability with competitors' systems.

One example of regulatory activity to promote competition is in Rep. of Korea, where the government's Telecommunications Strategy Council has the responsibility to adapt existing laws and regulations to ensure a liberal and competitive industrial environment for IoT. Where the Council finds regulations that hinder ICT convergence, it can request related ministries to improve these regulations. For new products and services, attention will be given to prompt processing and interim licensing[98].

At this relatively early stage of IoT market development, it is not clear whether it will support "more than a relatively small number of very large players," as is the case with existing Internet markets such as search and advertising. Competition regulators will need to monitor whether *ex post* investigations of market abuse will be sufficient to foster a competitive market and rapid innovation, including the ability of start-ups and individual entrepreneurs to create new products and services[99].

3.5.5 Privacy and security

Privacy and security are two significant (and closely related) issues in large-scale IoT deployments. Technologies already are available to address some of the underlying technical issues (particularly in sensors), such as key diversification and reader authentication. But these can have a significant impact on device size, cost, functionality and interoperability[100].

Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users and using vulnerable devices to attack local networks and other devices. This is a particular issue when devices are used in private spaces, such as individuals' homes (e.g., baby monitors). IoT system operators and others with authorized access are also in a position to "collect, analyse, and act upon copious amounts of data from within traditionally private spaces.[101]"

Electronic attacks could also lead to physical threats, for example if carried out against medical devices like pacemakers and insulin pumps, or car engines and brakes. Information about building occupancy could be used by burglars to target unoccupied premises, while location-tracking data hacks might enable physical attacks against specific individuals[102].

If compromised IoT devices can connect to systems elsewhere on the Internet, it becomes a potential route for further attacks. One security company announced in 2014 that it had discovered hundreds of home devices – including smart refrigerators – sending unsolicited e-mail. While a further analysis found this to be inaccurate, it also warned of recently discovered malicious software targeting Linux-based IoT devices[103]. Another common security and privacy issue is the use of default passwords on devices, which users are not required to change when setting up a device. One website has claimed to find 73,000 webcams accessible over the Internet using a known default password[104].

IoT devices can be harder to secure than personal computers. Many companies building IoT devices do not have previous experience in dealing with Internet security issues in their products. IoT devices are often inexpensive and resource-constrained (notably on power and battery life), which puts strong pressure on security costs and requires additional hardware or software to deal with threats. Combined with the limited Internet connectivity of some devices, this may make it more difficult to develop and apply regular security patches when vulnerabilities are discovered. Instead, vendors or owners of the devices have to provide ongoing support[105]. But most IoT devices contain multipurpose computers and can be reprogrammed beyond their intended purpose – with limited mechanisms for users to monitor the devices. And devices frequently share operating systems, embedded chips and drivers, meaning that a single vulnerability can often be used to attack multiple devices[106].

In large IoT systems such as smart cities, IoT insecurity can create significant vulnerabilities. It can be extremely complex to address all of the interdependencies and links among public and private-sector systems. One 2014 threat assessment found some 200,000 vulnerable traffic control sensors in cities such as Washington DC, New York, Seattle, San Francisco, London, Lyon (France), and Melbourne. The assessment also found such technologies being developed and used in critical infrastructure without security testing. Plus, third-party security researchers often cannot gain access to devices to carry out their own tests, due to their expense and limits on sales to governments and specific companies[107].

Companies developing and operating IoT systems will need to conduct security testing and then consider how security vulnerabilities can be fixed during the systems' likely lifetimes. Where security flaws cause consumer harm, consumer protection agencies may be able to take action to require remedies and implementation of better security processes to reduce the risk of recurrence[108]. EU rules require organizations that process personal data from IoT systems to carry out security assessments and make use of relevant security certifications and standards[109]. And companies need to ensure that where they use external service providers to manage IoT devices and data, those providers also take reasonable security precautions.

To meet these security and privacy challenges, regulators have suggested that companies developing IoT devices should follow a security and "privacy by design" approach, building security and privacy functionality into the device from the outset of the development process, when it is much more likely to be effective[110]. That said, there is so far little evidence of market demand for privacy-friendly services – partly because of the difficulties individuals have in assessing and weighing up complex privacy risks. And while regulators have been discussing privacy by design for over a decade, the specifics of implementation have been limited so far[111].

Companies can undertake "privacy impact assessments" when designing IoT systems, to consider how different design options might affect privacy. This can also reduce the risk of expensive delays and system redesigns – as was extensively debated during the development of the Netherlands' smart meter programme[112].

A significant amount of work already has been done on security and privacy issues by policy-makers and regulators in the EU and United States. Under the *General Data Protection Regulation* being debated in the European Parliament and Council of Ministers, there will be stronger regulatory incentives for companies developing systems that process personal data to protect security and privacy by design. The U.S. FTC also suggests that companies follow a "defence in depth" approach. This involves considering security measures at several different points in their systems, such as using access-control measures and encrypting data even when users are making use of encrypted links to home Wi-Fi routers. Of course, this will not protect the data between the router and the company's servers, or if the router is badly configured[113].

Privacy is a particularly strong regulatory issue in European countries. A comprehensive legal framework includes the Council of Europe's *European Convention on Human Rights* and *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, as well as the *EU Charter of Fundamental Rights*. This framework has been influential in the development of comprehensive privacy laws now in force in more than 100 countries around the world[114].

The EU already has a very detailed legal framework regulating the public and private sector's use of personal data, with a general *Data Protection Directive* (95/46/EC) relevant to IoT device manufacturers, social media platforms and app developers that access IoT data, and an *e-Privacy Directive* (2002/58/EC) also relevant to IoT device manufacturers[115]. The European Commission has already sponsored a process to create an RFID privacy code of practice, developed collectively by industry and civil society and approved by the EU's data protection authorities[116].

These authorities have issued a detailed opinion on the IoT's implications for privacy protection. They note that the IoT produces high-volume flows of personal data that could present challenges to traditional data protection regulation. For example, individuals will not necessarily be aware when data is shared or able to review this data before it is sent to other parties, creating a risk of self-exposure and lack of control[117].

A further privacy issue is the amount of personal information that can be derived from seemingly innocuous sensor data, especially when it is combined with user profiles and data from other sources. As European privacy regulators noted, "Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.[118]" Smart meter data, for example, can be surprisingly revealing about individuals' day-to-day activities, down to the detail of which programmes are being watched on a television[119]. Researchers have found that smart phone sensor data can be used to infer information about users' personality types, demographics, and health factors such moods, stress levels, smoking habits, exercise levels and physical activity – even the onset of illnesses such as Parkinson's disease and bipolar disorder[120].

This kind of information has obvious positive applications, such as in pricing health insurance. But it can also be used for other decisions related to employment, credit and housing. This could lead to economic discrimination against individuals classified as poor credit or health risks, or potentially to "new forms of racial, gender, or other discrimination against those in protected classes, if Internet of Things data can be used as hidden proxies for such characteristics[121]."

To protect individuals' privacy, the FTC has suggested that notice and consent be required when personal data is collected by IoT applications outside the consumer's reasonable expectation. That expectation should be based on the

Table 3.4: Potential IoT regulatory measures

	Potential regulatory measures
Licensing and spectrum management	• Further experimentation with use of white-space and shared-space technology. • Encourage development of LTE-A and 5G networks, and review the need for IoT-specific spectrum.
Switching and roaming	• Global agreement on updated E.212 standards, making appropriate use of GSMA standards, and provision of Mobile Network Codes to IoT service providers.
Addressing and numbering	• Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption.
Competition	• Consider measures to increase interoperability through competition and consumer law, and give users a right to easy access to personal data. • Support global standardization and deployment of remotely provisioned SIMs for greater M2M competition.
Privacy and security	• R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems, particularly targeted towards start-ups and individual entrepreneurs that lack resources to easily develop this functionality. • Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn. • Greater use of privacy impact assessments by organizations building and configuring IoT systems. • Development of further guidance from global privacy regulators on application of the principles of data minimization and purpose limitation in IoT systems. • More cooperation between telecommunication and other regulators such as privacy/data protection agencies.

context of transactions and companies' existing relationships with consumers. Similarly, the EU data protection authorities have noted that IoT data collected for one purpose may be analysed and matched with other data, leading to a range of repurposing. Such data reuse should be compatible with the original purpose of collection and known to the user (this is known as "purpose limitation").

A range of mechanisms could be used to obtain consent, including:

- choices at point of sale or device setup;
- QR codes or barcodes on a device that could take a user to a website;
- privacy dashboards, for example in smart phones; and
- by learning from consumer behaviour, such as through privacy preferences set on other related devices[122].

Data minimization remains an important privacy-protective principle for consumer IoT devices, limiting the amount of personal data collected or retained, and hence reducing risks from data breaches and misuse. The FTC foresees more flexibility for IoT services in collecting data not initially required to provide a service, while under stricter European rules the EU data protection authorities "cannot share this analysis"[123].

Table 5 below identifies possible measures regulators can consider to foster development of the IoT.

3.6 Conclusions

While it is difficult to make precise forecasts about the global impact of the Internet of Things, analysts seem almost unanimous that it will be extremely significant – with tens of billions of devices deployed and trillions of dollars of annual impacts within the next decade. IoT technologies could make an important contribution to addressing global challenges such as improving public health and quality of life, moderating carbon emissions, and increasing the efficiency of a range of industries across developed and developing economies.

The pace of IoT deployment will partly depending on overcoming the hurdles currently facing the development of cheaper, more reliable and well-connected systems. Common networks, technical standards, system components, and infrastructure build-outs, as well as strong public-private partnerships, can reduce the costs of IoT systems. Open data and platforms can make it easier for new systems to be developed, especially by individual entrepreneurs, start-ups and SMEs. Innovation centres and incubators can further encourage new businesses to enter IoT markets, increasing competiveness. Governments can take steps to encourage national transitions to IPv6, updating all their own systems and providing incentives to private-sector providers to do so.

Large-scale IoT systems like smart cities and international logistics chains need very cheap sensors that can last for long periods of time without needing repairs or new power sources. They also need the bandwidth to share data, whether by infrequent bursts or streams of high-resolution video. M2M systems rely on continued growth in coverage of 3G and 4G networks and support for remotely provisioned, embedded SIMs for more reliable and competitive communications.

Telecommunication regulators can have the greatest impact by supporting the continued development and deployment of high-speed cellular networks and tracking the need for IoT-specific spectrum. Licensing and spectrum management are important to ensure that IoT systems develop cost-effectively and have the necessary bandwidth to communicate. Better services can be provided at a significantly lower cost by updating standards (such as the ITU's Recommendation E.212) and providing Mobile Network Codes to M2M service providers. In the long run, shared-space technology has the potential to offer much greater bandwidth for IoT and other communication services.

The widespread use of common technical standards will be the key to a low-cost, interoperable IoT. This can be encouraged by continued cooperation between standards bodies and government support for standards use and participation. National and local government authorities can stimulate the availability of open IoT datasets, platforms and components. Municipal governments are playing a key role in smart-city and open-data programmes. They may find it easier than national governments do to experiment with new technologies and policies suited to local conditions.

Some countries are taking a relatively hands-off approach to IoT regulation, focusing instead on promoting economic growth and innovation. For example, the Korean government has recently planned to reduce IoT (as well as e-commerce and Internet finance) regulation to support a dynamic ecosystem for future growth. It still plans to protect users, prevent abuse of market dominance and protect Internet networks, and it will decide on which restrictions to maintain through social consensus.[124] Other countries and regions – notably the European Union – are taking a more pro-active approach to protect social values, such as privacy, as the IoT develops, while still paying strong attention to the need to promote the economic benefits of the technology. Such strategic decisions are political ones that can only be taken by national governments while sharing evidence and best practices through international forums such as the ITU.

Regulators can play a role in encouraging the development and adoption of the IoT, while promoting efficient markets and the public interest. Competition regulators will need to monitor whether *ex post* investigations of abuse of dominant positions prove sufficient to foster a competitive market and rapid innovation. Regulators should give particular attention to IoT privacy and security issues, which are key to encouraging public trust and adoption of the technology. While many telecommunication regulators already have responsibility for network security, this is an area where they could do more by cooperating with national privacy and consumer protection regulators to encourage development of a trustworthy IoT.

Endnotes

1 The author is grateful for suggestions and comments on earlier drafts by Rudolf van der Berg , Pierre-Jean Benghozi, Mailyn Fidler, Simon Forge, Ben Hawes, Gilad Rosner, and ITU staff.

2 Gartner, *Forecast: The Internet of Things, Worldwide, 2013*, at https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide- See also J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson and A. Marrs. *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, May 2013, p.51. See also J. Bradley, J. Loucks, J. Macaulay and A. Noronha, Internet of Everything (IoE) Value Index, *Cisco White Paper*, February 2013, at http://www.cisco.com/web/about/ac79/docs/innov/IoE-Value_Index_White-Paper.pdf

3 International Telecommunication Union – Telecommunications Standardization Sector, *Overview of the Internet of things*, Recommendation ITU-T Y.2060, June 2012, s.I.1.

4 ITU-T Recommendation Y.2060, note 6, s.8.4.

5 GMSA, *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, p.10, at https://gsmaintelligence.com/research/2014/12/understanding-5g/451/

6 GMSA, note 8, pp.7-10.

7 Sasu Tarkoma, *Evolution of Internet based applications: Internet of Things, 5G and smart devices*, Helsinki public lecture, 3 April 2014, at http://livestream.com/ITstriimIT/Hetky-THkerho--IoT-5G/videos/46998469

8 ITU-T Recommendation Y.2060, note 6, s.I.1.2.

9 M. Malone. Did Wal-Mart love RFID to death? *Smart Planet*, 14 February 2012.

10 J. Esmeijer, A van Veenstra, T. Bakker, A. van Nunen, B. Kotterink and M. Ooms. *New sources of growth: Knowledge-based Capital*, OECD, 2015.

11 Gartner. *Forecast: Mobile Payment, Worldwide, 2013 Update*, 4 June 2013.

12 M. Chui, M. Löffler and R. Roberts. The Internet of Things. *McKinsey Quarterly*, March 2010, pp.1-9, at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things

13 Esmeijer et al., note 13.

14 Business Insider Intelligence Estimates, 22 Dec. 2014, at http://uk.businessinsider.com/the-enterprise-internet-of-things-market-2014-12

15 S. Hilton, *Imagine an M2M world with 2.1 billion connected things…* Analysys Mason, 27 January 2011.

16 Frost & Sullivan, *Mega Trends: Smart is the New Green*, at http://www.frost.com/prod/servlet/our-services-page.pag?mode=open &sid=230169625

17 Cisco Internet Business Solutions Group, *Saudi Arabia Invests US$70 Billion in Economic Cities Project*, July 2009, at https://www.cisco.com/web/about/ac79/docs/success/Saudi_Arabian_General_Investment_Authority_SAGIA_Engagement_Snapshot.pdf

18 NewsCentral Media, PCCW to connect Modderfontein 'smart city', *TechCentral*, 22 April 2014, at http://www.techcentral.co.za/pccw-to-connect-modderfontein-smart-city/47706/

19 Kieron Monks, Wire the desert: The next generation of smart cities, *CNN*, 18 December 2014, at http://edition.cnn.com/2014/12/18/business/smart-cities-next-generation/

20 Robert E. Hall, The Vision of a Smart City, *2nd Life Extension Technology Workshop*, Paris, 28 September 2000, p.2, at http://ntl.bts.gov/lib/14000/14800/14834/DE2001773961.pdf

21 Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.57.

22 Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.56.

23 S. Mitchell, N. Villa, M. Stewart-Weeks and A. Lange. *The Internet of Everything for Cities: Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, Cisco Systems, 2013.

24 Navigant Research, *The Installed Base of Smart Meters Will Surpass 1 Billion by 2022*, 11 November 2013, at http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022

25 Navigant Research, Smart Electric Meters, *Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts*, November 2013, at http://www.navigantresearch.com/research/smart-meters

26 Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.57.

27 GB Smart Grid: a race worth winning?: a report on the economic benefits of smart grid, Ernst & Young, 2012, https://www.smartgrid.gov/sites/default/files/doc/files/Smart_Grid_Race_Worth_Winning_Report_on_Economic_Benefits_201209.pdf

28 Verizon, The Internet of Things 2015, p.6, at http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf

29 European Parliament Internal Market and Consumer Protection Committee, *MEPs back deal with Council on automatic emergency call system for cars*, 4 December 2014.

30 FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World*, January 2015, p.1, at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

31 Manyika, Chui, Bughin, Dobbs, Bisson and Marrs, note 4, p.54.

32 Counting every moment, *The Economist*, 3 March 2012, at http://www.economist.com/node/21548493/

33 See e.g. the European Commission's Horizon 2020 research programme.

34 European Commission, *Internet of Things in 2020: Roadmap for the future,* 27 May 2008, p.13.

35 Davey Alba, Alibaba Reveals a New Kind of QR Code to Fight Counterfeits, *Wired*, 18 May 2015, at http://www.wired.com/2015/05/alibaba-reveals-retro-way-fight-counterfeits-qr-codes/

36 Roy Want, Bill N. Schilit, and Scott Jenson, Enabling the Internet of Things, *IEEE Computer*, Jan. 2015, p.31.

37 Alba, note 38.

38 Want, Schilit, and Jenson, note 39, p.30.

39 Ovidiu Vermesan and Peter Friess (eds.), *Internet of Things – From Research and Innovation to Market Deployment*, Aalborg: River Publishers, 2014, p.45.

40 Want, Schilit, and Jenson, note 39, p.32.

41 EnOcean Alliance, EnOcean Wireless Standard ISO/IEC 14543-3-10: The interoperable wireless standard for home and building automation, at https://www.enocean-alliance.org/en/enocean_standard/

42 Republic of Korea Ministry of Science, ICT and Future Planning, *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, 8 May 2014, p.6.

43 P.J. Benghozi, S. Bureau and F. Massit-Follea , *The Internet of Things : What challenges for Europe?*, Éditions MSH-collection praTICs, 2009.

44 Selena Larson, Inside Amsterdam's efforts to become a smart city, *The Kernel*, 4 January 2015, at http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11313/amsterdam-smart-city/

45 ITU-T Focus Group on Smart Sustainable Cities, Multi-service infrastructure for smart sustainable cities in new-development areas, FG-SSC, May 2015.

46 Want, Schilit, and Jenson, note 39, p.32.

47 Mitchell, Villa, Stewart-Weeks and Lange, note 26, p.12.

48 Tarkoma, note 10.

49 GMSA, note 9, pp.3-9.

50 Tarkoma, note 51

51 OECD, Machine-to-Machine Communications: Connecting Billions of Devices, *OECD Digital Economy Papers*, No. 192, OECD Publishing, 2012, pp.26-27, at http://dx.doi.org/10.1787/5k9gsh2gp043-en

52 Tarkoma, note 51.

53 Tarkoma, note 51.

54 Eric Openshaw, Craig Wigginton, John Hagel, John Seely Brown, Maggie Wooll and Preeta Banarjee, *The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices*, Deloitte, 2014, p.11, at http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-Iotecosystem.pdf

55 Openshaw, Wigginton, Hagel, Seely Brown, Wooll and Banarjee, note 57, p.10.

56 Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, p.48.

57 Republic of Korea, note 46, p.4.

58 Benghozi, Bureau and Massit-Follea, note 45.

59 Mailyn Fidler, *Ubiquity, Interrupted? A Comparison of European, Chinese, and U.S. Governance of the Internet of Things as an Emerging Technology*, First Annual Conference on Governance of Emerging Technologies, Phoenix, AZ, 2013.

60 G. Tassey, Standardization in technology-based markets. *Research Policy* 29(4)-29(5), 2000,

60 pp.587-602.

61 Internet of Things Global Standards Initiative, at http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

62 FCC TAC IoT Working Group, note 81.

63 T. Wachtel. *10th Meeting of the Internet of Things Expert Group*. Brussels, 14 November 2012.

64 oneM2M, *oneM2M Security Solutions*, Technical Specification, 1 August 2014, at http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf

65 Industrial Internet Consortium, *About Us*, at http://www.iiconsortium.org/about-us.htm

66 AllSeen Alliance, *An Open Source project building the framework for the Internet of Things (IoT)*, May 2015, at https://allseenalliance.org/sites/default/files/resources/intro_to_alliance_5.21.15.pdf

67 Vermesan and Friess, note 42, pp.151-152.

68 Want, Schilit, and Jenson, note 39, p.33.

69 Want, Schilit, and Jenson, note 39, pp.33-34.

70 http://www.amsterdamopendata.nl/home

71 http://www.citysdk.eu/about-the-project/

72 Larson, note 47.

73 Larson, note 47.

74 European Commission, *Conclusions of the Internet of Things public consultation*, 28 February 2013.

75 FTC Staff Report, note 33, pp.vii-viii.

76 ITU-T Recommendation Y.2060, note 6, s.8.4.

77 Dan Worth, Microsoft and BT to begin white space spectrum trials, *V3*, 2 October 2013, at http://www.v3.co.uk/v3-uk/news/2298124/microsoft-and-bt-to-begin-white-space-spectrum-trials

78 US Federal Communications Commission Technological Advisory Council Internet of Things Working Group, Spectrum: Initial Findings, *FCC TAC meeting update*, 10 June 2014, at http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting61014/TACmeetingslides6-10-14.pdf

[79] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, p.24.

[80] Republic of Korea Ministries of Science, ICT and Future Planning, note 60, p.11.

[81] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, p.24.

[82] Republic of Korea Ministries of Science, ICT and Future Planning, note 60, p.4.

[83] OECD, note 54, p.20.

[84] The endangered SIM card, *The Economist*, 20 November 2014, at http://www.economist.com/news/business/21633870-moves-reinvent-or-even-abolish-sim-card-could-have-big-consequences-endangered-sim?frsc=dg%7Ca&fsrc=scn/tw_app_ipad

[85] GSMA, *How China is set for global M2M Leadership*, June 2014, at http://www.gsma.com/newsroom/wp-content/uploads/2014/06/china-report.pdf

[86] OECD, note 54, pp.30-31.

[87] Bundesnetzagentur, *Marktbefragung zu einem zukünftigen Nummernplan für Internationale Kennungen für Mobile Teilnehmer (International Mobile Subscriber Identity, IMSI)*, Mitteilung Nr. 819/2014, Amtsblatt Nr. 15/2014, at http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Technische%20Nummern/IMSI/Mitteilung819_2014.pdf?__blob=publicationFile&v=2

[88] The Economist, note 89.

[89] Belgisch Instituut Voor Postdiensten En Telecommunicatie, *Raadpleging Op Vraag Van De Raad Van Het Bipt Van 25 November 2014 Met Betrekking Tot De Herziening Van Het Beleid Inzake Het Beheer Van Het Nummerplan*, at http://www.bipt.be/public/files/nl/21394/Consult_review_KB_Nummering_NL.pdf

[90] CEPT ECC, Evolution in the Use of E.212 Mobile Network Codes, ECC Report 212, 9 April 2014, at http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF

[91] Want, Schilit, and Jenson, note 39, p.30.

[92] Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge and Hans Graux, *Europe's policy options for a dynamic and trustworthy development of the Internet of Things*, RAND Corporation, 2013, pp.50-52, at http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf

[93] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, p.23.

[94] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, pp.23-25.

[95] Benghozi, Bureau and Massit-Follea, note 45.

[96] Christopher T. Marsden, *Net neutrality: Towards a Co-Regulatory Solution*, Bloomsbury, 2010.

[97] Article 29 Working Party, note 122, p.19.

[98] Republic of Korea Ministries of Science, ICT and Future Planning, note 60, p.11.

[99] Schindler, Cave, Robinson, Horvath, Hackett, Gunashekar, Botterman, Forge and Graux, note 97, p.86.

[100] European Commission, note 77.

[101] Center for Democracy and Technology, *Comments to the Federal Trade Commission after November 2013 Workshop on the "Internet of Things"*, 10 January 2014, p.3, at https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf

[102] FTC Staff Report, note 33, p.12.

[103] Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, Symantec Official blog, 23 January 2014, at http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam#!

104 Kevin C. Tofel, Got an IP webcam? Here are 73,000 reasons to change from the default password, *GigaOm Research*, 7 November 2014, at https://gigaom.com/2014/11/07/got-an-ip-webcam-here-are-73000-reasons-to-change-from-the-default-password/

105 FTC Staff Report, note 33, p.13.

106 Ashkan Soltani, What's the security shelf-life of IoT? *Tech@FTC blog*, 10 February 2015, at https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot

107 Cesar Cerrudo, *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks*, IOActive Labs White Paper, 2015, at http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf

108 See for example the US Federal Trade Commission's orders Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014); Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent); and HTC America, Inc., No. C-4406 (July 2, 2013) (consent), discussed in FTC staff report, note 120.

109 Article 29 Working Party, note 125, p.18.

110 36th International Conference of Data Protection and Privacy Commissioners, *Mauritius Declaration on the Internet of Things*, 14 October 2014, p.2, at http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf

111 See B.J. Koops and R. Levene, Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law, *International Review of Law, Computers & Technology* 28 (2), 2014, pp.159-171; ENISA, *Privacy and Data Protection by Design*, December 2014.

112 C. Cuijpers & B.J. Koops, Smart metering and privacy in Europe: Lessons from the Dutch case. In S. Gutwirth et al. (Eds.), *European data protection: Coming of age*, Springer, 2012, pp.269- 293.

113 FTC Staff Report, note 33, p.28.

114 Graham Greenleaf, Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories, *Journal of Law, Information & Science* (2014) 23(1).

115 Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 16 September 2014.

116 Article 29 Working Party. *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*. 11 February 2011.

117 Article 29 Working Party, note 125, p.6.

118 Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 16 September 2014, p.8.

119 FTC Staff Report, note 33, p.17.

120 Scott R. Peppet, Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent, 93 *Texas L. Rev.* 85 (2014), pp.115-16.

121 Peppet, note 127, p.93.

122 FTC Staff Report, note 33, pp.39—42.

123 Article 29 Working Party, note 125, p.16.

124 Jack H. Park, Government to Ease Up on Regulations on Financial Technology, Internet of Things, *BusinessKorea*, 12 December 2014, at http://www.businesskorea.co.kr/article/7814/internet-deregulations-government-ease-regulations-financial-technology-internet-things

4 Interoperability in the digital ecosystem

Author: Urs Gasser, Professor of Practice, Harvard Law School; Executive Director, Berkman Center for Internet & Society at Harvard University

4.1 Introduction

Large parts of the world are now interconnected as never before. People stay in touch with far-away family and friends for little cost. They learn about news instantly, access knowledge remotely, collaborate more efficiently, and conduct every manner of business online. The most complex systems—government agencies, financial institutions, transportation infrastructures, health care and energy systems—are linked by new, ubiquitous information media, which are essential components of today's global economy. But as interconnected as things currently are, they will grow dramatically more so with the emergence of the *Internet of Things* (IoT).

The IoT is the term for how anything that *can* be connected to the Internet *will* be. Interconnectedness through the Internet means not only new forms of interactions with end users, but also new forms of interactions with other devices. This is a world in which the car of a driver who is running late automatically will send a text message to the driver's next appointment in order to let them know she's running late. Or, a jet engine can inform the ground crew that it needs maintenance before the plane takes off. City parking meters can help drivers find open spots in order to reduce pollution and congestion. A pill bottle can remind a patient to take the next dose. The possibilities for new forms of interconnectedness are staggering and endless.

Some experts believe that the market for IoT devices will grow exponentially over the coming years, resulting in over USD 1.7 trillion in value added to the global economy by 2019.[1] This explosion of new, connected devices will require new infrastructure and technologies. Some analysts expect that new infrastructure models will be deployed within two years, and many existing networks will become overwhelmed with IoT traffic within just three years.[2]

This explosion of new IoT technologies, however, is built primarily on a single concept: interoperability. In order for a car, a jet engine, a parking meter, or a pill bottle to send and receive important data, it needs to be able to connect seamlessly to other systems and networks in ways that are meaningful and secure. That ability to secure the necessary interconnection of systems is *interoperability* (or "interop").

This capacity for connection has the ability to make daily life more convenient or efficient. But the growing level of interconnectedness may come at a high price if it is designed or implemented poorly. Society must make trade-offs as people and devices become digitally connected everywhere and anytime. As individuals struggle to keep up with news and information, they become vulnerable, in ways that are not obvious and are often misunderstood. The same infrastructure that enables people to create, store, and share information can put their privacy and security at risk. Society's most advanced systems and infrastructures have become so complex that they are hard to manage effectively. And while many parts of daily life become more connected, some remain woefully under-connected.

For that reason, it is important to define the optimal level of interconnectedness and to understand how technology, markets, law, and regulation can shape the outcomes. As a first step, this chapter looks at a framework for assessing how complex systems, components, and applications are connected—or sometimes, inexplicably, still separate. Then the chapter evaluates some of the promises and the drawbacks that come with increased connectivity. Finally, the chapter looks at approaches to enabling interop, and the role that governments, regulators, and organizations such as the ITU can play in that process.

4.2 Interop framework and use cases

Defining interoperability is challenging because there is no one-size-fits-all definition. How one defines interop is based largely on context and perspective. For example, in the context of electronic health records, patients may define interoperability as seamless access to their medical records. But the third-party operator of the hospital's e-health records database may define interoperability as the ability to technically interconnect with the hospital's computer systems and integrate health records in a meaningful (and secure) way. In that regard, interop is not just one type of transaction or relationship, it encompasses many forms of interaction, often occurring simultaneously. A transaction as simple as sharing electronic vaccination records with a new doctor might require numerous and concurrent forms of interoperability in order to succeed.

Although interop can mean many things, it is fundamentally the ability to transfer and render useful data and information across systems, applications, or components. But this definition does not fully embrace the complex and varying layers of interop. In theoretical terms, interoperability functions across four broad layers of complex systems, as shown in Figure 4.1.

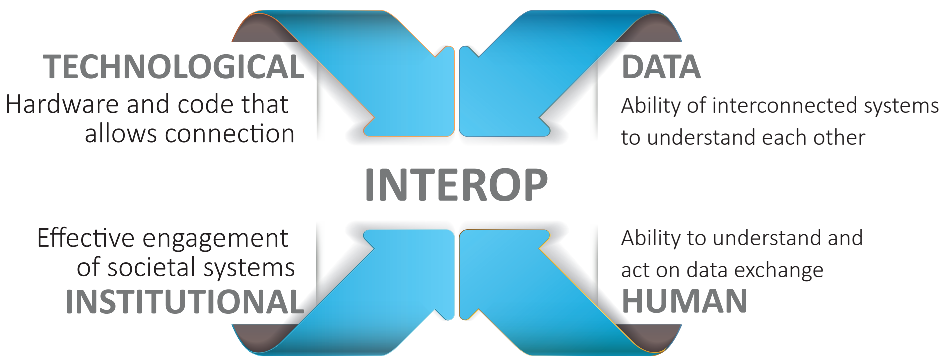
Many people think of the exchange of data through technological means when they think about interop. But case studies demonstrate that the human and institutional aspects of interoperability are often just as vital – and sometimes even more important-- than the technological aspects.[3] How individuals work together, often relying upon technological tools, can determine whether the most seamlessly interoperable systems prove effective at their given tasks. For example recent research on online learning tools has shown that the students who have both human and online instruction get the most out of the experience.[4] The human instructors bridge the gap for students when software alone falls short of meeting their individual needs. In other words, it is not sufficient simply to connect students with information without thinking about the other layers that affect their comprehension of the material.

What, then, do each of these interop layers mean?

- *Technological:* The technological layer is the hardware and code that allows one system to connect physically to another. Much like train tracks and roads allow cities to connect and share commerce, the technological layer allows systems to connect to one another and share data, often through an explicit, agreed-upon interface.

- *Data:* The data layer is the ability of interconnected systems to understand each other. Technological interoperability is often worthless without the data layer and the ability of interconnected systems to make use of the transmitted bits. The data and technological layers often are considered together because they are inextricably linked in many ways. However, anyone who has ever received an e-mail attachment that their computer could not open understands that simply having the technological capacity to

Figure 4.1 – Diagram of interop layers



Source: ITU

receive data is not the same as interoperability at the data layer.

- *Human:* This layer is the ability for humans to understand and act on the exchanged data. Although it is more abstract than the technological and data layers, this layer can be just as crucial for interoperability. Language is one form of human interoperability; in order to communicate, people need to use a common language. Another form of human interop is a willingness to work together. Interop often succeeds or fails based on the individuals and personalities at the end points of the data exchange, and their level of effort in working together successfully.

- *Institutional:* The institutional layer is the ability of social systems to engage effectively. The legal system is one example of an institutional layer of interoperability. For instance, in order for two companies in different countries to collaborate, they need to reach a shared understanding of applicable law and be comfortable that their rights can be vindicated. Interop at the institutional layer does not require homogeneity of legal systems; instead, it requires only *enough* commonality to protect the interests of both parties.

Although they are related concepts, it is important to clarify the relationship between interoperability and *compatibility*. Compatibility is a specific form of interoperability that represents certain design choices in the development of a system. For example, in 2014, the EU approved a directive that called for the use of a common standard for cell phone chargers.[5] This legislation addressed a narrow design choice: the compatibility of the cables that provide power to mobile devices. The interoperability of mobile devices is a far bigger and more complicated issue than a single element of compatibility, but the compatibility of cables certainly is one element of it. Throughout this chapter, it is important to bear in mind that compatibility is an important part of interop and can play an important role in how well and easily systems work together.

4.2.1 Mobile payments: Interop layers applied

In any complex, interoperable system, all of the four layers will play a role. In some examples, one layer may be more important than others, but successful interoperability relies upon interconnection at every layer. The recent growth of mobile payment platforms is a useful illustration of how the layers interact to shape the success of the platform as a whole. The mobile-payment ecosystem highlights the important role that the institutional and human layers have played.

Mobile payments are like traditional credit card transactions, just with a mobile device (typically a smartphone) instead of a plastic card. As smart phones have become more common, a variety of wallet-less electronic payment systems have proliferated, with mixed results. Beginning in 2011, Starbucks made it possible for customers to pay for their drinks using Starbucks' mobile app. Today, over 16 per cent of U.S. transactions at Starbucks are made through an app, representing more than 7 million payments per week.[6] Around the same time, Google announced Google Wallet, and although Google does not share detailed figures, there is evidence suggesting it has had limited use.[7]

The reportedly divergent results experienced by Starbucks and Google in this area have not discouraged other market entrants around the world. Recently, a federation of U.S. retailers, including the discount department store Walmart, announced CurrentC, a mobile payment platform designed to reduce the influence of traditional credit card companies and banks on retail transactions.[8] In October 2014, The Republic of Korea's Line messaging platform announced plans for a mobile payment service called Line Pay.[9] And in March 2015, South Korean electronics giant Samsung purchased LoopPay, a system that allows greater backward compatibility with older credit card retail terminals.

One of the most significant new entrants is Apple Pay, which was announced in September 2014. Within three days of rolling out its new app, Apple processed 1 million card activations.[10] The number of card-issuing banks grew from six in September 2014 to 2,500 in March 2015, and the number of retailers accepting Apple Pay tripled to nearly 700,000.[11]

What unites all of these mobile payment systems is their reliance on interoperability. The need for interop becomes apparent when one considers the variety of actors involved in a single transaction, as documented in Figure 4.2, below. Interconnecting all of these actors across a variety of merchants and devices requires numerous forms of interop at each layer. Although interop is necessary and present in every mobile payment platform, this example highlights a point addressed later in this chapter: interop is not a binary value – it can occur to greater and lesser degrees. The mobile payment competitors have taken different approaches, each trying to find the optimum level of interop, and Apple's and Starbucks' relative success in the mobile payment space demonstrates the importance of not neglecting the human and institutional layers.

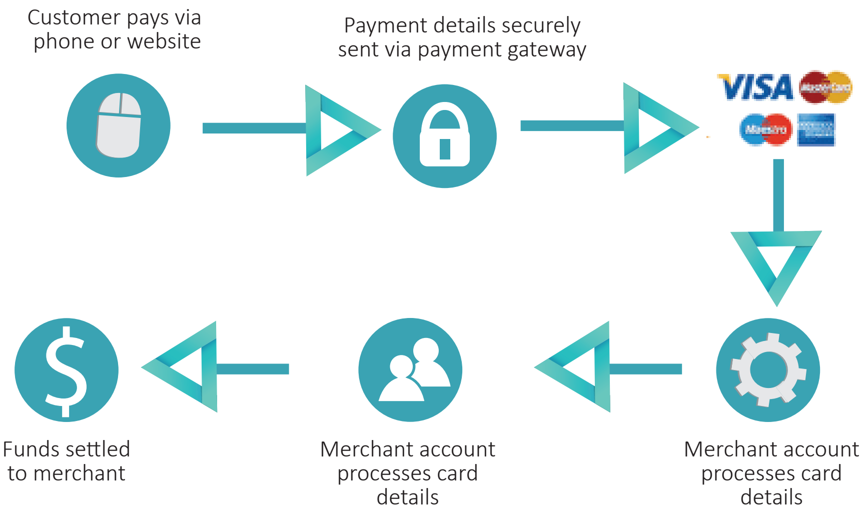
Consider some of the approaches the various payment platforms have taken at each layer:

Technological: Successful implementation of a mobile payment system requires multiple kinds of technological interoperability. One kind is the interconnection between banks and devices. For example, to set up a credit card to work with Apple Pay, Apple must have back-end compatibility with the processing banks in order to transmit user and card information to them.

Another type of technological interop is the ability of a mobile device to interconnect to the payment platform. Google Wallet, for instance, can run on a wide range of Android devices that contain a *Near Field Communication* (NFC) chip, which is necessary to communicate with the retailer's payment terminal.[12] Apple Pay also requires an NFC chip to exchange data with payment terminals, but it further requires that the device be an Apple iPhone with several security features, including a special encrypted chip and Touch ID for biometric identification. Because only the newest iPhone 6 and iPhone 6 Plus models have all of these technical components, those are the only devices that currently support Apple Pay, limiting the application's technological interop across devices.

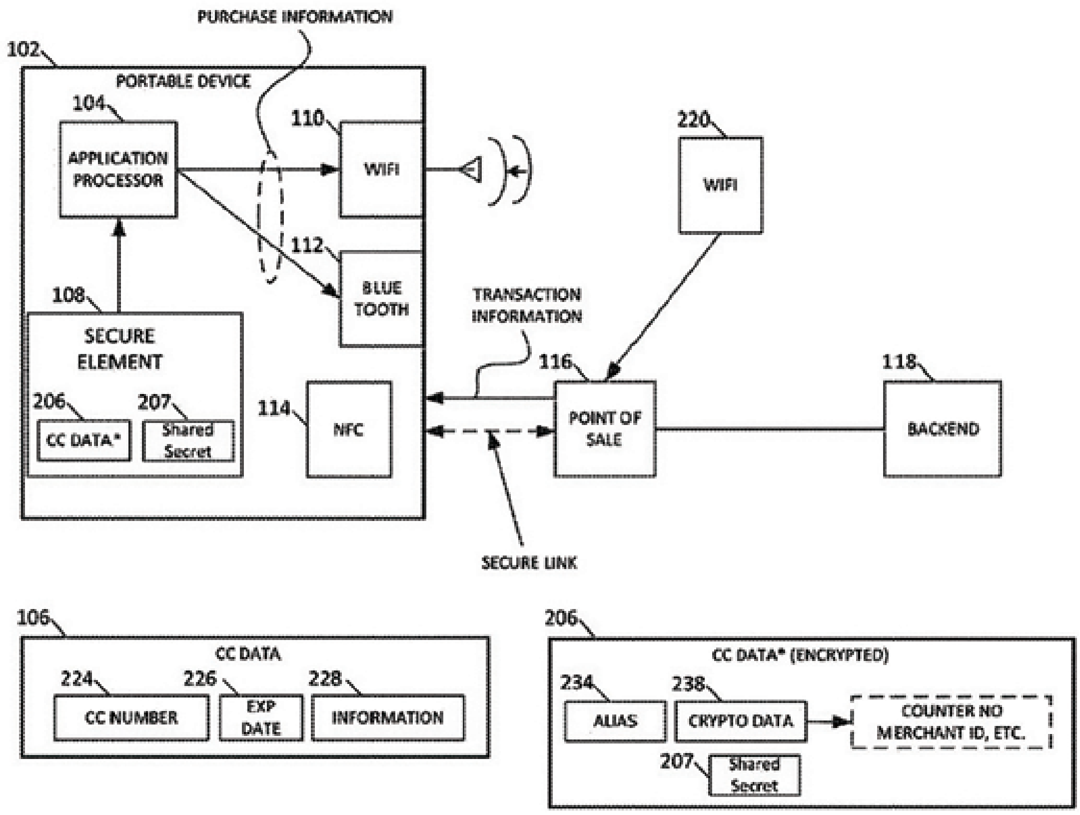
Another type of technological interop is the ability of the device to interact with retailers' payment systems. Because Apple Pay and Google Wallet use NFC communication, only retailers that have NFC-capable payment terminals can accept those services. Right now, only a small (but growing) number of payment terminals accept NFC, making this is a significant limit on technical interop. Figure 4.3 is a drawing from an Apple patent that shows interconnection with a retailer "point of sale." Although the patent does not necessarily describe the current iteration of Apple Pay, it highlights the complexity of the technological interop on the platform. CurrentC and Starbucks use bar codes instead of NFC, but this requires that the retailer payment system have an optical scanning device to read the bar code. Samsung's Loop Pay is designed to work with both NFC and existing magnetic card swipe terminals, dramatically increasing the technical interoperability.

Figure 4.2 – Diagram of mobile payment processing and various actors



Source: Web-Merchant.com, New to Online payments? http://www.web-merchant.co.uk/onlinepayments.asp

Figure 4.3: Apple patent diagram showing various components of Apple Pay system



Source: NFC World, http://www.nfcworld.com/2014/01/16/327536/apple-patent-combines-nfc-bluetooth-wifi-mobile-payments/

Data: For a retailer, simply having an optical reader or an NFC payment terminal is not sufficient to process CurrentC or Apple Pay payments, because retailers also need interop at the data layer in order to work with any given mobile payment system. For example, at the technical layer, Apple Pay and Google Wallet could work with any retailer payment reader that uses NFC. However, not all NFC readers can process Apple Pay or Google Wallet data. In fact, retailers associated with the CurrentC standard, including some of the largest retailers in the United States, disabled the use of their NFC terminals in order to stymie NFC-based competitors.[13]

Similarly, for a bank to interoperate with a mobile payment platform, it needs more than technical connections to the device. To increase transaction security, Apple Pay creates one-time-use secure tokens that are transmitted to the bank instead of credit card numbers. Using these tokens ensures that if a retailer is hacked, any captured numbers are unusable for future transactions.[14] However, use of these one-time tokens requires that the issuing banks be able to interpret these tokens and match them back to a specific user account.

Human: One of the biggest reasons why Apple Pay and Starbucks have been successful with mobile payments has been their respective approaches to the human layer. While other mobile payment systems are fairly complicated for the end users, Apple Pay and the Starbucks app were engineered for simple set-up. For example, Apple Pay requires only that the user photograph an image of their card. Then, to use Apple Pay, the user simply holds the device near an NFC terminal and activates the biometric fingerprint reader for verification. By contrast, as Figure 4.4 shows, setting up CurrentC requires multiple steps including entering a passcode, checking account data, and other identifying information.

Institutional: Many mobile payment systems operate over the existing institutional credit card network that comprises the global payment processing system. This system has already established the norms and rules that help ensure that retailers and banks are fairly compensated. One aspect of this system is the fee that retailers must pay to the credit card companies to cover the cost of the complex institutional network. These so-called "swipe fees" average up to about 2 per

Figure 4.4: Screen capture of instructions for adding payment information to CurrentC account

5. Adding a New Payment Account - Checking Account (ACH)

Want to pay with CurrentC using your checking account? Here's how:

- Open the CurrentC application
- Enter your 4-digit Passcode
- From the Home Screen select the **Accounts** button
- Make sure the **My Payment** tab at the top of the screen is selected
- Select the **Add** button
    - For iPhone and iTouch - The add button is a plus sign at the top right of the Accounts screen
    - For Android – Press your phone's menu button
- Click the **Add Payment** button
- Select **Checking Account** from the list of account types
- Enter your checking account information – *Note: This information is not stored in your phone.*
- Enter your personal information – *Note: Driver's license number and social security number are used to confirm your identity. This information is not stored in your phone.*
- Select the **Submit** button

Source: CincoTec, http://www.cincotec.com/blog/apple-pay-vs-currentc

cent of each transaction-- displeasing retailers.[15] For that reason, the CurrentC mobile platform, which is run by major U.S. retailers, is trying to circumvent the existing institutional payment structure. By withdrawing funds directly from end-user checking accounts instead of using credit cards, CurrentC aims to take advantage of the different institutional structure involving bank withdrawals, and thereby avoid the fees associated with credit card processing.

As the example of mobile payment systems demonstrates, all layers of interop are important. That is why no short definition of interop fully captures its scale and complexity. The example also highlights how technology, market, and law can either support or inhibit interoperability in a multitude of ways.

From a technical perspective, the mobile payments example shows that there is no single technical architecture for interoperability. Some market actors use NFC, others use optical bar codes, and still others use hybrid technologies. A company's choice of technological platform can have a big impact on its ultimate interoperability; the more widespread and available the technology is, the greater the opportunities for interoperability.

From a market perspective, the mobile payments example also shows the influence of *network effects* on actor behavior. Companies often set interop strategies depending on firm-specific factors, such as current market position, technological capabilities, and IP portfolio, among others. Perversely, network effects might be a disincentive for companies to use or market interoperable systems or devices. Apple, for example, seeks to use its mobile payment platform as a competitive differentiator. Thus, it has chosen not to interoperate with other mobile devices, limiting the platform to its newest iPhones.

From a legal perspective, the mobile payments market shows the influence of general laws such as competition law, consumer protection law, contract law, and tort law, as well as self-regulation. In particular, the self-regulation of the payment industry shows a bi-directional influence that simultaneously supports greater levels of interoperability and less. In the United States, new rules set by the industry will hold retailers liable for fraud unless they switched to new, interoperable payment terminals by October 2015.[16]

This self-regulation is increasing interoperability in several ways. First, the new payment terminals will support NFC payments, dramatically increasing interoperability between retailers and services like Apple Pay and Google Wallet. Second, self-regulation increases institutional interop by bringing the United States into line with European standards for more secure credit card processing. However, industry self-regulation arguably has also decreased interoperability in some ways, because credit card fees pushed CurrentC to adopt its less-interoperable approach to payment processing.[17]

The mobile payments example also highlights how interop is not a binary concept. There are degrees and types of interop, which fall along a multidimensional spectrum (explored in more detail in Section 4.5 of this chapter). Although all of the mobile payment systems involve various levels of interop, some take a more unilateral approach, while others rely upon collaboration. Because Google does not build smart phone hardware, it relies on cooperation from partners in order to deploy Google Wallet on compatible handsets. By contrast, because Apple controls its device ecosystem, it can deploy Apple Pay with less reliance on others.

The same interoperability diversity can be observed in regulatory approaches. As part of its *Cloud Computing Strategy*, for example, the U.S. Government variously and simultaneously mandates interop standards, influences interop through procurement strategies, and helps support the development of multi-stakeholder processes to develop additional standards and approaches.

The benefits and costs of interoperability are most apparent when technologies mesh seamlessly. Consumers consistently prefer systems that work together without asking them to work, making their lives simpler in the process. The data layer, a close cousin of the technology layer, turns out to be just as important as the technological layer. It is critical for data to be interoperable across systems; it must be readable and understandable. Without interoperability at the technological and data layers, interoperability at the higher layers in the model—the human and institutional layers—is often impossible. But the challenge of getting the basics of interoperability right, even at the fundamental technology and data layers, can be deceptively hard.

4.3 Benefits of higher levels of interop

Interoperability is not an end in itself. Instead, optimizing interop has societal value as a means to other ends. Innovation is one policy goal that often benefits from increased interop, but it can also have a positive impact on consumer choice, ease of use, access to content, and diversity, among other things. This section highlights some of the key ways that higher levels of interop can be beneficial.

4.3.1 Innovation

Perhaps the strongest example of how interop can foster innovation is the Internet itself. It possesses the ultimate interoperable design, allowing the convergence of multiple, previously non-interoperable networks and systems. It is on this open, interoperable infrastructure that the Internet of Things is being built. Every IoT device-- from a jet engine “requesting” service to a thermostat checking the weather-- relies on the fact that the protocols that enable devices to connect across the network are agnostic to the data transmitted using those protocols. In other words, high degrees of interoperability enable and foster innovation over the Internet, including deploying networked devices.

Companies with a strong interest in the IoT are currently hoping to replicate the success of the Internet by spurring innovation at the IoT layer, which itself runs on top of the Internet. For example, one consortium of tech companies has created Thread, an open protocol to help connect low-power devices. Another consortium of tech companies is creating a protocol to enable faster and easier device discovery and interconnection.[18] Outside of the commercial context, ITU also has been a leader in advancing standardization in the IoT space.[19] In all cases, the hope is that building protocols to enable interconnection will support increased innovation on top of an IoT platform.

In addition to economic innovation, interop also enables science and research. The European Commission recently released a report outlining the need for a “Digital Single Market” in the European Union and announcing 16 initiatives designed to spur its creation.[20] In that report, the Commission noted that a lack of interoperability in the “European data ecosystem” was hampering innovation, because “neither the scientific community nor industry can systematically access and re-use the research data that is generated by public budgets, despite strong demand.”[21]

It is worth remembering that although innovation is generally positive, it can include risks. Just as interop can help develop innovative devices and software, it can also support innovative devices and software with negative social impacts. Worms, viruses, spam, and other unwanted activity are in many ways just as "innovative," and just as dependent on interoperability, as positive developments. A recent example of this peril can be found in a vulnerability in the SSL protocol (which enables secure, encrypted communication across the Internet) that led to the so-called "Heartbleed" hacking episode.[22] Because the SSL protocol is interoperable, anyone with enough technical knowledge can write a version of the protocol that can be used interchangeably. One version, called OpenSSL, became so popular that it was running on an estimated 66 per cent of the Internet. Unfortunately, OpenSSL had a critical flaw—the Heartbleed—that allowed attackers to see encrypted communications. Thus, interop enabled this vulnerability to become widespread.

Additionally, high degrees of interop can sometimes threaten innovation. For instance, a successfully interoperable system's network effects can lead consumers to stick with an existing service. This might diminish operators' incentives to invest in an entirely new technology, i.e., a *radical* innovation that would replace the older system. In such a scenario, operators might implement only incremental improvements to existing, interoperable systems. This would foreclose opportunities for radical innovations that would more vastly improve services.

4.3.2 Competition

Standard economic analysis suggests that increased interoperability is likely to foster innovation by reducing lock-in effects and lowering barriers to entry. This pattern is observable in the subscription streaming video market. HBO, a movie network and content creator, recently began selling its HBO Now service directly to consumers over the Internet, breaking with its traditional business model of selling only through cable and satellite TV providers.[23] Under its old model, HBO's content distribution system needed to interoperate only with those cable and satellite systems. Under the new model, however, HBO needs interoperability with web browsers and devices such as Apple TV, Roku, Chromecast, and others.

This change toward increased interoperability has increased competition in two ways. First, it has increased competition for subscription TV services. By decoupling its content from cable and satellite TV systems, HBO put those operators on notice that they no longer have content monopolies to ensure customer lock-in. In fact, several cable companies have begun offering "skinny" packages consisting of high-speed broadband, HBO, and just a few other channels, in order to compete with lower-priced, online-only services like HBO Now and Netflix.[24] Second, by increasing its interoperability, HBO is competing in an entirely different market: online content streaming services. This shift has not gone unnoticed by Reed Hastings, CEO of Netflix, who recently remarked, "I predict HBO will do the best creative work of their lives in the next 10 years because they are on [a] war footing. They haven't really had a challenge for a long time, and now they do. It's going to spur us both on to incredible work."[25] This kind of competition benefits users by reducing prices and by providing incentives for product and service innovation.

Although interop generally supports competition, in some circumstances it could, counter-intuitively, lead to anticompetitive results. Certain arrangements that lead to interoperability and to greater innovation may boost a single firm -- or a few firms-- in a manner that is, over time, anticompetitive. For example, standards consortiums may sometimes create closed standards that enable interoperability across only their stakeholders' products.[26] In this way, interoperability can be employed as a tool for building closed ecosystems. The value to the consumer of being in the ecosystem (and benefitting from the interoperability the ecosystem provides) can in turn raise costs for switching providers and thus reduce competition.[27]

Even when more interoperability does lead to more competition, the net result is not necessarily maximum innovation. According to one economic theory, firms may have the strongest incentive to be innovative in circumstances where low levels of interoperability would promise higher or even monopoly profits. This sort of (Schumpetrian) competition incentivizes developing entirely new generations of technologies or ways of doing business (so-called "leapfrog competition") in order to replace incumbent players and achieve temporary dominance.

Amazon's strategy in the e-book market, for example, might be a case-in-point for this sort of competition. Initially, Amazon's e-books were incompatible with most non-Kindle devices. But this lack of interoperability actually aided the company's search for monopoly profits. Amazon e-books now can be read using Amazon's free reader software on Android, iOS, Windows, and OS X devices. Still, Amazon e-books can only be read either on Amazon devices or through Amazon's software.

4.3.3 Autonomy, flexibility, and choice

In almost all circumstances, increased levels of interoperability tend to enhance user choice and autonomy. In interoperable ecosystems, users are more likely to choose the best from among competitive and efficient options. Systems, applications, components, etc., may be tested, mixed, and matched for specific purposes. One way that interoperable systems offer choice is through *application programming interfaces* (APIs), which are instructions for how one application or system should talk to another.[28] Twitter had an open API, which allowed anyone to write a Twitter client that could access Twitter's underlying data. The Twitter API supported a vibrant Twitter client ecosystem, and users could switch easily between the Twitter clients of their choice. Twitter's decision to change its API in order to capture all of the client traffic (ultimately capturing the ad revenue) has reduced user choice and nearly eliminated the availability of third-party clients.[29]

Users are not the only ones with greater freedom of choice when the level of interoperability increases. Consider, for instance, e-book publishers that run the risk of getting locked into a single distribution channel. If Amazon builds up a dominant market position based on a non-interoperable system, publishers will have no choice but to sell to Amazon at nearly any price it demands. By contrast, an interoperable system would lower the barriers to entry, making it difficult for Amazon to lock publishers into bad deals. In fact, it was this fear that led to a recent high-profile dispute between Amazon and publishers.[30]

4.3.4 Access, diversity, and openness

Increased levels of interoperability can make it easier for users to access content. Creating an account can be a hurdle for users, and once they do so, they need to memorize an additional password. *Single-sign-on digital ID* infrastructure seeks to address both of these concerns. First, single-sign-on infrastructure allows users to log into new services using existing credentials, such as their Facebook account. This lowers the barrier to joining new services and speeds up the process.

Second, because the user can log in without creating a new account, it means that user needs to remember only their single-sign on password, instead of creating a new password. "Login with Facebook" is one example of this approach, which is intended to make it easier for users to log into a variety of online services, not just Facebook.com. As more sites interoperate with a single-sign-on platform, the value to the user increases, as it reduces access barriers to online services of various sorts, including e-commerce platforms.

Similarly, increased levels of interoperability can also make it easier for users to engage in commerce. The European Commission's report on the Single Digital Market noted that a lack of interoperability, primarily at the technological and institutional levels, made it hard for consumers to purchase online goods to be shipped from one EU country to another. This was reducing access to those goods and suppressing online commerce. In response, the Commission called on the member states "to improve the interoperability of systems for cross-border delivery of goods and services...."[31]

In addition, there appears to be positive correlation between interoperability and "diversity." As noted above, Twitter's open API supported a variety of clients. Moreover, when that API was restricted, it quickly led to a decrease in the diversity of Twitter clients, with several unable to sustain their businesses following Twitter's changes.

4.4 Potential risks and drawbacks

Interoperability is not an unalloyed good. In certain instances, greater interoperability brings drawbacks. These problems tend to be highly fact-specific and are often not problems related to interoperability *per se*. They relate to what people do with the interoperable systems.

4.4.1 Increased security risks

As described above, systems can increase interoperability by:

- providing greater opportunities for technical interconnection;
- being more open about the types of systems and services that can interconnect;
- supporting a greater variety of data; and by
- making it easier for humans to leverage the interconnections.

Unfortunately, each of these forms of interop can also increase the opportunities to exploit the system. A system that has more points of access allows (1) more types of systems to connect, (2) processes data with fewer limitations, (3) increases potential attack vectors and (4) creates more opportunities for nefarious actors to exploit data or to inject bad code. For example, single sign-on systems like "Login With Facebook" are convenient for end users, but they can also mean that a single stolen credential gives an attacker access to numerous online systems, instead of just Facebook itself.[32]

This security concern is not precisely a problem with interoperability, nor is it insurmountable. The fact that the systems can interoperate does not *per se* mean that more people have access to underlying data in a given system. But increased interoperability between systems can lead to vulnerability if sound security measures are not taken. For example, it was recently discovered that Apple Pay's mobile payment system was being misused to commit credit card fraud.[33] The problem was not caused by interoperability, but rather because some banks were not properly verifying account credentials when users set up Apple Pay accounts. Criminals were able to take advantage of this by registering stolen credit card numbers in Apple Pay. Interoperability may increase the number of opportunities for security breaches, or the potential fall-out from such breaches, but it does not cause the security vulnerabilities. By the same token, systems that are not interoperable at all are just as likely to have damaging security breaches if proper precautions are not taken.

4.4.2 Decreased privacy

The possibility, in certain situations, that interoperability might reduce individual privacy is among the most commonly voiced concerns. It is true that increased interoperability may raise the number of individuals with access to one's personal information. Single sign-on systems are the most obvious ways that interoperability might lead to less privacy. If technical and user controls are not well established, giving multiple service providers access to a user's online identity increases the risk of misusing that data. In the electronic health records context, where privacy is of the utmost importance, an interoperable standard may allow the capture or theft of highly sensitive personal data.

Interoperability builds more complex ecosystems, with more participants, creating more risk vectors. Against that backdrop, however, interoperability *per se* does not give rise to increased privacy risks. Rather, it is the specificities of its implementation. Even if one assumes a technically waterproof interoperability solution cannot be achieved—a highly debated assertion—one can imagine effective organizational or legal tools, such as privacy regulation, successfully addressing privacy concerns.

4.4.3 Increased homogeneity

Interoperability might lead to less diversity in a market. A single platform for many interoperable systems might become a *de facto* standard that constrains innovation. Again, it is not interoperability *per se* that causes such homogeneity, but rather the economic consequences of market actions made easier by the interoperability.

The Internet is a wonderfully interoperable system that has led to tremendous innovation, but the protocols that underlie it represent a form of homogeneity. Most of the interconnected systems that people use today rely on TCP/IP at some level to connect to the Internet. The protocols themselves do not include security components or end-to-end data reliability, requiring encryption to be added on top of the basic protocol.[34] In that way, the widespread prevalence of the Internet protocols constrains innovation. Security and other necessary components must be added on top of the protocol, because otherwise it would be too hard to innovate new protocols and get widespread adoption, even if those new protocols were arguably better. In the same way, e-mail protocols have become a *de facto* standard. This homogeneity constrains what is possible, ultimately providing an upper bound on the security that can be achieved in standard e-mail.[35]

4.4.4 Decreased reliability

The increased complexity of interoperable systems may lead to decreased reliability. Whether this drawback becomes a factor depends heavily on the approach taken towards interoperability. As more systems rely on interop, the overall network grows in complexity, and flaws in these systems might be difficult to fix quickly or even to identify. In some instances, flaws in one system may affect other, interconnected systems – leaving the interconnected networks powerless to fix them. This problem might affect consumers, too, who find they cannot identify a single point of contact in order to get a problem fixed. Consider a customer at a store who is having trouble using her mobile payment system. Is the problem with the retailer's payment terminal or the customer's mobile device? Is it the payment system or the underlying credit card infrastructure? It may be challenging or impossible for the customer to diagnose the problem. In fact, nearly two thirds of Apple Pay users have reported problems using the service, leading many of them simply to give up on the system, particularly if the problems are outside of the user's control.[36] As interoperability scales up, the level of complexity will continue to rise.

There is a variation of the reliability issue – over-reliance. As interoperability increases, downstream systems become increasing reliant on upstream systems. This problem was observed when Twitter's decision to change its open API threatened to disrupt the downstream systems that relied on that API. Even though there is no promise among the entities to maintain the status quo, the abandonment of it may threaten interoperability by reducing the incentive of downstream entities to invest or trust in it.

An open standards approach to interoperability holds out significant promise to ameliorate both the reliability and over-reliance challenges. In complex, interoperable systems, it would be helpful if firms could solve problems for consumers as seamlessly as possible across interconnected systems. Open standards could mitigate, though not completely solve, this issue. Problems could be solved collaboratively, with multiple stakeholders represented in the process of identifying and implementing joint solutions.

4.4.5 Decreased accountability

Against the backdrop of increased complexity, the question of responsibilities and liabilities calls for increased scrutiny. In the context of single sign-on for digital IDs, for example, one can imagine a scenario in which a third party, such as an advertiser, misuses a consumer's data. The lack of a contractual relationship with the advertiser may hinder the consumer's ability to receive proper compensation for the harm. But interoperability, again, is not the cause of the harm, and a careful drafting of contracts could avoid unintended and unnecessary liability exposure. As an alternative, the digital service provider could take a more active role in policing the third parties. Facebook recently took this step, demanding that companies using Facebook credentials submit to "an audit process that requires them to explain why they've chosen to collect certain pieces of customer information in their data payload." Based on those explanations, Facebook can choose to deny access to data.[37]

4.4.6 Decreased accessibility

Looking at the risks of decreased reliability and security from interoperability, there are concerns that these problems might induce some players to withdraw from the online environment. In the electronic healthcare record industry, for instance, there are concerns that interoperability might pose higher security risks than would non-interoperable solutions. Doctors and patients might then opt out of the system. Although that hasn't happened yet, if it does, accessibility will decrease and the efficiency and health gains of online distribution will be lost, at least in part.

4.4.7 Threats to business models

Higher levels of interop can have many benefits, but those benefits may be distributed unequally across a market. Indeed, some businesses may have a vested interest in maintaining *lower* levels of interop, allowing them to benefit from locking-in customers. For example, in 2012, Amazon sold its Kindle e-reader devices at cost, profiting solely from the sale of content to customers who were locked in to the Amazon ecosystem.[38] Amazon achieved this customer lock-in by limiting both technological and other forms of interop. At the technological layer, the company did not allow its e-books to be read through non-Amazon software or e-readers (although Amazon did enable the Kindle to interoperate in limited ways with the services of other firms, such as a daily download of the *New York Times* or reading e-books on a Kindle iPhone, iPad, or Android app). Similarly, the Kindle did not support common open formats such as EPUB. This lack of technical interop helped ensure that customers would rely on Amazon's marketplace for content.

Amazon has also tried to reduce interop at the data and human layers, by limiting publishers' alternatives to Amazon. As part of its business strategy, Amazon has priced e-books at prices lower than competitors' (sometimes at a loss) in order to encourage lock-in. Several book publishers began to fear that this customer lock-in would kill competitors and enable Amazon to demand monopoly pricing from publishers. Some of these publishers challenged Amazon's strategy, asserting that they wanted to set prices equally across all e-book stores. In other words, the publishers wanted to increase the interoperability of their content across platforms. This conflict between publishers and Amazon became a public dispute when Amazon pulled most Hachette books from its store in retaliation. After a protracted battle, the publishers won temporary control over the prices for their books.[39]

The fact that higher levels of interop may pose a threat to certain business models is not a downside of interop *per se*, nor is it a reason to avoid policies and strategies that promise higher levels of interop. In some circumstances, disrupting these kinds of business models may be a real benefit.[40] That said, it is important to acknowledge that not everyone views higher levels of interop with favour, and those whose business models are threatened may actively undermine interoperability.

Taken together, the risks and drawbacks of interop can paint a challenging picture. But the potential negative aspects of a highly interoperable future are not inevitable. The risks or benefits largely stem from how interoperability is implemented and regulated. As individuals, businesses, and regulators build an increasingly interconnected world at the technology and data layers, care must be taken to ensure that they avoid costs in areas like privacy and security that society is unwilling to pay. A theory of "interoperability by design" that builds in privacy and security protections from the start can help enormously in this respect.

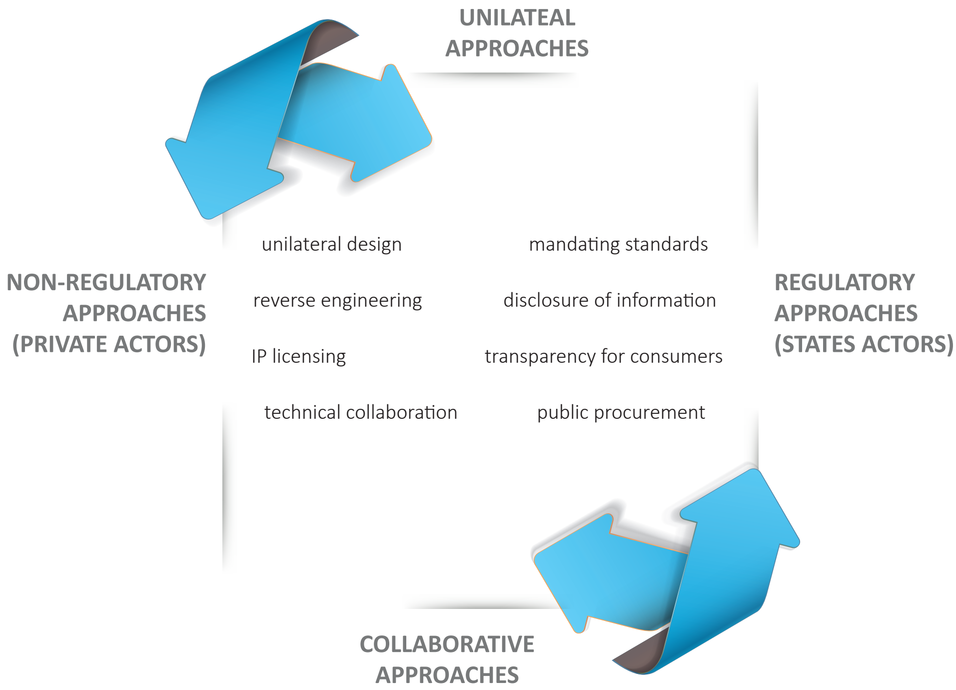
4.5 Approaches

As shown by several examples in this chapter, there are varieties of approaches to interop. It is useful to think about these approaches along a spectrum from unilateral to collaborative. In other words, there are many ways to incorporate varying levels of interop, ranging from providing an open API (a more unilateral approach) to working with competitors and other stakeholders to create open standards (a more collaborative approach). Moreover, this same spectrum-- from unilateral to collaborative-- is apparent across both private-sector and government actors, including national and transnational regulatory bodies. This spectrum of approaches is depicted in Figure 4.5 and described in the following sub-sections.

4.5.1 Non-regulatory approaches (private actors)

Many interoperability strategies rest on access to technology or technical specifications and involve licensing *intellectual property* (IP) rights or other contractual agreements. However, the degree of cooperation among different players and the corresponding licensing terms may vary considerably from case to case. The following sections sketch three clusters of approaches to interoperability that range from unilateral to highly collaborative.

Figure 4.5: Approaches to interop



Source: John Palfrey & Urs Gasser, Interop (2012)

4.5.1.1 Unilateral design and IP licensing

The first cluster of approaches includes those that are marked by a comparatively low degree of collaboration between the systems that are interconnecting. Unilateral design occurs when a market participant designs its products or services in a way that allows other players to offer interoperable products or services. The range of possibilities in this cluster of more "unilateral" approaches is considerably broad. For example, companies often use APIs as a unilateral invitation for others to interconnect. In the case of single-sign-on, digital ID offerings, companies like Facebook offer an open API that any app or online store can utilize, provided they comply with Facebook's rules for accessing the API. Twitter's revocation of its open API is a cautionary tale of how reliance upon unilateral forms of interop may be risky, because they can be withdrawn as easily as they are offered.

Another important and related way to achieve interop with minimal collaboration is through IP licensing, in which one party grants another access to technology, specifications, and/or rights associated with the technology's use. The effectiveness of a licensing approach to interoperability not only depends on the company's willingness to grant a licence in the first place, but also on the terms in the licensing agreement.

The scope of-- and compensation for-- the licence plays a particularly important role. IP licensing can be a cost-efficient path toward a higher degree of interoperability, especially in cases where transaction costs are minimized through sophisticated and "streamlined" licensing procedures. The flexibility of a licensing arrangement may decrease, however, if the ecosystem changes. This was precisely the pattern observed in the publishing dispute between Hachette and Amazon. When the market was relatively immature, the licensing agreements between the publishers and e-book makers were fairly simple, largely following existing licensing models. However, as the market matured and Amazon's Kindle became the dominant technical platform, the book publishers feared a loss of flexibility in the licensing terms. At that point, the licensing process became far more fraught, and the publishers sought more control over the pricing of their products.

4.5.1.2 Technical collaboration

Technical collaboration is a more collaborative form of interop. It usually involves some form of IP licensing at its foundation, but the cooperation goes beyond the mere granting of IP licences. Often, technical collaboration is an approach used by companies at different levels of the value chain, in order to improve the user's experience. A significant example of this is the level of cooperation required for many mobile payment systems, which require technical cooperation between retailers, device manufacturers, payment processors, and banks.

Technical collaboration shares many of the advantages of IP licensing and generally appears to be an effective, efficient, and flexible approach toward increased levels of interoperability. However, some scenarios entail fewer such advantages. One of these is a situation in which the collaborators grow so large that coordination and monitoring costs become too difficult or expensive. This challenge has occurred in mobile money markets in some countries. As a recent ITU report described, "In a country with just a few mobile payment operators, it might be possible to do this bilaterally or multilaterally. However, as the number of operators increases, the relationships between them, and the costs of the solution, grow exponentially."[41] Like other approaches, technical collaboration can also be misused to achieve anti-competitive objectives not aligned with increased interoperability goals.

4.5.1.3 Standards and open standards

Standards can be characterized as a collaborative effort to achieve higher levels of interoperability. *Open standards* have gained much attention in recent times, although the exact definition remains controversial. One interpretation is that open standards (a) are approved by formalized committees open to participation by all parties, and (b) are accessible to the public free of charge.

The healthcare field provides examples of both open and less-open standards, sometimes within the same organization or institution. One example is the ITU-T Focus Group on machine-to-machine interoperability, which focuses largely on e-health applications such as remote patient monitoring. It has released an open API and several free reports in order to support the ITU's standardization work.[42] By contrast, the ITU has used a more hybrid approach in the development of ITU-T H.810 standards for the interoperability of personal health systems. In that case, the ITU partnered with Continua Alliance, a non-profit organization that charges for access to its standards.[43]

Standards hold great potential to achieve high degrees of interoperability, but this approach also can limit overall effectiveness. Open standards initiatives are a purely voluntary effort, and anecdotal evidence suggests that companies with patent portfolios might easily interfere or even block such initiatives. Furthermore, standard-setting processes are often complex, time-consuming, and relatively expensive when compared to unilateral or bilateral approaches. Arguably, their cost efficiency is, therefore, comparatively low.

With regard to flexibility, standards reflect the characteristics of the specific environment in which they are intended to operate. This means that a standard may represent a snapshot of technology development at a particular point in time. Depending on the speed at which technology develops, a standard based on outdated assumptions might restrictively peg future developments to historical limitations.

4.5.2 Regulatory approaches (state actors)

As Figure 4.5 illustrates, Governments and regulators can also pursue interoperability through a variety of different approaches, from unilateral to more collaborative ones. These activities also vary significantly with regard to how specifically they address interoperability. On one side are approaches such as mandating standards or requiring the disclosure of interoperability information. On the other side are interventions or laws that are more generic and are aimed at increasing transparency or competition but do not address interop specifically. Particularly careful consideration is needed in interop-specific interventions, while the application of general laws and doctrines is much less problematic.

It is important to note that regulatory approaches can be carried out by a variety of different governing entities. At the national level, this could be a legislative body, an executive agency or ministry, or an independent regulatory authority. At the regional or international levels, this could be a multinational body or a coordinating agency like the ITU. The remainder of this chapter interchangeably refers to these various entities as "governments," "policy-makers" or "regulators." In all cases, the terms are simply referring to any regulatory body that exercises some form of legitimate governmental authority. The following subsections explore the various regulation-based approaches.

4.5.2.1 Mandating standards

The role of the regulator in the standards process can range from more unilateral to more collaborative. Regulators may mandate a standard that determines how, and under what terms, entities can interoperate. On the other end of the spectrum, the regulator might set a timetable for industry players and require them to establish and implement a common standard. Between the two extremes, all manner of hybrid approaches are possible.

The impact of the European Union's *Data Protection Directive* on the development of cloud computing standards demonstrates the interplay between regulation and interoperable standards. The *Directive* places strict limits on how personal data can be collected, stored, and processed. However, because the *Directive* and the national laws that implement it do not specifically address cloud computing, it has left open the question of how cloud-computing companies should fulfill their obligations. This situation has prompted standards-setting as entities look for ways to interoperate with each while complying with the law. Recently, the International Organization for Standardization and the International Electrotechnical Commission, two non-governmental standards-setting organizations, released a joint cloud computing standard that contributes to the already existing "jungle of standards."[44]

The effectiveness of this type of approach to interoperability is usually very high. A government-mandated standard can even establish an interoperable system in cases where industry players are unwilling to do so, whatever their motives might be. However, a government-mandated approach may be limited in efficiency and flexibility. Administering, monitoring, and eventually enforcing a standard can be costly. Further, a traditional, government-mandated approach often leaves very little flexibility. Not only are governments sometimes ill-equipped to choose the most suitable standard, but they also sometimes fail to respond to market developments or changes in technology.

4.5.2.2 Disclosure of interoperability information (compulsory licensing)

Another regulatory approach to interoperability involves a government mandating the disclosure of information needed to build interoperable systems, components, and applications. Such a regime may differ with regard to the group of people entitled to ask for such information, the possible consideration for the disclosing party, compensation, or the sanctions for non-disclosure. In some cases, however, the regulator can simply require industry participants to make interoperability information available, and leave it to the participants to resolve details like compensation. That is what occurred with mobile banking in Ghana, where the mobile carriers offered financial services in partnership with banks. In order to ensure interoperability across different banks and mobile carriers, the Bank of Ghana (the regulator) prohibited exclusive partnerships. In other words, the regulator required that mobile operators allow interoperability with multiple banks. The result was that every mobile operator offering banking services had at least three partner banks.[45]

The merits of this approach depend on its implementation – that is, the design of the relevant disclosure rules. There often can be a direct relationship between the amount (and type) of information to be disclosed, the number of parties granted access to the information, and the level of interoperability that may be achieved. The degree of flexibility also depends on the design, but disclosure rules can be implemented in a way that takes account of real-world conditions (*e.g.*, making the obligation to disclose dependent on market, product and service maturity). Finally, disclosure of interoperability information is very unlikely to create any kind of technological lock-in.

4.5.2.3 Transparency rules (labeling requirements)

In order to reduce potential information asymmetries, the government can use a traditional approach aimed at fostering transparency. It can mandate the disclosure of information about the interop characteristics of a certain product or service. Again, such regulation may vary in several ways, including the characteristics and appearance of the information to be disclosed. The government need not establish transparency in "specific" legislation addressing interoperability in a certain area. Such regulation could be-- and often already is, at least partially-- implemented pursuant to consumer protection or competition law.

Although often not mandatory, certification programs often serve this role of bringing transparency to interoperability. For example, after the ITU set the home networking standard G.9954 for existing-wire, multimedia home networking, the HomePNA association began certifying devices for compliance with the standard.[46] Similarly, the IEEE created a program to certify products conforming to ITU-T Recommendation G.8265.1 (relating to synchronization of mobile backhaul networks).[47] In neither case was transparency explicitly mandated, but increasing transparency about interoperability was necessary for those in compliance with the standards to maximize the benefits of their compliance.

Because labeling requirements contribute to interoperability in indirect ways, their effectiveness is difficult to assess. Much depends on the design of the labeling provisions and how well they balance between information insufficiency and overload. Recent research suggests that information needs to be embedded in consumer decision-making processes in order to be effective. While there are monitoring and enforcement costs associated with labeling requirements, it is likely that they are more efficient overall than the regulatory approaches outlined previously. Finally, the flexibility of labeling requirements is high, given the indirect nature of the approach and, therefore, the limited conflict with future technological developments.

4.5.2.4 Market power in procurement decisions

The government may favor interoperable products or services when undertaking procurement decisions, leading the market to adopt the interoperable solutions. Such an approach requires that the government possess substantial purchasing power in the relevant market. This is apparent in the move toward government use of cloud services, where governments are investing significant resources in moving services and data to third-party, cloud-based systems.

Cloud computing service providers, however, are interested in making their services as “sticky” as possible to minimize loss of customers to competitors. Ultimately, governments can lock themselves into a particular cloud service provider. In some cases, a fear of lock-in has proven to be a drag on the market, scaring away potential customers. This has been the case in Europe’s market for cloud computing services.[48] For that reason, governments can try to influence the market by hiring only companies that support data interoperability.[49] This approach was described in the European Commission’s *Digital Single Market* report, which notes that the use of procurement power is often the most effective way to translate standards into actual interoperability.[50]

This approach is effective only when a government's procurement decisions have a considerable and lasting market impact. It may turn out to be relatively inefficient when the government has to choose between an offer with lower upfront costs and an offer with higher levels of interoperability. The flexibility of the procurement approach is comparatively low, because the exercise of procurement power may create a technological lock-in on the part of the government (or else cause significant costs if the exercise of procurement power is to be repeated).

4.5.2.5 Competition law

Interoperability also can be achieved through an ex-post intervention grounded in competition law. The refusal of a dominant market player to disclose interoperability information may be considered an abuse of that dominant position. Even when a company discloses interoperability information at the technical layer, competition law still may prevent anticompetitive practices at the data layer.

Whether competition law extends to this level currently is being tested at the European Commission, which has recently filed a formal antitrust complaint against Google.[51] At issue in the case is how Google interoperates with sites that offer competing shopping services. Although Google will display data from comparison shopping tools that compete with its own services, competitors claim that Google tries to drive visitors to its own services. If the European Commission prevails in its case against Google, it will highlight the importance of paying attention to all of the interop layers, not just the technological layer. Similarly, the European Commission has recently launched an antitrust competition inquiry into the e-commerce sector of the European Union. It is exploring "barriers to accessing goods and services online across borders."[52]

Antitrust interventions are effective in establishing interoperability in specific areas. However, if they wind their way slowly to a resolution, they run the risk of lagging behind market development and becoming irrelevant. Further, governments typically incur significant costs to monitor and enforce the competition laws. On the positive side, however, the fact-based and narrowly tailored nature of antitrust interventions generally ensures the flexibility of the approach with regard to the market, technological, and legal environment in which it is applied.

4.5.2.6 Supplementing strategies

In addition to the approaches outlined in this section, governments and regulators also have at their disposal "supplementing strategies." These include funding research initiatives aimed at establishing higher levels of interoperability, facilitating standards-setting processes, and establishing public-private partnerships that foster interoperability. Although governments' roles may be naturally oriented toward top-down action, it is important for them to bear in mind the variety of bottom-up approaches in which they can participate.[53]

4.5.3 Benchmarks for Interop

Each of the approaches identified in Section 4.5.2 (both private-sector and regulatory approaches) has its own strengths and weaknesses or, in more economic terms, costs and benefits. One of the trickiest tasks is to evaluate them from a policy-oriented perspective and in an unbiased and balanced manner. On an abstract level, the following three benchmarks may be helpful starting places for evaluation.

4.5.3.1 Effectiveness

Each approach described above is likely to result in different levels of interoperability and can be expected to play a distinct role in maintaining an interoperable ecosystem. The suggested effectiveness criterion evaluates the respective contributions and compares the available approaches that are considered in a given situation. Understanding interoperability as a means and not an end in itself, the evaluation of an approach's effectiveness should also consider to what degree the respective strategy tends to enhance competition in the market, foster innovation, or contribute to other policy goals such as consumer autonomy and choice. To be effective, a solution must also provide interoperability over time, not just in the immediate circumstances.

4.5.3.2 Efficiency

In several instances, achieving and maintaining a certain level of interoperability comes with costs. The efficiency criterion seeks to measure the level of costs imposed on an affected player—companies, but also users and governments, among other stakeholders—for a given degree of interoperability and compare it with other available means of achieving interoperability. The costs of unintended consequences (some of them addressed in this chapter under the heading "potential risks and drawbacks") also need to be taken into account.

4.5.3.3 Flexibility

In order to be successful, a given approach to interoperability needs to be able to take into account important facts about the market. These include the market's maturity, product and service development, the features of current and future business models, the needs of users, etc. Looking forward, it is particularly important that the approach be responsive to technological development in order to avoid technological lock-in.

Depending on the context, the three benchmarks of effectiveness, efficiency, and flexibility might have different relevance or weight. One might imagine scenarios, for example, in which interoperability serves such an important goal (*e.g.*, emergency number compatibility) that flexibility – at least in the short run – is less important than a high degree of effectiveness in the immediate term. In other instances, a government might not want to impose standards, given their relatively high cost and poor flexibility, despite the approach's potential effectiveness.

4.6 The role of government

4.6.1 Governments have multiple roles

As noted above, governments and regulators can choose many possible approaches to fostering interoperability. Given the array of approaches, as well as the necessity of properly matching the approach to the situation, it is important to consider how governments can best deploy their array of tools in the "interop toolbox."

Of course, governments can act as regulators, but they can actually implement interop policy through several other roles. Consider, for example, the following roles that governments have played while pursuing interoperable cloud strategies:[54]

- Governments as users – Governments are adopting cloud computing services to take advantage of cost savings and innovative features – and, in turn, they are using their market power to shape interoperability.

- Governments as regulators – Governments can act through their legislative, judicial and regulatory branches to implement policy through the rule of law.

- Governments as coordinators – Governments might coordinate public and private initiatives, through standards-setting processes and by facilitating the sharing of information between private and public stakeholders.

- Governments as promoters – Governments can actively promote the industry as a whole by endorsing and funding incubation programs.

- Governments as researchers – Governments are conducting or funding research on technical or societal issues important for interop.

- Governments as service providers – Governments can choose to provide cloud services for use by other government agencies or the public.

Governments should critically consider the timing and type of any intervention on behalf of promoting interoperability. Regulators, for instance, need to determine carefully the appropriate time to intervene, for instance, by adjusting consumer protection or privacy laws. They need to strike the right balance between facilitating technological innovation and providing regulatory safeguards for users and other stakeholders. Ideally, the government responds to public guidance in making these determinations and engages in a multifactor analysis to determine the right time to intervene with the right intervention. Such an analysis would include assessing the maturity of the technology and market structure.

Even government use of procurement power requires careful consideration. By acting early to influence the market, governments can have the biggest impact on the development of a market and its use of interoperability. But as soon as industry practices and standards are set, they are much harder to influence. For that reason, some countries have found better results by anticipating needs early and entering the market when their influence can be most effective.

It is also critical to recognize that technology, markets, strategies, and rationales for adoption and promotion *change over time*. The dynamic nature of technologies, such as cloud computing, requires that governments engage proactively over time, adjusting their actions with the changing landscape. Governments should see this as a systematic learning process.

The National Institute of Standards and Technology (NIST) at the United States Department of Commerce has been effective at adapting to changing circumstances in its work on development of an interoperable smart grid. One example of this is how NIST managed the Smart Grid Interoperability Panel (SGIP), a multi-stakeholder body it convened in 2009 to help develop necessary standards. Initially, NIST staff held key leadership and technical roles on the SGIP. However, in response to a changing environment and the increased maturity of the smart grid industry, in 2013 NIST transitioned SGIP into an industry-led non-profit organization. By October 2013, SGIP had more than 200 members, and it had finalized 56 standards.[55]

4.6.2 Role of governments as legal stewards

Governments can also shape an important part of the institutional layer of interop in their role as caretakers of a robust and stable legal framework. The future success of emerging complex systems, such as cloud computing, will depend not just on market forces but also on a well-developed legal environment. Governments must establish trust and legal certainty for both users and providers of future interoperable systems.

The relationships between interop and the law are many, complex, and tangled. The law can help establish, adjust, or maintain interop. At the same time, interoperability is also a feature of the legal system itself. *Legal interoperability*, broadly defined, is the process of making legal norms work together across jurisdictions. This may occur either within the legal system of a single nation-state—between national and local legislation—or across national lines. Like technical interoperability, legal interoperability is not a goal in itself but, rather, a means to one or more ends.

The relationship between law and interoperability is multidirectional. Higher levels of interop are often the product of carefully designed legal interventions—or, at least, are fashioned in the shadow of the law. One example of this is the enforcement of competition law against powerful technology companies trying to leverage their market power by excluding competitors. The mandated disclosure of interoperability information as a matter of consumer protection is another.

Conversely, interoperability itself can prompt calls for new laws to address its effects; it may also lead to the adjustment or reinterpretation of existing legal norms. As an example, consider the relationship between interoperability and privacy. Technical interoperability leads to concerns about data privacy. In response, the European Court of Justice expanded existing privacy directives to include a "right to be delisted" that spans jurisdictions. The changes wrought by higher levels of interoperability in the technology sector are prompting calls for new forms of legal interoperability.

Governments have several options to increase levels of legal interoperability. The point is not to make the systems all the same but rather to make them work together in particular ways. It is not necessary for countries to turn over all legislative authority to the United Nations or to create a raft of new treaties that govern all jurisdictions. It is not possible to smooth out all cultural or legal differences through harmonization of laws. Nor should it be the goal to create one uniform "world law." Jurisdictions compete productively against one another, and learn from each other, by experimenting with new laws and policies. Governments need to aim for interoperability among legal systems at an optimal level, rather than a maximum level, just as they do with other interop challenges.

It is important to find this optimal level, because evidence suggests that legal interoperability, especially in the information economy, drives innovation, competition, trade, and economic growth. For instance, when China joined the World Trade Organization in 2001, it had to change many laws and enact new ones to satisfy the demands of its trading partners. China has made large-scale changes, for instance, in its system of intellectual property law. Though Chinese law is not the same as intellectual property law in the United States or Europe, it is dramatically closer to those standards today than it was a few decades ago.

The EU faces a similar challenge today in aligning online commerce rules with the divergent copyright, contract, and VAT laws of "28 national markets."[56] As part of its Digital Single Market objective, the European Commission has proposed 16 initiatives to bring about greater levels of legal interop.[57]

This level of legal interop, however, comes with challenges. As legal interop increases, companies find it feasible to enter markets that were previously off limits. But those companies frequently face challenging legal questions that require them to reconcile competing law and interests. For example, as Twitter expanded into more countries, it confronted an increasingly large number of demands to remove content. Initially, Twitter responded by removing Tweets worldwide. If a user in a single country demanded removal of a Tweet, Twitter would do that for all users, in all markets. However, Twitter eventually decided it would be better to use geolocation to remove Tweets only for users from the country that made the legal demand.

Sometimes friction, in the form of low levels of legal interoperability, may be desirable from a public policy viewpoint. For example, one of the most important considerations for governments is cybersecurity. Leaders are extremely concerned about the security implications of highly interconnected systems. Interoperability means that viruses and targeted cyber-attacks can have damaging consequences. Government-created friction at the technical and data layers may be controversial.[58] But friction in terms of low levels of *legal* interoperability across countries may be beneficial if it encourages greater diversity of non-interoperable systems that may serve certain defensive purposes.

Legal interoperability is a complex and critical issue, in part because it has the ability to either enable upward mobility in the global economy or to reinforce existing power structures, depending on the choices made. [59]

4.7 Important issues for the future

Interoperability is not an end in itself. And interoperability doesn't always have to be maximized. Instead, private actors and regulators must work carefully to optimize the level of interop necessary to meet their objectives, even though the process is neither easy nor simple. This chapter has described an interop framework, the potential costs and benefits of increased levels of interop, and a variety of approaches for encouraging interop. Thus, when determining the optimum level of interop, all of these factors must be carefully weighed and balanced.

With emerging and profound new systems and technologies, it is important to bear in mind some of the big questions and challenges that confront the Internet of Things and other, future interoperable technologies. Although these big questions do not yet have good answers, anticipating and considering them now may help regulators and policy-makers deal with them going forward. Some of these big questions are:

- **How does society address a proliferation of standards?** In several areas, notably e-health, there is now a seemingly ceaseless release of new standards – some of which, no doubt, add value. Many others, however, are conflicting efforts. If standards are meant to bring interoperability to otherwise incompatible approaches, what happens when the sheer number of conflicting standards fragments the market, undermining the original goal of interoperability? In the consumer goods market, the solution to this problem is generally to let the standards compete and let the invisible hand of the market choose among the competing standards. But that approach can be expensive in time and money. It may also delay in innovation as potential market participants wait to invest in the winning standard. For these emerging new technologies and systems, are such costs acceptable? Or, is there a way to accelerate the process of choosing the optimal standards?

- **How can interop better manage complexity and scale?** As described above, higher levels of interop can lead to highly complex systems. This complexity and scale, however, has many costs. It can make it hard to identify and correct failures. It can create security risks and magnify the impact of vulnerabilities. At certain scales, it can even represent a form of lock-in, as network effects become predominant. In many ways, successful interop can be its own worst enemy. How can interop better mitigate these problems in order to capitalize fully on the societal gains of large-scale interop?

- **How can highly interoperable systems better communicate with end users?** As described in this chapter, end users often do not know where to turn when something goes wrong in a highly interoperable system. If a system behaves like a single, cohesive unit, that is both a success for interop and an obfuscation to the end user. This presents a challenge for interop even under the best of circumstances, where the end-user might have access to multiple parts of the system and can interact with the operators through highly complex interfaces. However, in the Internet of Things or the wearables market, end users are unlikely to have access to large parts of the system, and the interface may be as small as a watch face. In those challenging circumstances, how can interoperable systems better communicate with end-users?

- **How do issues of surveillance and national security factor into the interop calculus?** When regulators and governments are weighing whether and how to intervene in order to encourage higher levels of interop, to what extent should surveillance and national security factor into those decisions? The Internet is value-neutral and networks can be used in ways that either benefit or harm society; interoperability merely amplifies both. Higher levels of interop do not inexorably lead to more surveillance or less. Greater levels of interop can create both a higher risk of surveillance and greater threats to national security. How, then, do governments approach interop issues when considered through the lens of their broader roles and responsibilities?

- **How do regulators optimize interop while operating within the constraints of their complex political environments?** Although regulators and policy-makers have many traditional means of increasing levels of interop (*e.g.*, mandating standards, passing legislation), this chapter has highlighted many of the other approaches in the regulatory toolbox. Indeed, in many cases, these alternative approaches may be the most effective. Governments, however, have many constituencies with competing interests. The balancing described in this chapter is challenging enough in a vacuum, and is even more so in the real world. For example, an agency may feel political pressure to demonstrate decisive action, when a more light-handed approach actually would better optimize interop. How can governments best take into account their constraints while still enabling interop?

The answers to these questions are not simple, but wrestling with them will be critical for designing the next generation of interoperable technologies.

Appendix 1: **Suggested additional readings**

In order to streamline the reading experience, Chapter 4 cites a relatively small number of works. A glance through those few notes, however, hints at the wider range of work by academics, practitioners, and regulators in this field. In addition to the notes cited in the chapter text, below is a selection of other readings that offer a starting point for readers who want to dig deeper into interop.

Stacy A. Baird "Government Role and the Interoperability Ecosystem" (*I/S: A Journal of Law and Policy* 5, no. 2 [2009]: 219–290).

Yochai Benkler, *Wealth of Networks* (2006).

Yochai Benkler, *The Penguin and the Leviathan: The Triumph of Cooperation over Self-Interest* (2011).

Laura DeNardis, *Opening Standards: The Global Politics of Interoperability* (2011).

"Network Effects," in David Easley and Jon Kleinberg, *Networks, Crowds, and Markets: Reasoning About a Highly Connected World* (2010).

Urs Gasser and John Palfrey, *Interop* (2012).

Marc Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (2006).

Viktor Mayer-Schoenberger, "Emergency Communications: The Quest for Interoperability in the United States and Europe" (Kennedy School of Government Faculty Research Working Chapters Series RWP02–024, March 2002).

John Palfrey, *Intellectual Property Strategy* (2011).

Hal Varian, Joseph Farrell, and Carl Shapiro, *The Economics of Information Technology* (2004).

Rolf H. Weber, "Legal Interoperability as a Tool for Combatting Fragmentation," CIGI (Paper Series No. 4, Dec. 2014).

Jonathan Zittrain, The Future of the Internet and How to Stop It (2008).

Endnotes

[1] John Greenough, *The 'Internet of Things' will be the world's most massive device market and save companies billions of dollars*, Business Insider (Feb. 18, 2015), http://www.businessinsider.com/the-internet-of-things-market-growth-and-trends-2015-2#ixzz3WBO0CLrW.

[2] IDC*, Press Release: IDC Reveals Worldwide Internet of Things Predictions for 2015*, Dec. 3, 2014, http://www.idc.com/getdoc.jsp?containerId=prUS25291514.

[3] Berkman Center for Internet & Society, *Interoperability Case Studies*, https://cyber.law.harvard.edu/node/92249.

[4] Justin Reich, *The Role of Humans in Blended Learning*, May 26, 2014, http://www.edtechresearcher.com/2014/05/the_role_of_humans_in_blended_learning/.

[5] Directive 2014/53/EU of The European Parliament And of The Council, 2014 O.J. (L. 153/62), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0053&from=EN.

[6] Marcus Wohlsen, *Forget Apple Pay. The Master of Mobile Payments is Starbucks*, Wired, Nov. 3, 2014, http://www.wired.com/2014/11/forget-apple-pay-master-mobile-payments-starbucks/.

[7] Charles Arthur, *How Many Google Wallet Users Are There? Google won't say - but we can*, The Guardian, Sept. 25, 2014, http://www.theguardian.com/technology/2014/sep/25/google-wallet-apple-pay-nfc.

[8] Josh Constine, *CurrentC is the Big Retailers' Clunky Attempt to Kill Apple Pay and Credit Card Fees*, Tech Crunch, Oct. 25, 2014, http://techcrunch.com/2014/10/25/currentc/.

[9] Catherin Shu, *Line Pay, the Messaging App's Mobile Payments Service Will Make Its Global Debut Soon*, Tech Crunch, Dec. 4, 2014, http://techcrunch.com/2014/12/04/line-pay-the-messaging-apps-mobile-payments-service-makes-its-debut/.

[10] Daisuke Wakabayashi, *Apple CEO Tim Cook Happy With New Apple Pay Service*, WSJ, Oct. 28, 2014, http://www.wsj.com/articles/apple-ceo-tim-cook-happy-with-new-apple-pay-service-1414474181

[11] Anthony Ha, *Apple Pay Now Accepted In Nearly 700k Locations*, Tech Crunch, Mar. 9, 2015, http://techcrunch.com/2015/03/09/apple-pay-stats/#rU8Np5:AqOz

[12] For more information on NFC, please see Daniel Howley, *What is NFC, and Why Does It Matter For The iPhone 6?*, Yahoo! Tech, Sept. 3, 2014, https://www.yahoo.com/tech/what-is-nfc-and-why-does-it-matter-for-the-iphone-6-96456683964.html.

[13] Jason Del Rey, *Why You Can't Use Apple Pay at CVS, Walmart and Other Retail Stores*, Re/Code, Oct. 28, 2014, http://recode.net/2014/10/28/why-you-cant-use-apple-pay-at-cvs-walmart-and-other-retail-stores/.

[14] Bob Sullivan, *How Tokenization May Change The Way You Pay*, CNBC, Dec. 14, 2014, http://www.cnbc.com/id/102264704.

[15] National Retail Federation, *Swipe Fees*, https://nrf.com/advocacy/policy-agenda/swipe-fees.

[16] Tom Gara, *October 2015: The End of the Swipe-and-Sign Credit Card*, Wall Street Journal, Feb. 6, 2014, http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/.

[17] Tony Bradley, *Blocking Apple Pay is a Terrible Strategy For CurrentC Merchants*, Forbes, Oct. 29, 2014, http://www.forbes.com/sites/tonybradley/2014/10/29/blocking-apple-pay-is-a-terrible-strategy-for-currentc-merchants/.

[18] Tina Amirtha, *Google's Secret Weapon in the Battle for the Internet of Things: Academia*, Fast Company, Feb. 10, 2015, http://www.fastcompany.com/3041698/googles-secret-weapon-in-the-battle-for-the-internet-of-things-academia.

[19] ITU, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

[20] *See* European Commission, Digital Single Market, http://ec.europa.eu/digital-agenda/en/digital-single-market.

[21] European Commission, Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence* (2015), at 59, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.

[22] The Heartbleed Bug, http://heartbleed.com.

[23] Miriam Gottfried, *HBO Now Spells Trouble for Pay TV's Tomorrow*, Wall Street Journal, Apr. 9, 2015, http://www.wsj.com/articles/hbo-now-spells-trouble-for-pay-tvs-tomorrow-heard-on-the-street-1428615881.

[24] *Id.*

[25] Emily Steel, *Netflix Is Betting Its Future on Exclusive Programming*, NY Times, Apr. 19, 2015, http://www.nytimes.com/2015/04/20/business/media/netflix-is-betting-its-future-on-exclusive-programming.html.

[26] Sam Paltridge, Michael Donohue, Brigitte Acoca, *2015 OECD Digital Economy Outlook: Chapter 5: Emerging Issues: The Internet of Things*, OECD, DSTA/ICCP(2014)15/CHAP5/REV1 (Mar. 20, 2015), at 38.

[27] Eric Jackson, *Apple Isn't a Hardware or Software Company – It's an Ecosystem Company*, Forbes, June 30, 2014, http://www.forbes.com/sites/ericjackson/2014/06/03/apple-isnt-a-hardware-or-software-company-its-an-ecosystem-company/ (describing how the value of being in Apple's ecosystem increases as their devices gain greater interoperability *within* Apple's own platform).

[28] Brian Proffitt, *What APIs Are and Why They're Important*, Read Write, Sep. 19, 2013, http://readwrite.com/2013/09/19/api-defined.

[29] Mike Beasley, *Twitterrific 5 for Mac may become the first casualty in Twitter's war on developers, but it won't be the last*, Nov. 25, 2014, http://9to5mac.com/2014/11/25/twitterrific-5-twitters-war-on-developers/.

[30] David Streitfeld, *Amazon and Hachette Resolve Dispute*, NY Times, Nov. 13, 2014, http://www.nytimes.com/2014/11/14/technology/amazon-hachette-ebook-dispute.html?_r=0.

[31] European Commission, Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence* (2015), at 67, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.

[32] Amit Chowdhry, *How Facebook Finds Out If Your Passwords Were Stolen*, Forbes, Oct. 22, 2014, http://www.forbes.com/sites/amitchowdhry/2014/10/22/how-facebook-finds-out-if-your-passwords-were-stolen/.

[33] Robin Sidel, *Apple Pay Sign-Ups Get Tougher as Banks Respond to Fraud*, Wall Street Journal, Mar. 6, 2015, http://blogs.wsj.com/totalreturn/2015/03/06/apple-pay-sign-ups-get-tougher-as-banks-respond-to-fraud/.

[34] Ian Peter, *Can TCP/IP Survive?* Circle ID, Sep. 7, 2004, http://www.circleid.com/posts/can_tcp_ip_survive (Article describing several of the weaknesses in the TCP/IP protocol).

[35] David Talbot, *Why E-mail Can't Be Completely Private*, MIT Technology Review, Aug. 14, 2013, http://www.technologyreview.com/news/518056/why-e-mail-cant-be-completely-private/.

[36] Tim Higgins, Elizabeth Dexheimer, *Apple Pay Running Into Hurdles at Checkout Counter, Survey Finds*, Bloomberg Business, Mar. 31, 2015, http://www.bloomberg.com/news/articles/2015-03-31/apple-pay-running-into-hurdles-at-checkout-counter-survey-finds-i7x95shl.

[37] Alexandra Larralde, *Social Login Trends Across the Web: Q4 2014*, Janrain, Jan. 8, 2015, http://janrain.com/blog/social-login-trends-across-the-web-q4-2014/.

[38] Reuters, *Amazon Kindle Sold 'At Cost,' CEO Jeff Bezos Confirms*, Huffington Post, Oct. 11, 2012, http://www.huffingtonpost.com/2012/10/11/amazon-kindle-lost-leader-bezos_n_1959919.html.

[39] David Streitfeld, *Amazon and Hachette Resolve Dispute*, NY Times, Nov. 13, 2014, http://www.nytimes.com/2014/11/14/technology/amazon-hachette-ebook-dispute.html?_r=0.

[40] *See* Part 3.2, *supra*.

[41] Venkatesen Mauree, *The Mobile Money Revolution: Part 2: Financial Inclusion Enabler*, ITU-T Technology Watch Report (May 2013), http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf, at p. 15.

[42] *See, e.g.*, ITU-T Focus Group on M2M Service Layer, *M2M service layer: Requirements and architectural framework*, Apr. 2014, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-M2M-2014-D2.1-PDF-E.pdf.

[43] ITU-T, *HSTP-H810: Introduction to the ITU-T H.810 Continua Design Guidelines*, July 11, 2014, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-EHT-2014-H810-PDF-E.pdf.

[44] Paul de Hert, Vagelis Papkonstantinou, Irene Kamara, *The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection*, Brussels Privacy Hub, Working Paper v. 1, N°2, Nov. 2014, http://ssrn.com/abstract=2542125, at p. 7.

[45] Venkatesen Mauree, *The Mobile Money Revolution: Part 2: Financial Inclusion Enabler*, ITU-T Technology Watch Report (May 2013), http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf, at p. 16.

[46] *HomePNA Certifies 9 More Products, 1 Reference Design, Increases Number of Reliable, Interoperable Products to 26*, Business Wire, Apr. 16, 2008.

[47] *IEEE Conformity Assessment Program (ICAP) Announces the Official Launch of the IEEE 1588(TM) Telecommunications Certification Program*, Marketwired, Oct. 9, 2013.

[48] *See* European Commission, Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence* (2015), at 61, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.

[49] *See generally* Urs Gasser, David O'Brien, *Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*, Berkman Center Research Publication No. 2014-6 (Mar. 7 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

[50] European Commission, Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence* (2015), at 66-67, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.

[51] Tom Fairless, Rolfe Winkler, Alistair Barr, *EU Files Formal Antitrust Charges Against Google*, Wall Street Journal, Apr. 15, 2015, http://www.wsj.com/articles/eu-files-formal-charges-against-google-1429092584.

[52] European Commission, Antitrust: Commission Launches E-commerce Sector Inquiry, Press Release, May 6, 2015, http://europa.eu/rapid/press-release_IP-15-4921_en.htm.

[53] Rolf H. Weber, *Legal Interoperability as a Tool for Combatting Fragmentation*, CIGI (Paper Series No. 4, Dec. 2014).

[54] *See generally* Urs Gasser, David O'Brien, *Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*, Berkman Center Research Publication No. 2014-6 (Mar. 7 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

[55] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, NIST Special Publication 1108R3 (Sept. 2014), http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf.

[56] European Commission, *A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen*, Press Release, May 6, 2015, http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

[57] European Commission, Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence* (2015), at 67, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.

[58] Cory Doctrow, *Crypto wars redux: why the FBI's desire to unlock your private life must be resisted*, The Guardian, Oct. 9, 2014, http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted.

[59] Rolf H. Weber, *Legal Interoperability as a Tool for Combatting Fragmentation*, CIGI (Paper Series No. 4, Dec. 2014).

5 M-services and applications: Perspectives on regulatory measures to foster diffusion and access

Author: Mercy Wanjau, Assistant Director, Communications Authority of Kenya

"The world was so recent that many things lacked names, and in order to indicate them it was necessary to point."

Gabriel Garcia Marquez[1]
One Hundred Years of Solitude

5.1 Introduction

We are living in the midst of a social, economic, and technological revolution. How we communicate, learn, socialize and conduct business has moved beyond the narrow confines of language and geographical proximity and onto the Internet. The Internet has, in turn, moved into our phones, laptops, homes and cities, and it continues to wield profound influence on civic, commercial and social engagement in society.

One of the outcomes is an explosion of data that is bringing numerous insights that are changing our world.[2] A study conducted in 2013 found that the impact of the mobile sector on other industries such as energy, health and financial was so profound that it could fundamentally change how those sectors operate.[3]

5.2 Welcome to the digital ecosystem

For the last two decades or so, mobile technology has been at the heart of the digital ecosystem, with innovations in voice, data and increasing speeds of broadband. This mobile revolution has helped to bridge access gaps, delivering services to businesses and citizens alike. The objective of this chapter is to discuss perspectives on regulatory strategies that can be adopted to facilitate diffusion and access of m-services and applications.

5.2.1 What are m-services and applications?

In beginning this discussion, it is important to mention that m-services and apps (i.e., applications) are different. Apps ride on networks that also deliver m-services (mobile services). Indeed, both can thrive on similar regulatory approaches, to some extent. However, at some point they call for differentiated regulatory intervention, in order to establish an enabling environment. Given this context, this chapter will illustrate regulatory strategies to promote the diffusion of both m-services and applications. Particular references will be made to m-payments and m-health, to highlight specific issues.

The portability of mobile has promoted ease of access to the Internet. Conventional services such as banking, access to government services, and education are now accessible in regions where these services were either unavailable or inadequate before. Governments throughout the world-- and particularly in developing countries -- are looking to mobile platforms for innovative ways to improve the delivery of public services and to foster participation in public policy-making.4 The unique capabilities heralded by the "Golden Age of Mobile" enable efficiencies that continue to hold much promise for citizens, businesses and governments alike.

The interface between the Internet and devices, particularly portable ones, offers an attractive distribution platform for multiple apps and services. Initially, mobile apps were offered to enable general productivity and information retrieval, including email, online calendars, contacts, stock market and weather information. However, public demand and the availability of developer tools drove rapid expansion into other categories, such as word processing; social media; picture sharing; mobile games; factory automation; GPS mapping and location-based services; banking; networking and file transfer; education; video streaming; order tracking; ticket purchases and, more recently, mobile medical apps and more. The popularity of mobile apps has continued to rise, as their usage has become increasingly prevalent across mobile phone device platforms.

Apps are usually available through application distribution platforms typically operated by the developer/owner of the mobile operating system. Usually, they are downloaded from the platform to a target device, such as an iPhone, BlackBerry, Android phone or Windows Phone, but sometimes they can be downloaded to laptops or desktop computers. Mobile applications usually help users by connecting them to Internet services more commonly accessed on tablets, smart phones or notebook computers. The bottom line is that mobile apps make it easier to use the Internet on their portable devices. But for these apps and services to be available, access to an ICT network is required.

5.2.2 Sector Growth

According to ITU statistics, the number of mobile-cellular subscriptions worldwide is approaching the number of people on Earth, which is estimated at about 7 billion. This corresponds to a penetration rate of 97 per cent, up from just 738 million in 2000. Globally, an estimated 3.2 billion people are using the Internet, of which 2 billion are from developing countries.

The statistics also indicate that mobile broadband is the most dynamic market segment, with a penetration reach of 47 per cent in 2015-- a value that has increased 12 times since 2007. The proportion of the population covered by a 2G mobile-cellular network grew from 58 percent in 2001 to 95 per cent in 2015. During the same period, 3G mobile-broadband coverage was extending rapidly and into the rural areas.[7] The fixed-broadband uptake was found to have grown at a slower pace, with a 7 per cent annual increase over the past three years. Fixed broadband was expected to reach an 11 per cent penetration rate by the end of 2015.

Looking towards the future, mobile networks will play an even more significant role in the post-2015 development agenda. This opportunity will arise through use of mobile networks as delivery media for m-services and applications. As countries continue to make positive progress in upgrading mobile networks, deploying 3G-plus technologies

Box 5.1: What is a mobile app?

A mobile app is a software program you can download and access directly using your smart phone or another mobile device, like a tablet or music player.

What do I need to download and use an app?

You need a smart phone or another mobile device with Internet access. Not all apps work on all mobile devices. Once you buy a device, you're committed to using the operating system and the type of apps that go with it. The Android, Apple, Microsoft and BlackBerry mobile operating systems have app stores online where you can look for, download, and install apps. Some online retailers also offer app stores. You'll have to use an app store that works with your device's operating system. To set up an account, you may have to provide a credit card number, especially if you're going to download an app that isn't free.[5]

What is mobile for development?

Mobile for development is a broad term that captures initiatives that bring together mobile network operators (MNOs) and the development community to promote commercial mobile services for the benefit of under-served people in emerging markets. These initiatives are driven by the premise that mobile is the predominant infrastructure in emerging markets; they seek to identify opportunities for social, economic and environmental impact.[6]

and adopting more enabling regulatory policies and practices, broadband and mobile devices will become more affordable, stimulating the development of the digital ecosystem. Additionally, it will be important to remove the barriers persons with disability face, enabling them to enjoy full and free participation in the development agenda.[8]

5.2.3 Drivers of m-services and apps

There are several trends that are building momentum for rapid dissemination of m-services and apps, and these are discussed in the following sub-sections.

5.2.3.1 Commitment to digital inclusion

The power of ICTs to enable the achievement of development goals has strengthened the case for "social inclusion" objectives, to include broadband connectivity, telephony service coverage, and Internet access-- all aimed at small and medium-sized rural communities and the urban poor. The increasing use of applications to deliver civic services, health, and education – and to drive businesses and commerce – entails the need to commit to digital inclusion. This will drive the articulation of coherent and comprehensive national broadband plans in order to achieve the intended benefits.[9] But there is no "one size fits all."[10] According to the OECD, as broadband technology continues to improve and bandwidth increases, its capacity to enable structural change in the economy will expand due to its impact on an increasing number of sectors and activities.[11]

5.2.3.2 Competition

The increasing reliance on competition as the primary driver of consumer benefits has spurred significant economic growth in many countries. For example, in 2014, mobile services added 3.2 per cent (USD 548 billion) to the United State Gross Domestic Product (GDP), exceeding the contributions to GDP of several other industries, including entertainment, transportation, automobiles, hospitality, and agriculture.[12] Robust competition has brought about lower prices, improved quality and greater innovation and diversity in consumer choice.

The rapid expansions of fixed and mobile broadband services, and the drop in broadband prices, have been major drivers of the Information Society. The biggest drop has occurred in developing countries, broadening the affordability and access to m-services and apps.[13] High-speed Internet access has continued to increase as broadband prices fall and mobile broadband networks expand rapidly. Almost all countries in the world have launched at least "third generation" (3G) mobile-broadband services, and the number of subscriptions has been growing rapidly. It is believed that by the end of 2015, mobile broadband penetration reached 47 per cent globally.[14]

5.2.3.3 Access to big data

Today, data is more deeply woven into the fabric of our lives than ever before. Data can be used to anticipate and solve problems, improve well-being, and generate economic prosperity. The collection, storage, and analysis of data is on an upward and seemingly unbounded trajectory, fueled by increases in processing power, the cratering costs of computation and storage, and the growing number of sensor technologies embedded in devices of all kinds.[15] Data collection and handling, as well as data aggregation and analysis, bring out new insights that are informing monetization opportunities in the mobile ecosystem.

5.2.4 Emerging concerns

The growing diffusion of mobile services and applications also raises concerns that need to be addressed in order to sustain the digital ecosystem. To start with, increased adoption of the digital inclusion agenda will mean recognizing the isolation of populations that have no access to m-services and apps. How is a regulator to respond and ensure that the benefits of social inclusion are enjoyed by all its citizens?

While competition has spurred consumer choice and enhanced benefits, the regulatory concerns remain: Is competition being encouraged adequately? Where meaningful competition is missing, are timely interventions being made to support universal service? Are regulatory principles in place to encourage investment and innovation?

Box 5.2: Karnataka app M-One

Karnataka state in India launched its ambitious mobile governance project on December 10, 2014. It is the first of its kind in the country. M-One will act as a single window to 637 services offered by the government, both central and state. More importantly, it will link the consumer to 3 644 private services at one touch.[16] The platform has a voice portal that can be accessed through any phone- landline or mobile- and also via computers, laptops and tablets.

The mobile app allows citizens to pay utility bills for electricity, pay property taxes, apply for a host of permits such as driving licences or passports, pay traffic violation penalties, book tickets on rail and road transport, etc. People can even lodge complaints with civil authorities, and the government is considering a women's safety app. Over 3 500 services related to healthcare and transport are also available.

M-One allows citizens to access many of these services even without a smart phone. The platform has a voice portal that can be accessed through any phone- landline or mobile- and also via computers, laptops and tablets. Consumers can call in and work through the interactive voice response system, send SMS messages, or use the services via the smart phone app for Android or Apple devices. All local languages and English will work. The project was devised by Karnataka's e-governance department in January 2013, with a goal of ensuring that "whatever is accessible on the computer to the urbanite will now be available to everyone, including those in remote areas and those who are travelling, at their fingertips."

Mobile phone penetration in India, according to a June survey by TRAI,[17] the telecommunication regulator, is 942.9 million. In Karnataka, 55 million of the 64 million people own mobile phones. This is far more than the personal computer penetration rate, which is an estimated 10 per cent of India's 1.25 billion population. Karnataka is working on integrating a pre-paid mobile wallet into the app, which will allow citizens to pay for any services, including utility bills and taxes.

Undeniably, markets continue to become more complex. Mobile network operators (MNOs) have become the custodians of sensitive data within the digital ecosystem, and this has raised privacy concerns related to consumers' use of mobile technology.[18] Are consumers able to make informed decisions about their information and privacy? Can they ensure that their privacy is respected and protected by those designing and building mobile applications? There are valid concerns about whether consumers are able to make informed choices in an increasingly complex marketplace.

M-services and apps are increasingly vulnerable to security concerns. Networks worldwide are falling victim to hacking by cyber criminals. Cases of fraud, misuse of data and use of mobile phones to commit crimes are all on the increase, undermining trust and confidence in the digital ecosystem.

These concerns raise weighty issues and call for a thoughtful consideration of policy and regulatory action going forward. While there is a need to protect personal freedoms, it is important to do it in a way that does not hamper innovation. It is important to uphold trust and confidence in the digital ecosystem and take active steps to mitigate the emerging concerns. Regulators need to consider whether their policy and regulatory frameworks are fit for purpose, in order to achieve a delicate balance for m-services and apps to thrive within the digital economy.

5.3 Policy and regulatory perspectives

This section of the chapter seeks to highlight policy and regulatory perspectives to be considered in promoting growth of m-services and apps, while at the same time ensuring that innovation is not stifled and that consumer benefits are maximized. In doing so, this section will identify critical regulatory principles that should be addressed and will offer perspectives for leveraging the anticipated benefits against the risks. The perspectives shared in this section will contribute to a series of critical questions that policy-makers and regulators can use as a guide in considering proposals to foster m-services and apps.

5.3.1 Goals of regulation

Most information and communications technology (ICT) regulatory frameworks were designed to guide structural changes as the sector transitioned from monopoly to competition. Regulations then were maintained to promote effective competition and foster the long-term development of the ICT market.[19] In recent years, the sector has undergone structural changes in response to convergence and innovation, and it needs to be flexible enough to accommodate further change and review. As Figure 5.1 illustrates, regulation is not intended to serve as an end in itself.

While the conventional regulatory framework is necessary to resolve disputes, address competition concerns, protect consumers, and attain national goals such as universal access and economic development, it can also become a bottleneck to innovation and investment if it fails to respond to the issues of the day. The need to adopt regulatory mechanisms within a cross-sectoral framework is a critical interdependency for m-services and applications. However, this was not anticipated within the conventional, "silo" style of enacting regulations. There must be a paradigm shift to permit a new way of doing things.

The first step is to identify the objective of regulation before articulating a framework to achieve that objective. The regulatory approach to be used is equally important once the object of regulation has been identified. In the early stages of competitive markets, the approach was to prescribe rules, rights and obligations. However, the general evolution has been toward a "light-touch" approach to encourage and foster m-services and applications by giving room to embrace ideas that were not anticipated earlier.

The evolution of the M-Pesa mobile money transfer service is a classic case in illustrating how a paradigm shift was needed to overcome traditional regulatory arrangements in order to enable the entry of an innovative m-service (See Box 5.3). Cross-sectoral forbearance was applied to deal with an innovation that was not anticipated and hence not accommodated by either the telecommunication or financial regulations that it straddled. The solution was a light-touch regulatory approach, a gradual introduction of payment-system regulation for better financial oversight, all combined with requirements for interoperability between the Safaricom network with the other networks, to foster competition.

Figure 5.1 Regulatory Goals

Source: Telecommunications Management Group, Inc.

5.3.2 To license or to exempt?

The regulatory goals being pursued have a direct bearing on the licensing approach that is adopted. Previously, regulators employed rigid service- and technology-specific licences that were often installed as an administrative catchment for revenue. Regulators now are encouraged to adopt more flexible licensing regimes, in order to accommodate technological and market changes. The convergence achieved within the digital ecosystem has eroded bright lines in the traditional licensing regimes, requiring a move away from technology- and service-specific licences and toward a unified authorization regime, or even to simple notifications, to promote the ease of doing business.[20] The licence or notification is retained to maintain regulatory accountability without being a barrier to new innovations.

Maintaining the traditional licensing regime, meanwhile, would require an MNO not only to obtain a licence to operate mobile services, but also a value-added services licence for each and every m-service and app operating on its network. Having to obtain licences from healthcare, education, financial and agricultural regulators, among others, would not only be highly cumbersome, it would severely restrict the diffusion of m-services and apps. Regulators, therefore, need to review regularly their licensing practices and approaches with a focus on identifying and removing potential barriers.

5.3.3 Competition for consumer benefit

New technical capabilities made possible by IP-based broadband networks have given rise to new entrants competing in traditional markets. They bring new business models and completely different cost structures than traditional providers employ. New technologies and upgraded networks also have enabled the introduction of a wide variety of new services and applications. What are the impacts of these changes on the competitive environment?

The emerging scenario introduces regulatory complexity and the need to address several principles that are critical in promotion of competition.[21] These questions are particularly valid in a market with dominant operators that can skew the market and abuse their dominant positions, to the detriment of their competitors and customer bases. As mobile markets continue to become more competitive, regulators should be alert for the many ways in which dominant operators can engage in anticompetitive behavior (*e.g.*, predatory pricing, cross-subsidization, price

Box 5.3: M-Pesa

Developed in Kenya, M-Pesa is one of the world's most successful mobile money transfer services. It was launched in 2007 by Safaricom, Kenya's largest MNO. Through it, millions of people with access to a mobile phone – but with limited or no access to a bank account – can send and receive money, top-up airtime and make bill payments.

Customers register for the service at an authorized agent. This is often a small mobile phone store or retailer. The customer deposits cash in exchange for electronic money, which they can send to their family or friends. Once they have registered, all transactions are completed securely by entering a PIN number, and both parties receive an SMS confirming the amount that has been transferred. The recipient, who does not have to use the same network, receives the electronic money in real-time and then redeems it for cash by visiting another agent.

There are several mobile money schemes established worldwide. Why has M-Pesa been the most successful? The financial sector regulator, Central Bank of Kenya (CBK), the telecommunication Regulator (then CCK, now the Communications Authority of Kenya or CA) and the Ministry of Finance conducted a due-diligence assessment of the risks before commissioning the project. CBK put in place minimum standards to promote trust and confidence in the payment system and promote consumer welfare. It also gave a special licence to Safaricom that contained less stringent conditions than licences given to banks and other financial institutions.

The regulators' initial decision to allow the scheme to proceed on an experimental basis without a formalized regulatory framework was the root of this success. Regulatory forbearance allowed innovation to thrive without being "boxed in" by conventional practices. Having established a base of initial users, M-Pesa enjoyed the network effects of being hosted by the largest MNO. The more people signed up for it, the more it made sense for others to do so.

While regulatory forbearance was exercised in the inception stages in order to encourage innovation and uptake, a measure of formal oversight has been adopted over time to monitor payment systems and to prescribe anti-money-laundering measures. The *National Payment Systems Regulations* became law in August 2014.

On the telecommunication side, the M-Pesa agency system initially operated within the Safaricom network only, but it's now interoperable with other networks. The accommodation for interoperability came in the wake of a petition by Airtel to the CAK to compel Safaricom to open up its M-Pesa network.

Source: Author

discrimination, discriminatory provisioning of network facilities, overpricing of essential facilities and other network elements and services provided to competitors, unfair trade practices, tie-in sales, and anticompetitive bundling).

One of the more likely outcomes is that an m-service or app that rides on a large network will ultimately benefit from network effects, much to the discomfort of other operators in the same market. This happened in Kenya when Airtel Money, which operates the second-biggest mobile money platform in Kenya, petitioned the Competition Authority of Kenya (CAK) to investigate Safaricom for alleged abuse of its position as the market leader in M-commerce.[22]

Airtel Kenya had claimed that Safaricom's charges for customers to send money to Airtel Money accounts were double the amount Safaricom charged to send money to its own customers. Airtel Kenya also wanted Safaricom to allow M-Pesa agents to deal with other agents like Yu money, Airtel money and Mobikash.[23] In a demonstration of regulation in a multi-sectoral space (and of regulatory forbearance), the CAK deferred the issue to the Central Bank of Kenya (CBK) Communications Authority of Kenya (CA).

In July 2014, the CA ordered Safaricom to allow its mobile money agents to also operate with other platforms. The CA further recommended that the CBK handle the petition on M-Pesa tariffs, as these were charges for financial services.[24] The M-Pesa agency system initially operated within the Safaricom network only, but now is interoperable with other networks.

The scenario just described raises several issues for regulators to consider when attempting to foster diffusion of m-services and apps. It indicates that assessment of competition concerns in the digital economy requires an in-depth investigation to evaluate the "pain point" being raised. It is clear that a restrictive arrangement does arise when an m-service is locked into an MNO or when an app is locked into a single operating system. This has the potential to raise competition concerns. The lock-in effect has spurred discussions about platform agnosticism and the creation of open mobile apps. This related to a desire to see free sharing of apps on the mass market, in order to achieve critical development goals in fields such as m-learning, as well to use commercial resources in order to achieve development goals.[25]

Some of these issues can be clarified through asking questions such as these:

- Are the regulatory arrangements for infrastructure-sharing adequate to achieve goals for national access?
- Are the exclusive arrangements governing m-services and apps riding on MNOs and operating systems raising competition concerns?
- What is the impact of these exclusive arrangements on pricing? Are the tariffs fair and non-discriminative?
- Have all relevant stakeholders in this issue been identified and consulted widely for input?

Answers to these questions will guide appropriate regulatory interventions to avoid entrenching anti-competitive market features. Particularly important are considerations of pricing, as the cost of sending a text message or purchasing an app ultimately will determine the affordability and access to the m-service or app. Regulators must ensure that the interconnection framework is clearly defined and that interconnection charges are based on objective, economically sound, and solidly substantiated costs.

It is also apparent that in aiming for a robust competitive environment, the telecommunication construct for competition regulation may be inadequate. It is incumbent on regulators to set appropriate safeguards and then to intervene to leverage opportunities in the digital ecosystem. Introduction of number portability, interoperability and infrastructure-sharing are other mechanisms that could also be considered. These safeguards will be discussed later in this chapter.

5.3.4 Stimulating demand – universal access

The network reach and intelligence to support access to m-services and apps remains on the regulator's radar now, more than ever before. The urgency to bridge access gaps compels new ideas and creativity in order to identify optimal strategies for achievement of universal service.

Traditionally, efforts to address access gaps were directed at deployment and improvement of telecommunication infrastructure – but only within access networks. Today, a more integrated, multi-sectoral approach is needed. Networks still have to be expanded to include broadband capabilities, but a broader approach will stimulate the development of content that is relevant in context and language. This is the way to foster the development of m-services and apps.[26]

National broadband plans can no longer call for deliverables within just the telecommunication sector. The roll-out of mobile networks and broadband capacity needs to be seen in a holistic way, looking beyond the ICT sector's horizon, in order to include other actors in the broadband ecosystem and allow them to contribute to universal access.[27] This will avoid vertical, "silo" interventions and enable the identification of where m-services and apps can plug in, in an integrated and interoperable manner, with existing systems and solutions.

This holistic approach would include financing mechanisms to accommodate local content development, application development, development of assistive technologies, incubation, scaling and monetization. It would also prompt a radical re-thinking around the nature of universal service obligations imposed on service providers.[28]

The Broadband Commission has set ambitious goals to make broadband access universal, in order to drive prices down and make services affordable.[29] International commitments such as this prompt regulators to adopt urgency in articulating an integrated, national approach. There is no one-size-fits-all solution. Each country must quantify the unique hurdles to be overcome and the resources and investment required to overcome them. Each country must develop a comprehensive plan at the national level to address its universal access gaps.

In the health sector, for example, different countries have adopted varied focus points in the development of m-health applications, in response to the health needs of their populations. In some cases, the m-services and applications are accessed through the Internet while in others, it is through SMS. There are different categories of m-health services and apps, including data collection; disease surveillance; treatment adherence reminders; emergency medical response systems; support to health care professionals or rural health workers; supply chain management; health financing; disease prevention and health promotion.[30]

The continual review of universal access policies and mechanisms is necessary in order to establish and maintain a universal service framework that will achieve public policy objectives of availability, affordability and accessibility of services in a fast-converging sector. Strategies to embed diverse innovative mechanisms, such as public-private partnerships and multi-stakeholder projects, in the design of universal access policies will be crucial for them to remain agile and responsive to ever-changing demands.[31]

5.3.5 Pressure for resources

Meanwhile, regulators must contend with growing demand for the resources that underpin mobile

Box 5.4: "m-cessation" (m-health for smoking cessation)

A project was launched in Costa Rica in April 2013 to prevent smoking-related diseases such as cancer and other lung diseases. Tobacco smoking had been recognized as a big problem in Costa Rica, and many health costs were considered preventable if individuals would quit smoking.

The project included building and maintaining a database of mobile numbers based on a registration process, creating tailor-made short messages and developing two-way communication with smokers. A mechanism for feedback and reporting management was established at the Ministry of Health to support the project.

Source: M-Powering Development Initiative services and apps, including radio-frequency spectrum and addressing resources.

5.3.5.1 Spectrum

All wireless communications require radio spectrum. New entrants have made their way into the sector by leveraging new spectrum access methods and new business models.[32] As a result, there is a proliferation of m-services and applications, which adds pressure on regulators to free up access to more spectrum for broadband wireless network access. Both licensed and unlicensed spectrum is needed to support the digital ecosystem.[33]

How should regulators respond to this pressure? At this point the primary regulatory objectives will be threefold: (1) to ensure availability of adequate spectrum to accommodate the increasing number of apps and m-services being delivered over mobile or WiFi networks; (2) to avoid erecting barriers on pricing or even competition; and (3) most importantly, to ensure that existing spectrum policies can help create an environment for innovators to use spectrum as a resource for new technological goods and services.[34]

5.3.5.2 Incumbents versus new entrants

Legacy systems continue to pose roadblocks on the way to innovation. One of these barriers is the legacy method of spectrum allocation, which prescribes exclusive use and a high cost of access. This barrier to market entry and growth often blocks innovation. Existing players tend not to be interested in disruptive ideas, especially if there is a threat to their revenues and profitability. Policy-makers need to adopt transformative approaches to guide future spectrum policy development and encourage incremental innovation.[35] It will be important to provide a transparent, market-based mechanism for spectrum access and to eliminate any service and technology restrictions that may have been part of spectrum licences in the past. Those restrictions may not be valid within a converged environment and may restrict the emerging, innovative ways that the spectrum can be put to use.

In an effort to find solutions to share existing spectrum, it is prudent to consider new, flexible approaches to spectrum licensing (or within a licence-exempt framework). In fact, some old certainties and assignment methods that were based on clear lines between licensed and license-exempt frameworks are beginning to blur – with potentially uncertain results.

Perhaps more can be done at a spectrum policy level to provide a wider range of spectrum products.36 One idea is to enable a "staircase" of spectrum access, matching levels of spectrum access to diverse needs and funding constraints. This may, in turn, introduce spectrum access methods that allow low- to no-cost access to spectrum, reduce barriers to entry and foster more flexible methods of allocating, clearing, using and/or sharing spectrum.[37] Additionally, database and sensing technologies are also driving opportunistic sharing, challenging current licensing conventions.[38]

The momentum around Dynamic Spectrum Access (DSA) technology continues to gather, and in most cases, it is initially targeted at the white spaces in TV spectrum. DSA is an efficient and optimized technique of using under-utilized frequency bands to improve the way wireless devices access spectrum resources. In TV broadcast spectrum, for example, under-utilized channels-- known as TV white spaces-- can be used to extend bandwidth capacity for wireless devices.

Singapore, was one of the very early adopters of DSA technology in its search for more bandwidth to meet the need for more connectivity. There are several ongoing commercial trials and pilots worldwide – in the UK, Philippines, Ghana, Kenya, Botswana and Namibia, to name a few. In Africa, Microsoft has exclusively focused on demonstrating the technical feasibility of using TV white space technology to extend affordable Internet in under-served areas, using solar power in off-grid areas.[39]

Perspectives are not fully settled on adoption of new spectrum access methods such as DSA. While they have been deployed commercially in some countries, others have adopted a cautious approach. Going forward, regulators will engage in a cost-benefit analysis between (1) using innovative means for spectrum access to bridge the digital divide and obtain national coverage and (2) the implications of adopting a fixed or variable (dynamic) power-level approach when it comes to TV White Space regulation.

5.3.5.3 Numbering and addressing resources

Every mobile device connected to the Internet requires a unique "IP address" to route data packets globally across the web. The current addressing system, called IP version 4 (IPv4), was deployed on 1 January 1983 and uses 32 digital bits to represent addresses, generating a theoretical total limit of 4.3 billion addresses. Given the significant growth of connections, numbering ranges will soon be in short supply,[40] requiring the transition to IPv6.[41] Regulators must anticipate the needs for huge quantities of numbering and addressing resources with the advent of the digital age, and provide those resources in advance.

5.3.6 Protecting the Consumer

The explosion of mobile services and apps has created tremendous choices for consumers, who can now use services from a variety of providers. These changes have come in the wake of disruption of the old regulatory constructs, creating a complex landscape for the consumer to maneuver through. Regulators have a responsibility to create consumer awareness and act as custodians for the consumer, ensuring compliance with regulatory standards such as quality of service.

5.3.6.1 Quality of service

Consumers are continually seeking enhanced user experiences online. High broadband upload rates facilitate a collaborative online environment by encouraging user contributions, while high download rates enhance the accessibility of content. High bit-transfer rates enable interactive functions such as real-time feedback and video calling. Some services like telemedicine and e-learning require access at up to 100 Mbit/s, while standard applications such as email and web browsing can function with speeds as low as 0.5 Mbit/s.

Evolving consumer needs demand higher speeds and reliable quality of service in order to ensure the secure transmission of sensitive data, such as for m–banking and m-health services, across networks and borders. The rise in consumer needs is prompting the re-definition of public policy goals for universal service from basic voice to include Internet access[42] or broadband.[43] The quality of service on a wireless connection will depend on other uses of the same access network and the backhaul capacity from the relevant base station to the core network. The need to uphold high quality of service is critical in order to achieve seamless connectivity and optimal traffic management.

5.3.6.2 Compliance and Enforcement

The success of regulatory initiatives depends entirely on achieving compliance thresholds for various regulatory parameters: quality of service, type approval, licensing, network rollout obligations, competition, consumer protection, etc. The planning, compliance, monitoring and enforcement functions, therefore, constitute critical success drivers within the digital ecosystem.

5.3.6.3 Promoting choice

Regulators have at their disposal certain mechanisms – both old and new – to employ in order to promote consumer choice and competition. Consumers' ability to choose one service provider over and to transition effectively is a hallmark of consumer enablement. Earlier consumer-protection efforts tended to focus on providing adequate information on service descriptions, prices and complaint mechanisms. The digital ecosystem presents new opportunities and, alongside them, significant threats.

New concerns have arisen on the asymmetry of information between those who hold data and those who unintentionally or inadvertently supply it. It is therefore imperative for a consumer to be well aware of privacy and data protection concerns arising from the treatment and management of consumer information. Consumers are key stakeholders, and they usually are open to the benefits of innovation. They can be useful in upholding performance within the digital ecosystem if they are aware of their rights and obligations, as well as those of other pertinent parties.

5.3.6.4 Dealing with lock-in arrangements

Today, regulators need to respond to situations in which service providers may try to lock in customers by imposing long-term contracts with their customers, forcing them to pay termination fees to change service providers. Other consumers may be locked-in because the m-services they like are offered by the service provider only to its own customers (see the Safaricom and M-Pesa situation discussed earlier). This makes it difficult for consumers to move their data and information from one provider to another.

Such practices raise consumer-protection and competition concerns. While it is incumbent on consumers to make informed decisions when signing up with a service provider, it is equally important that consumers be able to switch providers. Responding to these concerns, the EU modified its *Universal Service Directive* in 2009 to require member states to limit customer contracts to no more than 24 months and to direct operators also to offer 12-month contracts.[45]

5.3.6.5 Number portability

Mobile telephony has re-defined *connectedness* to the point that calling a person is really calling a number, because people and businesses become closely associated with their phone numbers. Number portability, therefore, is a huge consumer and competition consideration in providing consumer choice. Porting allows more consumer choice and enables individuals to move their number together with any m-services and apps that are tagged onto that number.

5.3.6.6 Standards and interoperability

From traditional mobile voice services to m-health, m-education, m-agriculture, m-payments, m-investment and m-donations, it is clear that we are now in the era of m-everything! The ability to interoperate and interconnect devices so they can "speak" to one another continues to herald numerous possibilities.[46]

The proliferation of platforms, applications and services that cater to specific devices, however, can create isolated islands of device ecosystems in the absence of full interoperability across multiple operating systems.[47] There is a critical need to lift traditional barriers that operators have imposed to further their proprietary technologies and to lock in commercial gain. Further, the adoption of common standards and interoperability sets the stage for scaling and monetization of m-services and apps, allowing for cheaper access, allocation of benefits to broader segments of the population, and achievement of development goals.

One of the critical pillars in driving a digital agenda is improved standard-setting procedures and increased interoperability. Legacy type-approval processes need to be reviewed in order to assure an expanded space for mutual recognition through type acceptance. European public authorities are particularly active in promoting interoperability.[48] Showing a commitment to this critical success factor, the Digital Agenda for Europe requires that all new IT devices, applications, data repositories and services interact seamlessly anywhere – just like the Internet.[49] The *Digital Agenda* identifies improved standard-setting procedures and increased interoperability as the keys to success.

Many governments and regulators promote interoperability and open systems by enforcing anti-trust regulations and adopting open-source software and open standards in their own digital activities.[50] French legislation, for example, mandates that when digital content is protected by proprietary digital rights management technologies, providers must give other software and hardware developers access to the necessary technical documentation to make their systems interoperable. For this reason, Apple's iTunes is under scrutiny both in France and elsewhere in the EU.[51]

The idea of fostering interoperability can be controversial, because it seemingly proposes cooperation among competitors.[52] It suggests trade-offs that must be faced on the road to universal interoperability.[53] Indeed, some forms of interoperability have often received equivocal support, leading to uncertainty about the strength of governments' commitments to fostering competitiveness in the digital ecosystem and the aim of growing the "knowledge economy." [54]

In June 2014, Tanzanian MNOs became the first in Africa to enter into an interoperable mobile money pact.[55] This was achieved following months of negotiation and regulatory facilitation to reach "interconnection" arrangements akin to those typically used for voice calling and text messaging. This agreement will enable customers to send and receive money across networks, and the e-money will go directly to the respective subscribers' e-wallet accounts.

5.3.6.7 Accessibility standards for persons with disabilities

According to the *World Report on Disability,* produced jointly by the World Health Organization and the World Bank, more than 1 billion people in the world today experience disability in one form or another.[56] This statistic represents about one-seventh of the earth's inhabitants. As of September 2015, the *Convention on the Rights of Persons with Disabilities* (CRPD) had 159 signatories and 157 parties, making the Convention the fastest-negotiated human rights treaty in the history of the UN.[57] Article 9 of this Convention articulates the need to ensure access to ICTs, including the Internet, for persons with disabilities. This commitment gains a new prominence in the context of emerging m-services and applications and their linkage to services such as health, education and banking. The mobile apps trend underlines the need for a policy priority to enable people with disabilities to overcome ICT access barriers and to build-in accessibility as a feature of networks, systems and policies.[58]

Implementation of the CRPD treaty commitments at the national level will entail articulating domestic public policies to achieve minimum accessibility standards and guidelines for services provided to the public.[59] It will also lead to development of accessibility and assistive-technology standards for mobile products and services, ensuring greater interoperability in order to increase the availability of cheaper assistive technologies, products and services.

5.3.7 Infrastructure sharing

The reach of an MNO network has in the past largely determined its profitability and even its market dominance. Not surprisingly, then, incumbent operators have often resisted efforts to encourage infrastructure-sharing and maintained efforts to keep their competitive advantage over newer entrants. But preserving infrastructure silos means that some consumers cannot access m-services and apps not hosted on their service providers' networks.

One of the innovative regulatory approaches to address this would be to mandate infrastructure-sharing as a way to broaden the geographical reach of MNO networks and in this way enlarge the platform on which m-services and apps can ride. This innovative approach would resonate particularly in the developing world, as it would enable m-services and apps to reach remote and uneconomical areas faster. It would also enable the implementation of national broadband plans and network upgrades. In this way, ICT infrastructure would be optimized as a utility for provision of m-services and apps by all sectors such as education, health, sport, transport and agricultural support.[60]

5.3.8 Trust and confidence

A lack of trust and confidence can act as a major barrier to growth in a data-driven economy. Regulators should instigate an increase in consumer protection by encouraging MNOs to enhance the security of their networks through adoption of encryption technologies. This is a critical requirement to ensure that sensitive data being transferred over the network (for example, mobile payments) is transmitted securely and seamlessly.[61]

Robust security measures are, therefore, critical for the whole value chain, including device and chip manufacturers as well as software vendors. Reducing vulnerabilities in devices, applications and web services should be a priority for everyone in the digital ecosystem.[62] Trust and confidence in ICT security and privacy is recognized as one of the main pillars of the Information Society.[63]

More and more, regulators are being called upon to respond to numerous public security concerns or "mobile menaces" involving serious crimes--kidnapping, terrorism, drug trafficking and money laundering-- committed using mobile phones. This calls for regulatory action to preserve the integrity and reputation of mobile services as safe for society and consumers to use. Kenya, for example, dealt with such concerns through legislation mandating that MNOs keep details of individuals who subscribe to their services.[64]

In this light, the development of comprehensive privacy and data-protection legislation at the domestic level becomes vital, and regulators should play a key role in shaping this going forward. The security and privacy of peoples' personal information, however, remains a challenge due to a patchwork of geographically bound privacy regulations.

5.3.9 Regulating in a multi-sectoral environment

It is clear that ICT sector regulators cannot claim exclusive and total scrutiny and authority in an environment that is fast converging and integrating to create a new landscape. The reality is that multiple agencies will need to address mutual and overlapping issues. They all will have to offer their expertise and give greater visibility and commitment to digital inclusion. The telecommunication sector regulator will need to reach out to other regulators in collaboration and partnership-- this is the new normal.

5.3.9.1 The emergence of stakeholder diversity

The m-service and app ecosystem works on different business models and is capable of attracting any number of users. So, regulators should be careful to identify all the stakeholders involved in any issue, on a case-by-case basis. The cross-sectoral effect of many of these issues will bring in a broad array of stakeholders and "influencers," ranging from midwives and teachers in rural areas (for m-health and m-education services and apps) to hardware and software developers or city residents (for m-transport and smart metering services and apps). The content and context of each m-service and app will attract a unique range of stakeholders as broad as the capability of the service or app. All of these stakeholders will want to influence regulatory outcomes.

Stakeholder engagement assumes a new prominence in a cross-sectoral environment. The ICT regulators need to create awareness in order to spark interest in commercial deployment of m-services and apps. More than ever before, regulators must consult within a multi-stakeholder framework and seek feedback, communicate effectively and recognize the aspirations of stakeholders in order to foster the spread of m-services and apps. Box 5.5 illustrates how a broad range of stakeholders can be involved in developing and using an m-health service.

Emerging trends point toward more cross-sector collaboration and partnership in order to handle the multiple issues to be reconciled. It is also clear that for the digital ecosystem to thrive, all key stakeholders must pull together in order to reap the benefits in a fast-evolving sector. The continuous identification, mapping and engagement of stakeholders become important because of the characteristically short time frames within which to make gains and the cross-sectoral scanning for stakeholders.

Due to the disruptive nature of the digital economy, ICT sector regulators often will be presented with issues that, while pertinent, are not in their area of expertise. The development of m-banking, m-agriculture, m-health etc. means that the intimate interface between the ICT sector and another, specialized sector can lead to dual jurisdiction on some issues.

5.3.9.2 Collaboration across sectors

Regulators have adopted many approaches to handle issues of shared jurisdiction. Often, these scenarios arise from innovative initiatives and so may not have been anticipated or formally authorized. For example, there was no formal platform for collaboration between the CBK and the CCK during the M-Pesa deliberations in Kenya. The absence of a formal arrangement should not deter best efforts to collaborate, particularly when the parties recognize an idea whose time has come. Steps can be taken later to formalize the collaboration.

In order to collaborate with a third party, regulators must be clear about the powers they have under the law, in order to determine the limits of that collaboration. All parties should be clear about their mutual strengths, which are determined by their legal mandates, so they can be sure what their roles will be in conducting their collaboration. ICT regulators already have pursued collaborations with competition authorities and financial regulators, and a lot more work with other sectors is likely as m-services and apps continue to permeate all areas of life.

Going forward, regulators should commit proactively to seeking out opportunities to work with each other. Collaboration is not driven merely by the need to facilitate an innovative idea, but more structurally, to identify gaps or barriers to innovation and bridge them to benefit the whole digital ecosystem. The following sub-sections

Box 5.5: Bhutan Epilepsy Project

In the deep, remote valleys of the Kingdom of Bhutan, a small country in South Asia bordered by China, India, Nepal and Bangladesh, a boy pulls onto his head a plastic headset that looks like a shower cap. This is how the boy will be diagnosed with epilepsy, using fast-growing mobile health technology to bring improved medical care to under-served parts of the world. The readings will be taken through the headset using a new cellphone application.

Just how under- served is Bhutan? It does not have a single neurologist, nor does it have any technology to diagnose epilepsy, one of the most common neurological disorders (and one easily treated with medication). With a population of 730,000, Bhutan faces a high burden of epilepsy (estimated at 1 out of 1 000 people). Most Bhutanese live in rural, mountainous villages, preventing them from receiving trained help for seizure disorders.

What are the telecom statistics in Bhutan like? Despite living in rural areas, the Bhutanese are extremely well connected. More than 90 per cent own a cell phone, making the country an ideal setting for the Bhutan Epilepsy Project. It is analyzing the mobile electroencephalography, or EEG, of patients rather than the stationary EEG technology, which is the standard epilepsy diagnostic tool in American hospitals.

The long-term goal of the project is to train the Bhutanese research coordinators to become more skilled at employing EEGs themselves. Another goal is to encourage the Bhutanese to communicate with hospitals and health facilities in other places through the use of simple text and personalized messaging.

Source: The Boston Globe, May 22, 2015[65]

Stakeholders

Government	Mobile Network Operators
Hardware and software vendors	M-Health project team
Project funders	Health care professionals and associations
Medical doctors	Psychiatrists
Neurologists	Nurses
Community workers / educators etc.	Data Readers
Programmers	NGOs
Child rights activists	Patients
Parents/Guardians (for minors and patients who lack capacity)	Regulatory authorities
ICT Ministries / regulators	Healthcare Ministries / regulators
Ministries handling social services	UN Specialized bodies
ITU	WHO
UNICEF	UNESCO
Application developers	Developers of healthcare related content
Media	Others

Source: M-Powering Development Initiative Report 2015 at page 4[66].

illustrate areas of potential collaboration in the interest of sustainability and the achievement of development goals.

5.3.9.3 Collaboration to enable availability of big data

"Big data" continues to transform the way we live and work, altering the relationships between government, citizens, businesses, and consumers. Public policy can set a platform for the public and private sectors to maximize the benefits of big data while minimizing its risks. Ideally, public policy should identify opportunities for big data to grow economies and promote the development of scalable, replicable and commercially sustainable mobile applications and services.

However, it has not been possible to seize such opportunities in some countries due to policy gaps. For example, in some countries, meteorological departments have blocked MNOs from using private weather information, reinforcing government monopolies on this type of information. This kind of barrier hinders the uptake and value propositions of some commercial services and apps, including for agriculture solutions.[67] Regulators could consider partnering to unlock opportunities with development potential and to leverage the widespread use and availability of mobile networks and services.

5.3.9.4 Collaboration to enable protection of intellectual property rights

In the digital economy, copyright law continues to perform the critical function of encouraging new creative work. But it also has a wider impact, playing a significant role in fostering innovation.[68] The impact of copyright is therefore now much wider than the creative industry alone. Digital technologies, the companies that exploit them and the business models they facilitate are all potentially impacted by copyright.

Endemic copyright infringement facilitated by broadband infrastructure has drawn the MNOs and Internet communities into a debate on intellectual property rights (IPRs). The film, music, software, publishing and television industries are putting pressure on communication regulators to more actively address copyright infringement by companies and consumers. Yet, at the same time, regulators must encourage investment and service innovation within the digital economy.[69] The ICT sector regulator needs to ensure that there is a balanced, proportionate and robust mechanism for players in the digital economy to flourish, so that societal benefits can be realized.

IPR issues commonly fall outside the mandate of the ICT regulator. Pursuing partnerships with IP regulators will be mutually beneficial in efforts to encourage development of relevant digital content and in fostering an open and competitive digital environment.

5.3.9.5 Collaboration for optimal taxation

MNOs are significant contributors to national economies, and they do stimulate activities in the wider economy, further boosting GDP. A range of taxes are levied on MNOs and consumers, such as excise duties on mobile handsets, sales taxes on airtime usage, and revenue share levies on mobile operators. These taxes contribute to a high tax burden, which can prevent consumer take-up of mobile services, discourage consumer usage and hinder investment in networks and services.

According to the ITU, although telecommunication/ICT sector tax revenues play an important role in supporting national public services, this role must be weighed against the potentially adverse effects that over-taxation can bring to the growth of the telecommunication/ICT sector, broadband penetration, and national economic growth.[70] In this regard, the European Commission High Level Expert Group on Taxation of the Digital Economy has examined the best ways of taxing the digital economy in the EU, weighing both the benefits and risks of various approaches.[71]

Adoption of an optimal taxation policy that balances government revenue needs, socio-economic development goals and international competitiveness is imperative. The impact of both direct and indirect taxation on the ICT sector remains a continuing concern for governments, businesses and consumers alike. Affordability and access to mobile services are vital, so regulators should play a key role on sector taxation matters to amplify the positive impacts from adjustment of tax rates.

In Kenya, the removal of a 16 per cent value-added tax (VAT) on mobile phone handsets in June 2009 boosted handset purchases by more than 200 per cent, and mobile penetration increased some 50-70 per cent. From 2009 to 2012, airtime prices fell by 70 per cent and usage of mobile services rose by 113 per cent. Through increased handset circulation, a higher share of consumers has access to high-value mobile services like m-banking, m-agriculture and m-health offerings.

5.4 Rights-based regulatory approaches and statutory recognition

This chapter charts the adoption of light-touch regulatory mechanisms to foster the diffusion of m-services and apps. It is important, however, to note that some countries have adopted statutory pathways – a more formal approach- to define obligations for diffusion and access to m-services and apps. As previously discussed, regulatory approaches are not uniform, and countries have the freedom to address their own unique circumstances as they deem best. This aspect is important because in such situations, m-services and apps are fostered through mandatory requirements in response to unique national circumstances.

The trend toward rights-based regulatory approaches has been driven by the social inclusion theory. In recent times, this theory has inspired legal challenges that have confirmed that Internet and broadband access are basic human rights.[72] This is the view that all people, including persons with disabilities, must be able to access the Internet in order to exercise and enjoy their rights to freedom of expression and opinion and other fundamental human rights. This imposes on governments a responsibility to ensure that Internet access is broadly available, and that countries do not unreasonably restrict an individual's access to the Internet and, therefore, to m-services and apps.[73]

Internet access is recognized as a right by the laws of several countries-- among them Costa Rica, France, Spain, Estonia, Finland and Greece. One of the benefits of this approach is that statutory recognition gives impetus to implementing Internet or broadband access plans, accelerating access to m-services and apps. While these countries are the forerunners of this rights-based approach, it remains to be seen whether other countries will follow their lead.

Some countries have used statutory pathways to push for the adoption of specific m-services and apps to meet certain public policy goals. For example, in order to help mitigate the consequences of serious road accidents across the EU, the European Commission adopted two legislative proposals in June 2013 to ensure that by October 2015, cars automatically will call emergency services when involved in serious crashes.[74] This "eCall" system automatically dials 112-- Europe's single emergency number – after an accident.[75] The Commission proposed two pieces of legislation to help create and implement the system. The proposed legislation will focus on deployment in passenger vehicles through the type-approval process.[76]

Other recent examples, such as ERA GLONASS[77] and SIMRAV,[78] indicate a growing preference for legislative fiat over voluntary approaches to introduce services into the market. ERA GLONASS in Russia stemmed from recent legislation requiring installation of monitors and in-vehicle sensors to automatically transmit location details and summon assistance via emergency cellular service.

Similarly, the Brazilian government introduced legislation to tackle the very high levels of vehicle crime in the country through a program called SIMRAV. This program will mandate installation of telematics systems in all new vehicles in Brazil. Around 25 million vehicles are anticipated to be equipped through SIMRAV by the end of 2015, and Stolen Vehicle Recovery service subscribers could exceed 2.5 million by 2013.

Regulatory approaches need to be flexible enough to respond to harmonization efforts across sectors and even geographical regions. Clear consideration is needed to ensure that the regulatory approach adopted is not a barrier to future innovation and progress. If in doubt, do not prescribe or regulate, because innovation needs time and freedom to blossom.

Box 5.6: GSR-15 Best practice guidelines to facilitate the uptake and widespread use of mobile services (m-services) and applications (apps) through targeted regulation

Regulators at the 2015 Global Symposium for Regulators (GSR-15) recognized that fourth-generation regulation based on a light-touch approach-- and promoting healthy (active and sustainable) competition, innovation, consumer protection and empowerment-- can go a long way toward responding to the dynamic transformation of ICT markets and achieving social and economic goals. The GSR-15 regulators' findings include the following:

I To stimulate demand:

- Governments can benefit from the knowledge and experience of stakeholders to draw up holistic strategies for use of m-services and apps.

- Regulators have a role to play in supporting and encouraging partnerships to facilitate the development of m-services and applications and to raise awareness of how they can help increase economic productivity.

- Governments can promote the development and distribution of appropriate digital content, including multi-language content and content in local languages.

II To facilitate availability, access and use of m-services and apps:

Regulators believe that unified rules for facilitating infrastructure deployment and open access to networks at national and regional levels can strongly contribute to stimulating the development of m-services and apps. Cooperation among all public authorities involved at the international, regional, national, and local levels is key.

The Regulators recognized the importance of:

- Designing flexible, incentive-based and market-oriented policy and regulatory frameworks with regard to spectrum allocation and assignment for mobile broadband services, to create trust and provide for the necessary conditions for these services to thrive.

- Revisiting and reviewing current Government policies to make sure that they are still valid and appropriate, and ensuring privacy and security of government, business and consumer data.

- Open and collaborative regulatory frameworks to promote the development of cross-cutting services such as m-commerce, m-banking and mobile money, as well as m-health.

- Promoting network-sharing practices in all network and value-chain layers, while maintaining healthy competition between network providers.

- Putting in place innovative, out-of-the-box measures to stimulate the take-up of services and the creation of locally-relevant apps.

- Acquiring digital skills, which are essential for the wide take-up and efficient use of m-services and apps.

III Protecting consumers and suppliers:

Regulators recognized the importance of:

- Adopting cross-sectoral regulatory frameworks to provide for consumer protection and freedom of choice, as well as the proper exercise of consumer rights.
- Educating and empowering consumers by various measures and initiatives.
- Retaining the ability to choose and switch between service providers.
- Encouraging the adoption of measures for enhancing the security of m-services and apps; creating reliable digital identities; using subscriber identification and registration to protect consumers; safeguarding consumer personal data…and promoting transparency of online communications and transactions, in particular.
- Recognizing that multi-stakeholder collaboration is essential to ensure that the rights and best interests of both consumers and suppliers are protected.
- Adopting privacy policy that includes measures to alert users and give them control over data practices.

IV Roles of ICT stakeholders:

Regulators and policy-makers should work with government agencies, private-sector and non-governmental structures to mainstream ICTs, and m-services and apps, into their national social and economic strategies and design holistic policies and regulations allowing for synergies and cross-pollination to occur between the m-services and apps economy and the other sectors.

ICT regulators should adopt targeted regulatory measures to promote the development of broadband networks and services and provide for affordable and widespread access to m-services and apps guaranteeing healthy competition. Meanwhile, regulators should also promote innovation and ensure consumer protection. Cross-border harmonization of relevant regulatory policies, as well as enhanced collaboration among national government agencies, regional and global organizations, is essential.

Source: GSR-15 Best practices guidelines, available at: *www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-Consultation.aspx*

5.5 Conclusion: setting new regulatory objectives

The emerging digital ecosystem is generating many risks and challenges for government policies, even as it presents new opportunities to create social and economic value. Just as any healthy ecosystem enables its stakeholders to interact for the benefit of all, a healthy digital ecosystem should enable investors to create economic value and deliver well-being to society. But it will be necessary to set new regulatory objectives to address the critical uncertainties present in this ecosystem.

Establishing an environment that fosters creativity and innovation, enables competition, promotes consumer choice, and fully exploits the transformative potential of digital technology means finding a delicate balance that both stimulates and protects all stakeholders. Having recognized the phenomenal opportunity that diffusion of m-services and apps represents, governments and regulators could consider seeking technical assistance from specialized agencies such as the ITU. Policy-makers need to better understand the digital landscape and evaluate their existing frameworks, in order to align them with appropriate policy and regulatory frameworks.[79]

There is no single regulatory approach to foster m-services and apps within the digital ecosystem. Countries have their own unique circumstances and different priorities. One theme running through this chapter is that ICT regulators cannot resolve all of the challenges alone. A cross-sectoral environment calls for a balanced approach in order to foster mutuality of purpose among different regulators. Meanwhile, the disruptive nature of technologies has opened up a new era, in which ICT regulators can, and should, seize the moment to influence and promote m-services and apps.

The regulatory architecture of today should build a digital future we can be proud of. More than any other period in history, governments are suited to articulate public policy that will ensure that the digital ecosystem continues to work for individual empowerment and social good. The perspectives discussed in this paper have highlighted the need for a regulatory framework that is open, forward-looking, neutral and flexible. This will allow new technologies, innovative services and new business practices to enhance market competitiveness and maximize economic opportunities.

With the changing environment, the old regulatory construct has been eroded, opening up new possibilities. Rules need to be re-written, in some instances, to accommodate the emerging realities. This chapter recognizes that regulating in a fast-changing sector is like aiming at a moving object. Regulators need an agile, flexible and adaptable approach to allow for changing technologies and markets. Overall, it seems that "light touch" nurturing of the digital economy is a safer regulatory option than overly strong intervention in most cases.

An innovative and effective regulatory environment does not develop in isolation. It needs inspiration. It needs collaboration. It needs diverse opinions from multiple perspectives to challenge a good idea and transform it into a great one.

List of acronyms

App	Application
CA	Communications Authority
CAK	Competition Authority of Kenya
CBK	Central Bank of Kenya
CCK	Communications Commission of Kenya
DSA	Dynamic Spectrum Access
DRM	Digital Rights Management
EEG	Electroencephalography
EU	European Union
GDP	Gross Domestic Product
GNI	Gross National Income
GPS	Global Positioning System
GSMA	GSM Association
HIV/AIDS	Human immunodeficiency virus infection and acquired immune deficiency syndrome
ICT	Information and communication technology
IDA	Infocomm Development Authority of Singapore
IP	Internet Protocol
ITU	International Telecommunication Union
IPR	Intellectual Property Rights
IFI	International Financial Institution
MDG	Millennium Development Goal
M-services	Mobile services
MNO	Mobile Network Operator
OECD	Organization for Economic Co-operation and Development
SDG	Sustainable Development Goals
SMS	Short Messaging Service
TV	Television
TVWS	Television White Spaces
UHF	Ultra High Frequency
UN	United Nations
UNFPA	United Nations Population Fund
VHF	Very High Frequency
WiFI	Wireless Local Area Network
WHO	World Health Organisation
WIPO	World Intellectual Property Organization
3G,4G	Third generation, Fourth Generation

Endnotes

1 A Colombian novelist, short-story writer, screenwriter and journalist (March 1927 – 17 April 2014).

2 If you think that you are suffering from information overload then you may be right – a new study by the University of Southern California shows that everyone is bombarded by the equivalent of 174 newspapers of data a day. Further, every day the average person produces six newspapers worth of information compared with just two and a half pages 24 years ago – nearly a 200-fold increase. http://www.telegraph.co.uk/news/science/science-news/8316534/Welcome-to-the-information-age-174-newspapers-a-day.html (accessed on Feb.23, 2015).

3 Chetan Sharma, Mobile 4th Wave: Evolution of the next trillion dollars, Mobile Future Forward, September 10, 2013, Seattle at page 7.

4 See results of the United Nations Public Service Awards Winners 2014 available at : http://workspace.unpan.org/sites/Internet/Documents/2014%20UNPSA%20List%20of%20Winners.doc.pdf (Accessed on March 3, 2015).
Digital India is an initiative of the Government of India to integrate the government departments and the people of India. It aims at ensuring that government services are made available to citizens electronically by reducing paperwork. The initiative also includes a plan to connect rural areas with high-speed internet networks.

5 https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps (Accessed on May 18, 2015).

6 http://www.gsma.com/mobilefordevelopment/overview (Accessed on May 18, 2015).

7 ITU ICT Facts & Figures 2015. Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Accessed on June 2, 2015).

8 Making Mobile Phones and Services Accessible for Persons with Disabilities: A Joint Report of ITU and G3ICT, November 20111 at page 58. The Convention on the Rights of Persons with Disabilities, which came into force in May 2008, enshrines the principle that all persons with disabilities must be able to enjoy basic human rights and fundamental freedoms, one of which is the right of persons with disabilities to access information and communications technologies and systems on an equal basis with others and without discrimination.

9 Robert Frieden, "Lessons from Broadband Deployment in Canada, Japan, Korea and the United States" Telecommunications Policy 2005 at Page 9.

10 Some countries choose to have one policy for universal service and re-define universal standards to include broadband. Others have a policy for universal access and another for broadband deployment. Still others set a general target for access nationally while others differentiate from region to region. In Malaysia, for example, broadband and universal service policies are separate, and levels of access are terraced by region.

11 http://broadbandtoolkit.org/4.2.

12 United States Federal Communications Commission contribution to the 2015 Global Symposium for Regulators Consultation.

13 Measuring the Information Society Report, 2014.

14 ITU ICT Facts & Figures 2015. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

15 Big data: Seizing opportunities, preserving values, Executive Office of the President, May 2014.
https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pd (Accessed on May 13, 2015).

16 http://ibnlive.in.com/news/karnataka-launches-m-one-app-citizens-can-access-637-government-services/517116-62-129.html (Accessed on May 4, 2015).

17 http://www.trai.gov.in.

18 Big data: Opportunity or thereat? B Andrew Haire & others, GSR 2014 Discussion Paper.
Available at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Session3_GSR14-DiscussionPaper-BigData.pdf (Accessed on March 27, 2015).

19 www.ictregulationtoolkit.org /6.2.

20 http://www.ictregulationtoolkit.org/3.8.1.2 Licensing for Converged and Next Generation Networks.

21 GSR Discussion Paper (2014): Why competition matters and how to foster it in a dynamic ICT sector. Hernandez et al.
Available at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20

presentations%20-%20GSR14/Session%202%20GSR14%20-%20Discussion%20paper%20-%20Competition.pd (Accessed on May 20, 2015).

22 Safaricom ordered to open M-Pesa platform. Available at: http://www.kbc.co.ke/safaricom-ordered-to-open-m-pesa-platform/ (Accessed on June 1, 2015).

23 Ibid.

24 Ibid.

25 M-Powering Development Initiative Report 2015 at page 14. Available at: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/m-PoweringDevelopmentInitiative_Report2015.pdf (Accessed on May 28, 2015).

26 M-Powering Development Initiative Report 2015 at page xi. Available at: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/m-PoweringDevelopmentInitiative_Report2015.pdf (Accessed on May 28, 2015).

27 See example of The National Broadband Strategy for Kenya. Available at : http://ca.go.ke/images//downloads/PUBLICATIONS/NATIONAL%20BROADBAND%20STRATEGY/National%20Broadband%20Strategy.pdf (Accessed on May 18, 2015).

28 This framework should not be limited to the creation of a Universal Service Fund and should be open to other mechanisms such as internal cross-subsidies, public-private partnerships (PPPs), pay or play mechanisms, General Government Budget Contributions/Grants, Interconnection Surcharges, a municipal network alternative, and other funding approaches.

29 http://www.broadbandcommission.org/Documents/Broadband_Targets.pdf (Accessed on May 20, 2015).

30 M-Powering Development Initiative Report 2015 at page 5. Available at: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/m-PoweringDevelopmentInitiative_Report2015.pdf (Accessed on May 28, 2015).

31 See key elements to consider in development of an effective framework to address universality in GSR 2009 Background Paper, Trends in Universal Access and Service Policies by Sofie Maddens. Available at : http://www.ictregulationtoolkit.org/en/toolkit/docs/Document/3829 (Accessed on May 20, 2015).

32 The Aspen Institute, Communications and Society Program, "Spectrum as a Resource for Enabling Innovation Policy" Feb, 2013 at viii Foreword.

33 GSMA, Mobile Policy Handbook, October 2014 at page 9.

34 Ibid. at v Foreword.

35 See sample proposals from The Aspen Institute, Communications and Society Program, "Spectrum as a Resource for Enabling Innovation Policy" Feb, 2013 (Available at: http://csreports.aspeninstitute.org/documents/Spectrum-Resource-Enabling-Innovation-Policy.pdf) (Accessed on May 4, 2015).

36 Ibid.

37 One such proposal from the United States President's Council of Advisors on Science and Technology (PCAST)—published in mid-2012— PCAST recommendations was the adjustment of policy initiatives including maintaining the clearance and auctioning approach, to enable a "staircase" access to spectrum. This would allow start-ups with limited resources to initially test their ideas using an experimental license. They can then transition to early commercial service using free unlicensed access, perhaps in TV white space. Next, as business grows, they can move to shared licensed access to federal spectrum for a moderate fee. Finally, as the full potential of the business becomes clear, they can acquire spectrum at auction in a conventional manner. The range of proposals is available at: President's Council of Advisors on Science and Technology, "Realizing the full potential of government-held spectrum to spur economic growth," July 2012. Available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf. (Accessed on May 16, 2015).

38 GSR 14 Discussion Paper: New frontiers in spectrum licensing, Alden et al. Available at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Session4_GSR14-DiscussionPaper-SpectrumLicensing.pdf (Accessed on May 29, 2015).

39 Microsoft Research: Pilots & Demonstrations. Available at: http://research.microsoft.com/en-us/projects/spectrum/pilots.aspx (Accessed on June 1, 2015)

[40] IPv4 and IPv6Issues, World Telecommunications Policy Forum (May 2013) Available at: http://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ipv4-ipv6-en.pdf (Accessed on May 29, 2015).

[41] A detailed discussion on the Need for more IP addresses can be found at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR_paper_theNeedforMoreIP%20Addresses_fin.pdf.

[42] Kenya: The Kenya information and Communications (Universal Access and Service) Regulations, 2010. Accessed at: http://www.ca.go.ke/images//downloads/sector_regulations/(Universal%20Access%20and%20Services)%20Regulations,%202010.pdf on May 16, 2015.

[43] Nigeria: http://www.ijeit.com/vol%202/Issue%2012/IJEIT1412201306_22.pdf (Accessed on May 16, 2015). International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 12, June 2013 117 Sustaining Broadband Infrastructure Expansion through Universal Service Provision Fund (USPF) E. C. Arihilam, Okorie. Emeka, Nwakanma Mary N. at page 118.

[44] India: http://www.usof.gov.in/usof-cms/usof_roadmap.htm (Accessed on April 4, 2015).

[45] EU, "DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," 2009, http://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN.

[46] Your Building Has Data. What Is It Telling You? Available at: http://insights.wired.com/profiles/blogs/your-building-has-data-what-is-it-telling-you#axzz3arCbnctM (Accessed on May 22, 2015).

[47] Nakazawa & Edwards, A Bridging Framework for Universal Interoperability in Pervasive Systems at page 1. Available at: http://www.cc.gatech.edu/~keith/pubs/icdcs06-bridging.pdf (Accessed on May 22, 2015).

[48] World Economic Forum, Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015
http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf at page 5 (Accessed on May 22, 2015).

[49] Digital Agenda for Europe. Available at: http://ec.europa.eu/digital-agenda/en/our-goals/pillar-ii-interoperability-standards (Accessed on May 22, 2015).

[50] World Economic Forum, Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015
http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf at page 5 (Accessed on May 22, 2015).

[51] Ibid.

[52] See contestation in Kenya between MNOs : Airtel had petitioned the Competition Authority of Kenya () to compel Safaricom, Kenya's biggest telco to open up its M-Pesa agency network. Available at: http://www.businessdailyafrica.com/Corporate-News/Safaricom-wins-M-Pesa-charges-case/-/539550/2396726/-/v7sxibz/-/index.html (Accessed on May 22, 2015).

[53] Nakazawa & Edwards, A Bridging Framework for Universal Interoperability in Pervasive Systems at page 1. Available at: http://www.cc.gatech.edu/~keith/pubs/icdcs06-bridging.pdf (Accessed on May 22, 2015).

[54] World Economic Forum, Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015
http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf at page 5 (Accessed on May 22, 2015).

[55] http://www.theeastafrican.co.ke/business/Tanzania-telcos-in-Africa-first-interoperable-mobile-money-pact/-/2560/2337358/-/137voj6/-/index.html (Accessed on May 22, 2015).

[56] Available at: http://www.who.int/disabilities/world_report/2011/en/ (Accessed on September 18, 2015).

[57] Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=iv-15&chapter=4&lang=en (Accessed on September 18, 2015).

58 Available at: http://www.who.int/disabilities/world_report/2011/en/ at page 184 (Accessed on September 18, 2015)

59 The ITU and G3ict developed a Model ICT Accessibility Policy Report that identifies concrete steps national ICT policy-makers and regulators can take to promote ICT accessibility and transpose their CRPD commitments into national frameworks. The report is available at: http://www.itu.int/en/ITU-D/Digital-Inclusion/Pages/Reports.aspx.

60 M-Powering Development Initiative Report 2015 at page xi. Available at: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/m-PoweringDevelopmentInitiative_Report2015.pdf (Accessed on May 28, 2015).

61 GSMA Mobile Policy handbook, October 2014 at page 182.

62 GSMA, Mobile Policy Handbook, October 2014 at page 9.

63 World Summit on the Information Society, Geneva Action Plan , Action Line C5 http://www.itu.int/wsis/docs/geneva/official/poa.html (Accessed on May 12, 2015).

64 Kenya Information and Communications (Registration of SIM-Cards) Regulations, 2015. http://www.ca.go.ke/images//downloads/sector_regulations/(Registration%20of%20subscribers%20of%20Telecommunication%20services%20regulations)%20Regulations,%202012.pdf. These regulations are currently under review.

65 Available at: http://www.bostonglobe.com/business/2015/05/21/mobile-health-technology-helps-tackle-epilepsy-bhutan/c6vmO7XOznyDegIa4BYSAM/story.html (Accessed on June 3, 2015).

66 Available at: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/m-PoweringDevelopmentInitiative_Report2015.pdf (Accessed on June 3, 2015).

67 GSMA Mobile Policy Handbook at page 36.

68 GSR 2011 Discussion Paper : "Intellectual property rights in today's digital economy" by Adam Denton (Available at: https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/documents/05-Intellectual-property-E.pdf).

69 GSR 2011 Discussion Paper : "Intellectual property rights in today's digital economy" by Adam Denton (Available at: https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/documents/05-Intellectual-property-E.pdf).

70 Taxing telecommunication / ICT services: An overview (2013) Available at: http://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Taxation%20Study-final-en.pdf (Accessed on May 20, 2015).

71 2014 Report of the Commission Expert Group on Taxation of the Digital Economy. Available at: http://ec.europa.eu/taxation_customs/resources/documents/taxation/gen_info/good_governance_matters/digital/report_digital_economy.pdf (Accessed on May 9, 2015).

72 http://broadbandtoolkit.org/4.2.

73 http://muftinternet.com/policy/countries-with-right-to-internet-access-as-human-right/ (Accessed on May 18, 2015).

74 http://europa.eu/rapid/press-release_IP-13-534_en.htm, Press Release issued in Brussels on June 13, 2013.

75 The eCall system communicates the vehicle's location to emergency services, even if the driver is unconscious or unable to make a phone call. It is estimated that it could save up to 2 500 lives a year.

76 GSMA Mobile Policy handbook, October 2014 at page 11.

77 http://www.u-blox.com/en/ecall-era-glonass.html (Accessed on May 16, 2015).

78 http://www.gsma.com/connectedliving/wp-content/uploads/2012/05/m-Rodrigues-da-Luz-GSMA-LATAM-Summit-2012.pdf: (Accessed on May 16, 2015).

79 See Bhutan Project Report on Emerging Mobile Applications Opportunity June 2012, available at: http://www.itu.int/ITU-D/asp/CMS/Docs/Bhutan%20EV4.pdf (Accessed on June 2, 2015)

6 Conclusion

Midway through the 2010s, evidence points strongly to the potential for a global take-off of mobile broadband services, bringing with it expanded access to the Internet and the Digital Economy. ITU statistics indicate that the number of mobile-cellular subscriptions worldwide is approaching the number of people on Earth, which is estimated at above 7 billion-- up from just 738 million in 2000. This corresponds to a global mobile service penetration rate of 97 per cent. Meanwhile, an estimated 3.2 billion people globally are using the Internet, of which 2 billion are from developing countries.

Just to pull these two trends together, the statistics also indicate that mobile broadband is the most dynamic market segment, with a penetration reach of 47 per cent in 2015-- a value that has increased 12 times since 2007. The proportion of the population covered by a 2G mobile-cellular network grew from 58 percent in 2001 to 95 per cent in 2015. During the same period, 3G mobile-broadband coverage was extending rapidly and into the rural areas.[1]

Are we even now entering the era of the Digital Economy? If not, it is perhaps within striking distance. For this reason, this sixteenth edition of *Trends in Telecommunication Reform* has pursued the theme of "exploring regulatory incentives to achieve digital opportunities." Put another way, with the promise of an exponential leap in connectedness so tantalizingly close, what can regulators do to make sure their citizens get there – and hopefully, get there together?

Taking the Last Steps to the Digital Economy

Building up from the foundation, the first step has to be an exploration of investment and financing. Governments can set the tone for promoting investment by providing clarity on passive infrastructure-sharing rights, working with local and national governments to promote technology pilots, and supporting community broadband initiatives. They can also help new entrants by expediting licence applications and easing civil planning and construction restrictions. Governments and regulators can proactively champion pilot projects that explore disruptive technologies, such as using broadcasting (i.e "TV white-space") spectrum to promote broadband services in rural areas not considered to be commercially reachable with more traditional network approaches.

Governments can continue to fund broadband networks using public–private partnerships (PPPs) in areas where it is not commercially viable for operators themselves to invest in broadband infrastructure. Meanwhile, investment is coming from new sources. At the "macro" end of the market, new players from the global high-tech industry, such as Google, Microsoft and Facebook have invested in broadband networks and emerging technologies. They are drawn into the telecommunication market space by a desire to generate downstream revenues by leveraging increased use of broadband networks into demand for their content and services.

At a lower (perhaps even "micro") scale, innovative investments using crowdfunding, digital currencies, pension funds and charities largely involve higher-layer services (for example, development of apps and electronic games) and developed markets. This is partly due to the maturity of the Internet ecosystems in those developed markets, which foster technical innovation. But they offer new avenues, both for investors and for those who may need investment capital, to develop apps or community-based infrastructure or content.

Building infrastructure for the digital economy remains expensive. Accelerating broadband deployment, particularly outside the main urban areas, is challenging and requires innovative solutions. Governments often favour promoting infrastructure-sharing, also known as "co-investment," as a way to maximize the incentives for investors and operators to risk entering new markets. Lowering and sharing the risks of sunk costs and boosting the accessibility of networks leads to the building of more network capacity and results in lower prices for consumers.

Governments can play a key role in fostering network-sharing and spectrum "pooling" through network build-out requirements, open access mandates and less-restrictive spectrum licensing.

One possible approach is for governments to contribute assets and infrastructure, potentially through public utilities, in co-ventures with private operators. There is also real benefit in governments' providing a high degree of up-front certainty about regulatory treatment of sharing arrangements for new network build-outs.

Introducing the Digital Ecosystem

Investment and infrastructure-sharing address the basic building blocks of *connectivity*, but the true value of *connectedness* includes higher layers – beyond the network layer. True *interoperability* comprises everything from technological interconnection through data compatibility and even human and institutional connections and compatibility. At the technological level, the exchange is simply ones and zeros – electronic exchanges of signals. At the next level up, data must be framed, transmitted and decoded through a common intelligence – a common set of hardware and software that allows data to become information. Human minds, however, perform the critical function of converting information into *knowledge* within the context of inter-cultural and inter-societal interoperability. The digital ecosystem, then, assumes a holistic aspect that includes everything from basic technical interconnection up to institutional cooperation – including the work of policy-makers and regulators at local, national and even inter-governmental levels.

One of the earliest manifestations of this holistic connectivity is likely to be the *Internet of Things* (IoT), a term coined to help us understand the complexity of literally billions of devices, appliances and systems interconnected with each other – and often with the global, universal Internet. As noted in Chapter 3, Consumers will encounter IoT in everything from parking meters, thermostats, cardiac monitors, tires, roads and car components, to supermarket shelves and many other types of physical objects and appliances. IoT-enabled objects and devices can share data directly using protocols such as Wi-Fi and Bluetooth, via mobile phone networks and specialized radio networks, or over the global Internet. Device manufacturers, network operators, application platform architects and software developers are forming a broad ecosystem that is even now developing IoT services.

IoT devices will have the biggest societal impact where they are used together in larger, inter-connected, systems. At the macro-level, two of the areas of greatest IoT development and investment are:

(1) "Smart cities" – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities; and

(2) Smart power and water grids – which will see improved efficiency in the transmission of power and the monitoring and maintenance of delivery systems.

Apart from the kind of machine-to-machine (M2M) interoperability implied by the IoT, human knowledge is increasingly implicated in the profusion of digital wireless services and applications ("apps") being developed and disseminated. Conventional services such as banking, access to government services, and education are now accessible in regions where these services were either unavailable or inadequate before. Governments throughout the world-- and particularly in developing countries -- are looking to mobile platforms for innovative ways to improve the delivery of public services and to foster participation in public policy-making. The potential for economic growth, improved human connections and communication and cultural exchange – just to scratch the surface – are tremendous and exciting.

Of course, this is why the major software and computer companies around the world are so eager to become constructive players in the growth of infrastructure. The more infrastructure is built, the greater will be the global reach of their by-now nearly ubiquitous mobile services, operating systems and apps.

Clearly, a comprehensive, digitally connected ecosystem calls for holistic approaches to policy-making and regulation. One could be forgiven for paraphrasing Samuel F.B. Morse (inventor of the telegraph) and asking, "What have we wrought?" The answer is that we are daily and monthly creating nothing less than the most interconnected system of communications and knowledge-sharing in human history (along with an entire environment of interconnected machines). And there is no end in sight.

The Role of Governments

Governments, however, have an opportunity to leverage this engine to boost Internet access and foster national and local content, in local languages and with immediate relevance to communities. To generate the kind of broadband capacity needed in most countries, there will need to be both distance-learning students and social networking subscribers. There will need to be both commercial content (some of it international) and national and local content. That is because investment will not happen unless there is pent-up demand, and demand will not happen until there are sustainable and essential services and apps to draw people onto the web. Governments themselves can play a strong role in generating content through e-government services and sponsoring cultural content, local app development and increased broadband access.

Governments also cannot ignore the ongoing challenges posed by the digital economy – and the larger digital ecosystem. Along with the immense positive aspects, there are some well-known problematic implications such as identity theft, phishing and other Internet frauds, malware of all kinds, privacy abuses and lack of control over personal information, dissemination of inappropriate material, psychological dependence or "addiction" to the Internet or Internet content, etc.

On the economic side of things, the challenges posed by the potential systematic hacking and theft of commercial data have been all too real. On the other hand, regulators also must guard against abuses of market power, in which operators may try to limit competition in downstream markets by "locking in" content providers or end users to their proprietary networks or content. Discussions and debates in recent years over "network neutrality" issues convey the high stakes for competition and consumer protection.

Clearly, many of the challenges involve protection of consumers – including vulnerable populations such as the elderly (often dubbed "digital immigrants") and children (usually seen as "digital natives"). Telecommunication sector regulators may well be practiced at the art of protecting consumers from operator price-gouging or quality-of-service violations. The new challenges posed by the digital ecosystem, however, are often outside their jurisdictions and beyond the scope of their legal authorities.

This does not mean, however, that sector regulators have no responsibility or capability to help protect consumers in these areas. They can cooperate and collaborate with other government offices and regulatory authorities to generate innovative educational and enforcement approaches to safeguard the integrity of networks and services and to help consumers defend themselves. There is a clear need for cross-sectoral cooperation among legislators, policy-makers and regulators, with multi-disciplinary teams needed to address non-traditional problems. Moreover, there is an opportunity to work with the experts in the private sector to harness their resources, capacities and experience, either through public-private partnerships or monitored self-regulation.

Perhaps the greatest challenge for policy-makers and regulators is to step back and survey the current state of their own telecommunication and ICT markets. They can then define with more accuracy the requirements and goals that must be addressed, as well as the highest-priority issues and challenges that must be addressed first. Once these goals and objectives are identified, governments can then look to their current procedures and laws to determine whether they have the proper regulatory instruments already in place to tackle their top priorities.

If not (and perhaps even in cases where they do), regulators need to assess whether a strong government intervention is needed, or if it would do more harm than good. In many instances, a "lighter-touch" approach involving mediation or negotiation among operators, or providing greater awareness and education to consumers, may be a logical approach – or at least the best starting point. Even where regulatory intervention is required, it should be targeted to achieve the desired result with the narrowest-possible impact.

In the middle of the second decade of the new century, the world can no longer ponder the "if" or "when" of the digital economy – which is, in fact, a digital ecosystem. Many of us are living in it, and many of our children are being raised in it. For those of us who are not, the clock is ticking on a generation that must catch up to it or potentially be left behind. The issues posed by this new ecosystem and the rapidly approaching era of 5G wireless services and the IoT – they are not just coming, they are already here.

Perhaps the best way to sum up where we find ourselves in 2016, with regard to the creation of the Information Society, is to drum up an old, familiar quote from the Twentieth Century British Prime Minister Winston Churchill: "This is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."

Endnotes

1 ITU ICT Facts & Figures 2015. Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Accessed on 31 January, 2016).

ALSO AVAILABLE FROM ITU

PUBLICATIONS

Trends in Telecommunication Reform: getting ready for the digital economy, 2015 (15th Edition)........185 CHF
Trends in Telecommunication Reform: 4th generation regulation: driving digital communications ahead (14th Edition)........Free
Trends in Telecommunication Reform: Transnational aspects of regulation in a networked society, 2013 (13th Edition)........185 CHF
Trends in Telecommunication Reform: Smart Regulation for a Broadband World, 2012 (12th Edition)........176 CHF
Trends in Telecommunicatiosn Reform: Enabling Tomorrow's Digital World, 2010/11 (11th Edition)........117 CHF
Trends in Telecommunication Reform: Hands-on or Hands-off? Stimulating Growth Through EffectiveICT Regulation, 2009 (10th Edition)......106 CHF
Trends in Telecommunication Reform: Six Degrees of Sharing, 2008 (9th Edition)........106 CHF
Trends in Telecommunication Reform: The Road to Next-Generation Networks (NGN), 2007 (8th Edition)........100 CHF
Trends in Telecommunication Reform: Regulating in the Broadband World, 2006 (7th Edition)........95 CHF
Trends in Telecommunication Reform: Licensing in an Era of Convergence, 2004/05 (6th Edition)........95 CHF
Trends in Telecommunication Reform: Promoting Universal Access to ICTs, 2003 (5th Edition)........90 CHF
Trends in Telecommunication Reform: Effective Regulation, 2002 (4th Edition)........90 CHF
Trends in Telecommunication Reform: Interconnection Regulation, 2000-2001 (3rd Edition)........90 CHF
Trends in Telecommunication Reform: Convergence and Regulation, 1999 (2nd Edition)........75 CHF

Please contact the ITU Sales Service:

Tel.: +41 22 730 6141
Fax: +41 22 730 5194
E-mail: sales@itu.int
Website: www.itu.int

Note: Discounts are available for all ITU Member States, Sector Members, Associates and Academia and Least Developed Countries.

International Telecommunication Union
Sales and Marketing Division
Place des Nations
CH-1211 Geneva 20
Switzerland

sales@itu.int
www.itu.int/publications

ISBN: 978-92-61-16551-2

Printed in Switzerland
Geneva, 2016

Photo credits: ©Shutterstock